

EASY NAC

CGX ACCESS DEPLOYMENT GUIDE

Installation and Configuration Guide

Easy NAC, CGX Access, and vLinks are trademarks of InfoExpress, Inc. Other product and service names are trademarks and service marks of their respective owners.

Copyright © 2023 InfoExpress Incorporated. All Rights Reserved. InfoExpress products and services are protected by one or more of the following U.S.

Patents: 8347351, 8347350, 8117645, 8112788, 8108909, 8051460, 7523484, 7890658, 7590733.
Additional patents pending.

www.infoexpress.com

www.easynac.com

V3.2.231219

Contents

Overview	9
Appliance Licensing Options.....	11
Appliance Specifications (as of Jan 2024).....	11
VM installation	12
Installing on ESX or ESXi server	12
Installing on Hyper-V server	13
Configuring CGX Access	16
Appliance Placement	16
Initial configuration	16
Basic IP configuration.....	17
Captive Portal IP Address.....	18
Remediation Portal IP Address.....	19
Connecting to Active Directory	19
AD Integration	20
Notifications: Email, SMS, Syslog, Slack, Teams and WhatsApp.....	22
Notification Contacts:	23
Configuring Notifications	23
E-mail Action Button.....	25
Protecting Additional Subnets	26
Adding Network Adapters	26
Using 802.1q trunk ports.....	27
Additional 802.1q configuration in VMware ESX / ESXi	28
Additional 802.1q configuration in Hyper-V server.....	30
Enforcement Overview	35
Configuring Access Policies.....	36
Auto Trust Policy	36
Access Group (ACLs).....	39
ACL Examples.....	40
ACL Syntax	41
Tagging Devices and Allowlisting.....	43
Tags.....	43
Allowlist \ Blocklist \ Excludelist \ Routerlist	45
The Excludelist	48
The Routerlist.....	48
Device Discovery	48

Device Profiling.....	49
DHCP Profiling.....	49
Fingerbank	49
NMAP Profiling.....	50
UPNP Profiling.....	51
SNMP Scan.....	52
Configuring Device Profiler Policies.....	53
Device Detail Data.....	53
Device Profiling Policies	53
Anti-spoofing Protection.....	56
Setting Fingerprints.....	56
MAC Spoofing Detection	57
IP Spoofing Detection.....	57
Fingerprint Rescan Interval.....	58
Multi-Factor Authentication	59
Mismatched Authentication	59
Rogue DHCP Server Detection	60
Time \ Location \ List Policies.....	62
Location Policy	62
Time Policy.....	63
Device-Lists Policy.....	64
Configuring Guest Access	66
Customize Captive Portal	66
Customize Guest Portal.....	67
Guest Registration Templates	69
Customizing Device Registration Templates for Guests	70
Setting up Sponsors.....	73
Sponsoring Users	74
Configuring Device Registration	75
Customizing the Device Registration portal	75
Confirm Active Directory settings.....	75
Customizing Device Registration Methods	77
User Experience	78
Integration: Anti-Virus \ Endpoint Management.....	80
Bitdefender Integration	81
Carbon Black Cb Response Integration.....	84

Carbon Black Cloud Integration	87
CrowdStrike Integration.....	90
Cybereason Integration	93
ESET Antivirus Integration	95
FireEye HX Integration.....	97
HCL BigFix Integration.....	99
Ivanti Security Controls	101
Kaseya VSA Integration	103
Kaspersky Antivirus Integration.....	105
ManageEngine Desktop Central Integration.....	107
ManageEngine Patch Manager Integration.....	109
Microsoft Intune Integration.....	111
Microsoft SCCM \ WSUS Integration.....	118
Microsoft Windows Management Instrumentation (WMI).....	120
Moscii StarCat Integration.....	123
Okta Integration	125
Palo Alto Cortex XDR Integration	127
SentinelOne Integration	131
Sophos Integration	134
Symantec Endpoint Protection Manager - 14.x	137
Trend Micro Integration.....	140
Trellix ePolicy Orchestrator Integration	143
Webroot Integration	145
Orchestration with Syslog.....	148
Syslog Event Creation.....	149
Orchestration - Email Alerts	151
Email Event Creation.....	152
Advance Security	154
Malware Lateral Spread Protection - Zero-Day.....	154
Policy-Based Response	155
Clearing Zero-day Events	155
Handling Exceptions.....	156
Deception – Hacking Detection	157
Policy-Based Response.....	158
Credentials used	158
Edge Protection – Layer-2 Security	159

Policy-Based Notifications	159
Agent Support	160
Working with Agents	161
Hosting Agents.....	162
Installing Agents	163
On-demand Agents (Recommended for Consultants)	164
Agent Compliance Policies.....	165
Policy Manager	165
Policies.....	166
Policies Best Practices	167
Requirements to Pass a Policy	167
Requirements Priority	168
Requirement Best Practices	169
Remediation	169
Pop-up Messages	170
Remediation Actions.....	170
Auto-remediation	171
Remediation Best Practices.....	171
Using Active Directory User Group in Auto Trust Policy	172
Prerequisites.....	172
DNS server and Domain Settings for CGX Access.....	172
Configure Active Directory User Group.....	172
Joining CGX Access to Active Directory	173
CyberGatekeeper Agent Authentication Plugin.....	174
Add the User Group as a condition in Auto Trust Policy	175
Troubleshooting Agents.....	175
Installation Issues.....	175
Connection Issues	177
Advanced Configuration Options	179
Administration Permissions	179
Configuring 2FA for CGX Admin Login	181
Configuring Radius for CGX Admin Login or BYOD Authentication.....	183
Radius Server Configuration.....	183
CGX-Access Configuration	183
Customizing Landing Pages	185
High Availability	187

Requirements	187
Configuration – Standalone Appliances	188
Configure the Primary unit	188
Configure the Backup unit	189
Configuration – Centrally Managed Appliances	191
Configure the CVM to be an Arbiter (optional)	191
Configure the Primary unit	192
Configure the Backup unit	194
Making HA Configuration Changes	196
Replace a Primary	196
Replace a Backup	196
Restore from a Backup Image	196
Upgrade to a New Version	196
Other Reconfiguration Changes	196
Central Visibility Manager	197
CVM Overview	197
Required Ports	197
Configuring a Central Visibility Manager	198
Configuring an Appliance to be Centrally Managed	201
Deployment Manager	203
Software Updates	204
Central Visibility Manager – Device Roaming	206
Central Visibility Manager – Integration Proxy	207
Maintenance and Support	209
Upgrading firmware	209
Collecting Logs (Dump2)	210
Appendix A – Certificate Management	214
Option 1 - Generate Certificate Signing Request (CSR) to obtain a certificate from your CA	214
Option 2 - Upload certificate and private key to CGX Access. (When CSR is not generated)	218
Appendix B – vLinks Deployment	221
vLinks Overview	221
vLinks Central Setup	222
vLinks Remote Setup	227
Appendix C – Inline Enforcement	233
Inline Enforcement Overview	233
Features	233

Requirements	233
Sample Test Network.....	234
Configuration	234
Location	235
Network Interfaces.....	235
Bridge IP	236
Access Control List.....	237
Enforcement Ranges	238
Agent Requirement	240
Appendix D – Enforcer Agents.....	241
Enforcer Agents Overview	241
Enforcer Agent Install.....	242
Accepting the Enforcer Agent	244
Appendix E – WhatsApp Integration.....	246
WhatsApp Prerequisites Steps	246
WhatsApp Registration Process.....	246
Enabling WhatsApp Alerts	249
Enabling WhatsApp for Guest Approval	250
Appendix F – 802.1x RADIUS Proxy	252
Radius Proxy Overview	252
Requirements	252
Features.....	252
Configuring Radius Proxy settings on CGX Access	253
Appendix G – Using NPS to Authenticate CGX-Access users	257
Add admin group/users to Active Directory.....	257
Configure Network Policy Server.....	258
Configure CGX-Access to allow login using radius.....	262
To authenticate BYOD users via Network Policy server	263

Disclaimer

The information in this document is subject to change without notice. The statements, configurations, technical data and recommendations in this document are believed to be accurate and reliable but are represented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document.

This document is provided for your use to help understand the behavior of the product.

Although the information is believed to be substantially accurate at the time that it was written, this document doesn't imply that specific features or functionality are present in your version of the product.

InfoExpress Inc. makes no express or implied warranties regarding the product's features or behavior as described herein. For product specifications, please refer to the product documentation included with product installation.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners.

The information in this document is proprietary to InfoExpress Inc.

Easy NAC Solution

Overview

The Easy NAC solution with CGX Access appliances provides the following features:

Agentless Visibility

CGX Access lets you see devices that join your network, without the use of agents. Visibility is immediate, with any untrusted device being immediately restricted, as desired. Devices will be both passively and actively profiled to determine operating system, manufacturer, and type of device.

Easy to Implement Enforcement

CGX Access uses ARP enforcement with DNS and HTTP redirection to control which devices can access the network. ARP enforcement is an out-of-band enforcement method that doesn't require network changes. It works with any network infrastructure, both managed and unmanaged switches. For Remote Access VPN protection, Inline enforcement can be used.

Simple LAN \ WLAN Protection

It is easy to control which devices are allowed to access the network. Untrusted devices and rogue infrastructure that joins the network will immediately be detected and automatically restricted in real-time. Devices can be allowed access with simple ON \ OFF controls or policies can be set for automated access.



Automated MAC Address Allowlisting

CGX Access will regularly check with your Active Directory server to verify which devices are domain-joined. Devices that are confirmed as domain-joined will automatically be granted full access to the network. Devices that are not domain-joined can be manually tagged as approved. In addition, device profiling can also be used to automate the process of tagging approved devices.

Anti-Spoofing Protection

CGX Access provides a fingerprint feature to protect against MAC address spoofing. All devices on the network are profiled for their MAC address, IP, Operating System, Hostname, and other attributes. This information can then be used to set a unique fingerprint for each device. Once a fingerprint has been set, the device(s) will be protected from spoofing.



Enforce Anti-Virus and Security Policies

CGX Access integrates with enterprise Anti-Virus vendors and leading endpoint management solutions, to verify endpoint security is active and up to date. By integrating with leading security solutions, CGX Access can enforce compliance with security policies. Devices out-of-compliance can be restricted at the point of network access.

Orchestration

Security appliances that are designed to monitor devices and network traffic can send event-based alerts for administrative action. CGX Access can receive e-mail alerts or event-based syslog messages from Firewalls, APT, IPS, SIEM, and many other types of security devices and then take immediate action when necessary. If CGX Access receives an alert that a device has malware, we can restrict it immediately.

Malware Lateral Spread Protection– Zero-day Protection

CGX Access unique layer-2 visibility of the network allows for the immediate detection of suspicious behavior, such as devices making excessive connections attempts to endpoints on the same network segment. This real-time detection provides immediate protection against zero-day malware propagating on the network.

Deception – Hacking Detection

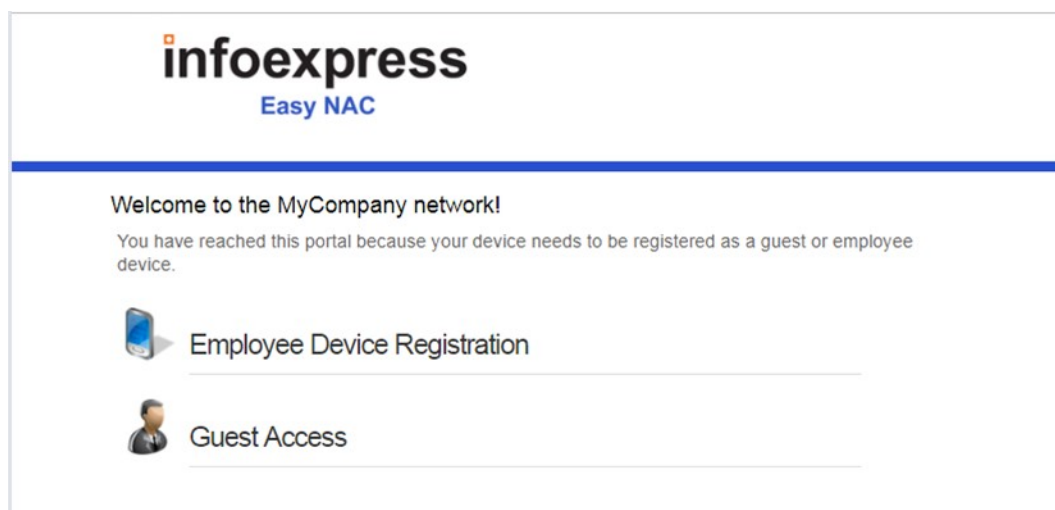
The Easy NAC solution will host fake services such SSH, Telnet, FTP, etc. on every VLAN or subnet its protecting, creating a distributed honeypot. These fake services serves no real business purpose, so if any person or bot tries to login to these fake services, it's a strong indicator of hacking activity. With virtual honeypots on every VLAN, it provides early indication of hacking activity before hackers reach the core of the network.

BYOD Registration

CGX Access provides a self-registration portal to automate the BYOD registration process. Policies can be set, by groups, to limit the number and type of BYOD devices. It improves security by tracking device ownership, restricting the locations, and limiting network access to approved resources.

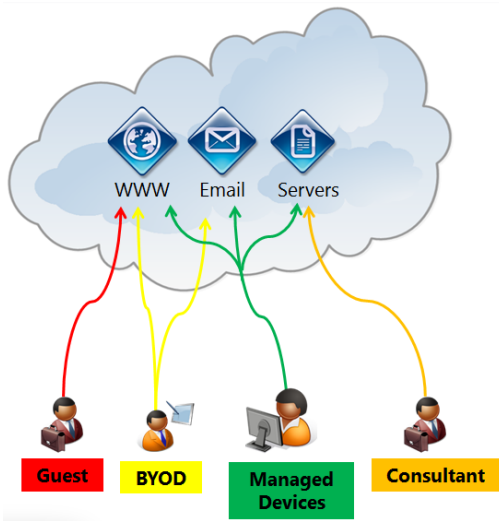
Guest Access

CGX Access lets sponsors register guest accounts or authorize guests to create their own accounts via the landing page. Sponsors can authorize individual registrations or register groups for classes or meetings with configurable expiration times.



Role-based Access Control

CGX Access enhances security by limiting devices to only the resources required. Guests are limited to internet only access. BYOD and consultant devices can be limited to specific resources.



Appliance Licensing Options

CGX Access is available as a physical appliance or as a virtual appliance. Licensing is based on the number of devices that CGX Access solution has visibility of. When using the Central Visibility Manager, a distributed license option will enable a license to be shared between multiple appliances.

Please contact your authorized partner or InfoExpress for up-to-date information on licensing. sales@infoexpress.com

Appliance Specifications (as of Jan 2024)

Appliance Specifications	Access Mini CGXA-S10	CGX Access CGXA-S100	Access 200 CGXA-S200	Access 500 CGXA-S500	Access 600 CGXA-S600	Access VM ENAC-VM
Scalability						
Maximum Devices	300*	2500*	5,000*	10,000*	10,000*	10,000*
Maximum Subnets	10	100	100*	200*	200*	200*
Number of Ports	4	8	8	8	10 2 pairs of by-pass NICs.	8-10 virtual adapters

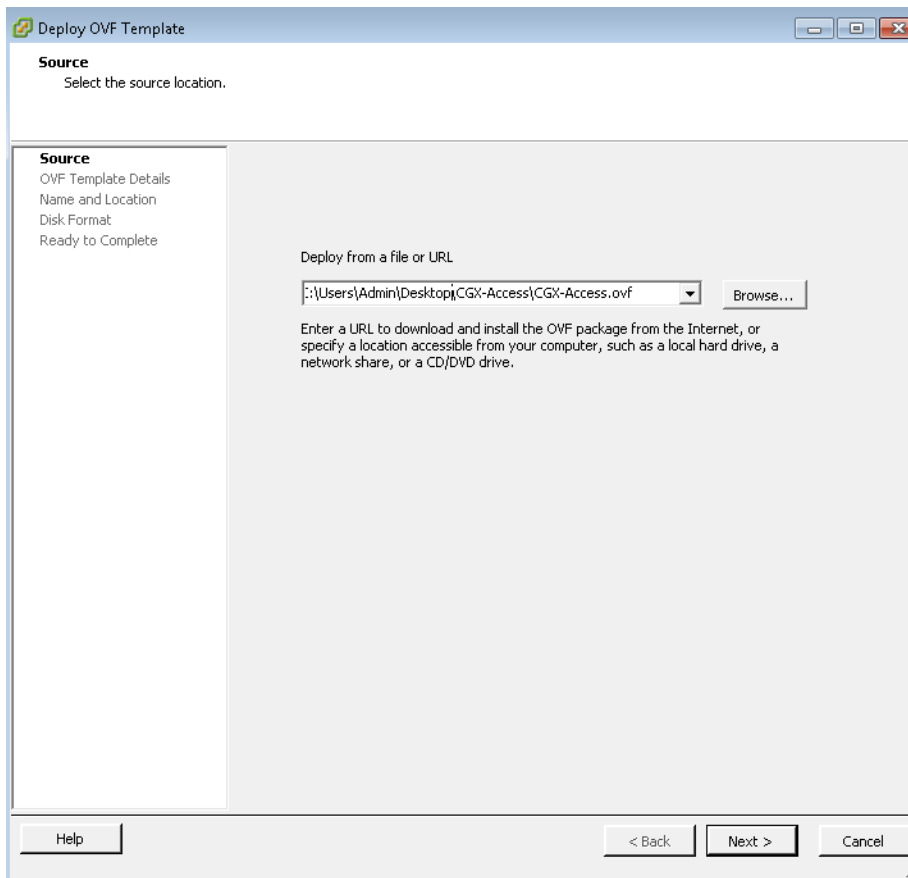
* Capacity is approximate and depends on VLANs protected, endpoints, and features enabled.

VM installation

Installing on ESX or ESXi server

The virtual CGX Access appliance can be deployed as an .ovf template native to VMWare. You will need the CGX Access .ovf image, which is usually provided as a zip file. Please contact InfoExpress or your business partner to obtain this file.

- Unzip the provided file to a location accessible to the vSphere client application.
- In the VMWare vSphere Client, choose File - Deploy OVF Template
- On the first screen, select the .ovf file

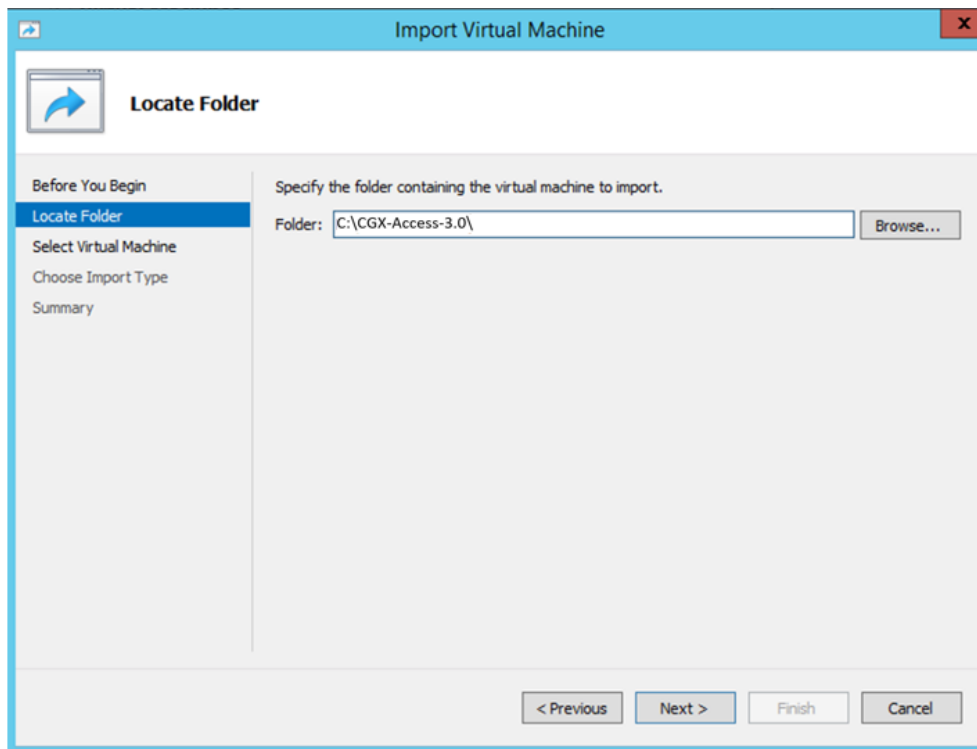


- Click next on the OVF Template Details screen. (There may be a warning screen here, but you can proceed).
- Provide a name and optionally a location for the template and click 'Next'
- Select the datastore where the virtual machine files should be kept and click 'Next'
- Select the desired format for your installation and click 'Next'
- Select the desired network mapping for the interfaces and click 'Next'
- Verify the options and click 'Finish' when ready to proceed
- The vSphere client will then proceed to deploy the image.

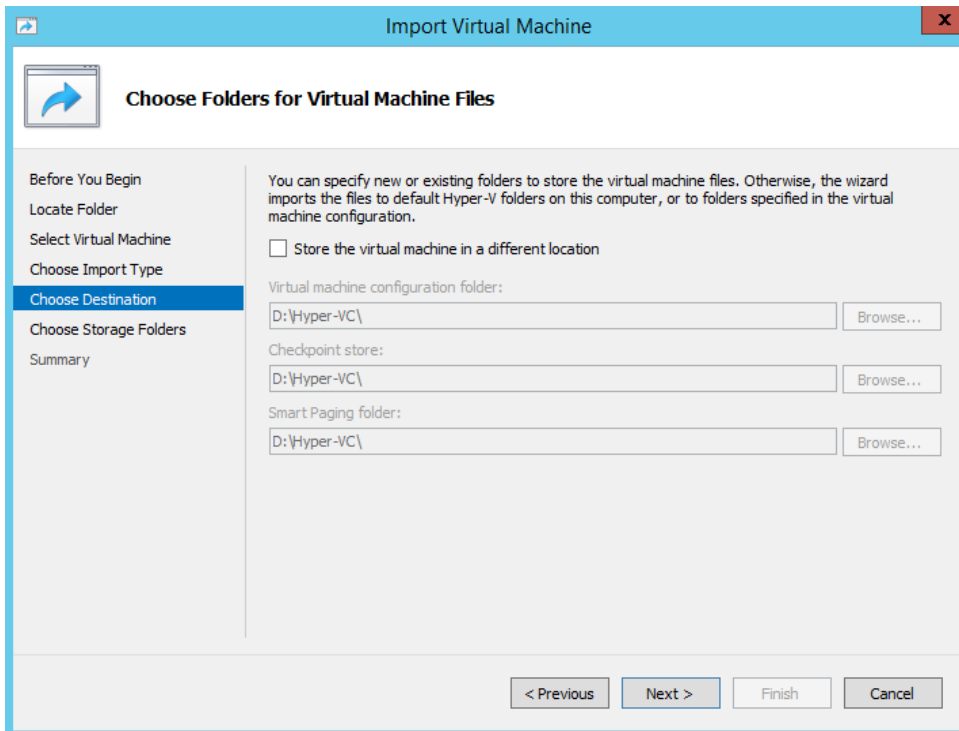
Installing on Hyper-V server

The virtual CGX Access appliance can be deployed using Hyper-V Manager, Windows Server 2012 R2 and above only. The CGX Access Hyper-V image is usually provided as a zip file. Please contact InfoExpress or your business partner to obtain this file.

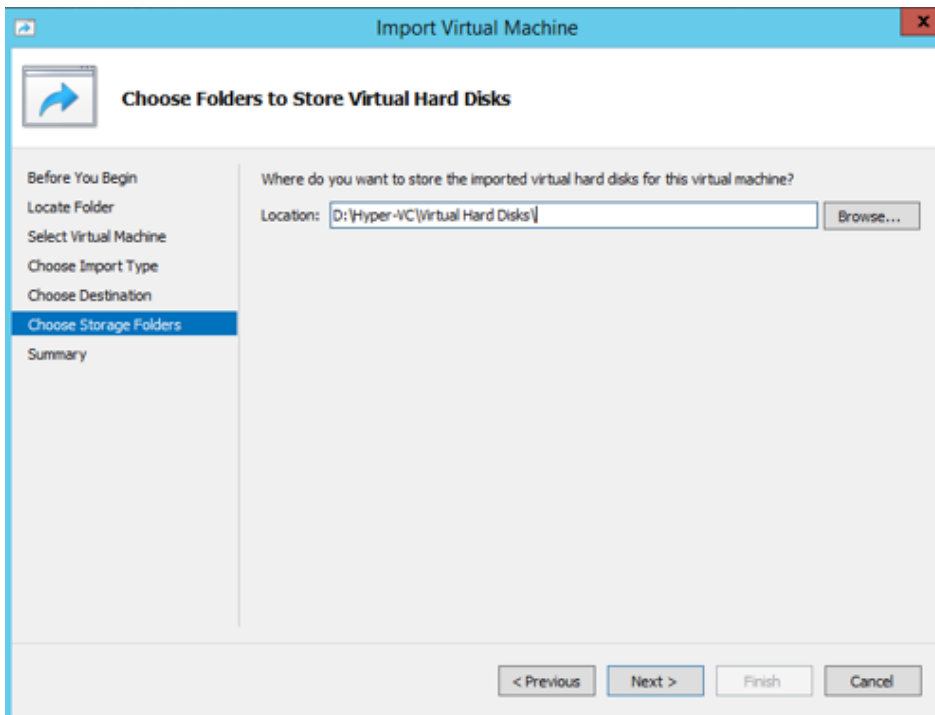
- Unzip the provided file to a location accessible to the Hyper-V Manager.
- In the Hyper-V Manager, Click Action menu and select Import Virtual Machine
- On the first screen, Specify the folder of extracted image and click next



- Select the listed virtual machine 'CGX-Access-3.0.ovf'. Click next.
- Choose Import type as 'copy the virtual machine (create a unique ID)'
- Click Next and specify the Destination folders for different settings

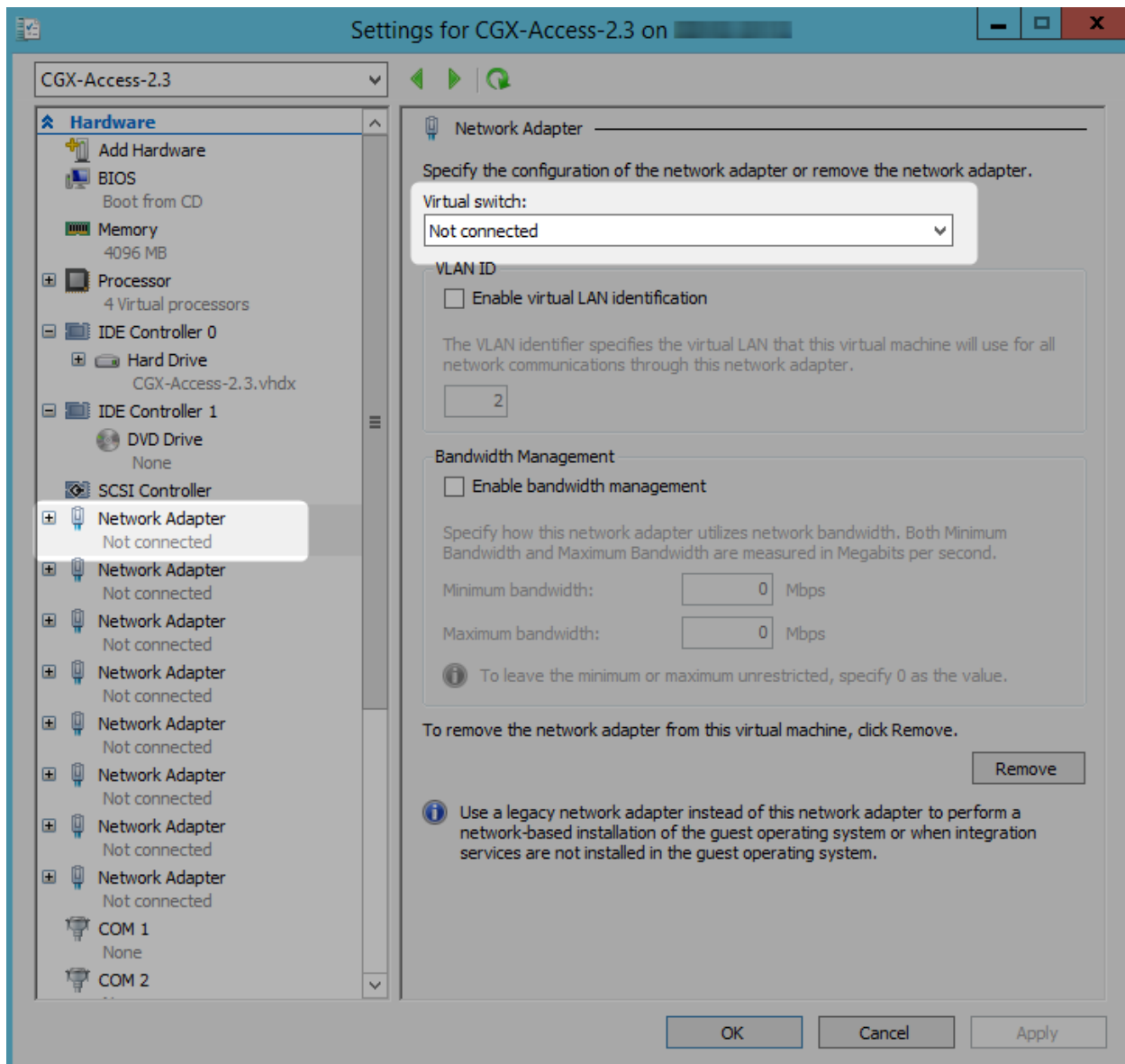


- Select the Virtual Hard Disk destination folder in the next screen.



- Verify the options on Summary page and click 'Finish' when ready to proceed.
- The Wizard will then proceed to deploy the image.
- The Virtual Machine will be listed in Hyper-V Manager.
- Select the virtual machine 'CGX-Access-3.0' and click 'Settings' from 'Action' menu.

- Select the Network Adapter and assign a Virtual switch from the right-side drop-down box as highlighted below and Apply the setting.



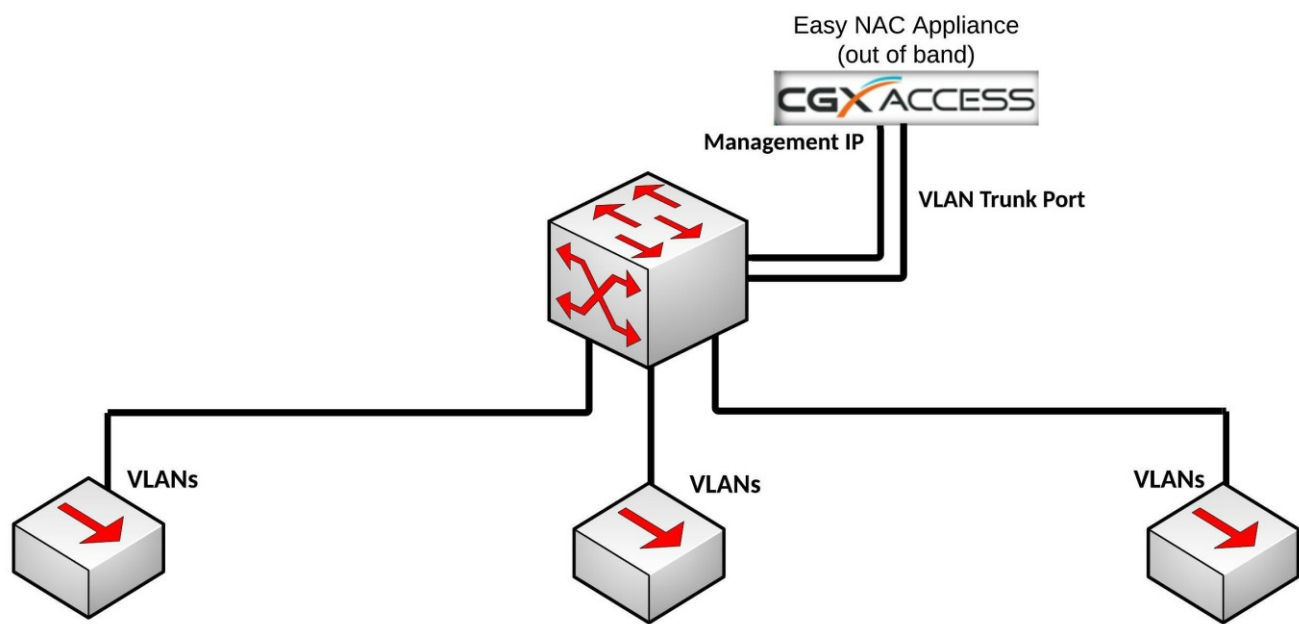
Configuring CGX Access

This section will walk the administrator through the steps needed to configure a CGX Access appliance.

Appliance Placement

CGX Access provides protection \ access control on the subnets it is attached to, with layer-2 visibility. The CGX Access appliance can protect up to 200 VLANs concurrently with the use of 802.1q trunk ports. The Managed IP interface is the primary interface and is used for appliance management. The CGX Access appliance should be able to communicate with the AD server via the Managed IP.

For simple one subnet testing, the Managed IP should be on a subnet you wish to enforce access control on. To support multiple VLANs, additional network interfaces or trunk ports can be used.



Initial configuration

CGX Access typically requires three static IP addresses in a deployment. One IP is used for management of CGX Access appliance. The second IP is used for the captive portal (landing page), and a third IP is used for a remediation portal. When protecting additional VLANs, each additional subnet protected will also use one IP on its respective subnet. For example, when protecting ten subnets, a total of twelve IPs will be used. These additional IP's can be dynamically assigned by DHCP.

Note: The CGX Access appliance provides built-in ARP-based enforcement. Enforcement can be enabled on up-to 200 VLANs, including the subnet with the Managed IP.

Basic IP configuration

- For physical appliances, use a direct connect ethernet cable for SSH access to the default IP Address 10.0.0.250/24. Alternatively, plug-in a keyboard and HDMI monitor.
- For virtual appliances, open a console window and power on the VM.

Once the boot cycle is complete you will be prompted for a login.

- Login as `admin/admin`.
- From the main menu choose 1 (Run setup wizard) and follow the prompts to set the Managed IP address and netmask, the default gateway, DNS servers, system name, time zone and date/time.

Note: Keep the admin password in a safe place. If it is lost without having access to an alternate admin level account, there will be no way to recover the password.

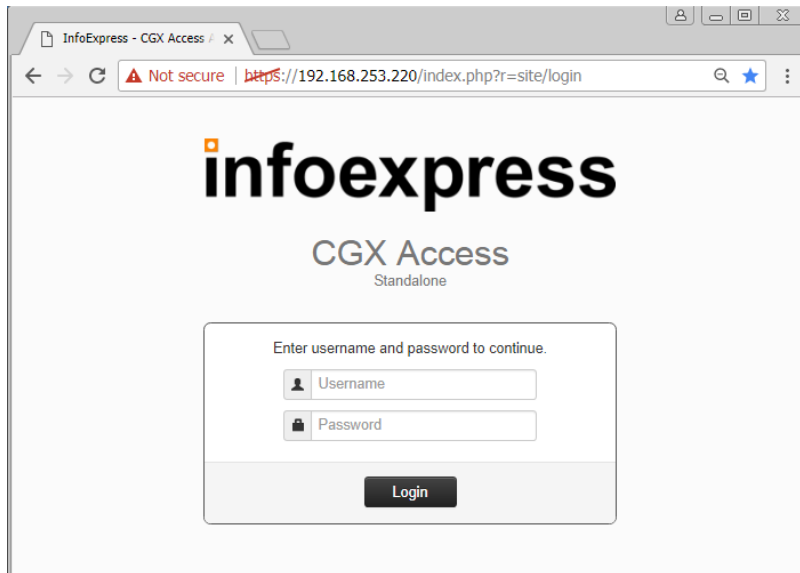
Default user accounts are:

- `admin` - used for initial setup and configuration as well as SSH access for maintenance tasks
- `cguser` - used for uploading files through ftp

Note: The default passwords are the same as the username. These default passwords should be changed.

When the setup wizard completes, the system should be accessible on the network.

- Confirm that you can ping the management IP from another system on the same subnet and also from a system on another subnet. If the pings fail double check the physical or virtual connections and the basic IP configuration
- Connect to the CGX Access web GUI by opening `https://<Managed ip>` (that was configured previously). Compatible browsers include:
 - Microsoft Edge
 - Firefox v65 or higher
 - Chrome Version 89 or higher
 - Safari v12 or higher



- Login as user admin (default password admin). A modern browser such as Chrome is strongly recommended. Older versions of IE or Firefox may not display the pages correctly.

Captive Portal IP Address

A separate IP address will be used for the Captive Portal \ Landing pages. When configured, new devices joining the network can be redirected to this page, using the default "DNSREDIRECT(CaptivePortal)" rule in the default "Restricted" Access Group (ACL). To configure this Captive Portal IP address...

- In CGX Access GUI go to Configuration → Appliance Settings
- Provide IP and subnet mask in the field provide

Networking:

Adapters	IP / Netmask	Gateway	Metric	VLAN ID	Location	Configuration	State	VLAN
Adapter #1 MAC: 00:50:56:a4:e4:12 Speed: 10 Gb/s	10.160.0.100/255.255.255.0	10.160.0.1	1		Cloud demo	Managed IP	↑	+
Adapter #2 MAC: 00:50:56:a4:89:0c Speed: 0 Gb/s	/		500			Off		+

Submit Network Changes

DNS & Domain Name:

DNS Servers: 8.8.8.8 1.1.1.1

Hostname: cgx-access

Domain Name: easynac.demo

Submit DNS & Domain Name

Landing Pages:

Support NAT'd:

Host Name for Captive Portal: []

Captive Portal's IP Address: 10.160.0.101/255.255.255.0 Adapter #1

Host Name for Remediation Portal: []

Remediation Portal's IP Address: 10.160.0.102/255.255.255.0 Adapter #1

Submit Landing Pages

- Click "Submit Landing Pages" button

Remediation Portal IP Address

An additional static IP can be assigned to an optional Remediation Portal. When configured, the non-compliant endpoints can be redirected to this page, so they are aware their device is restricted and know the reason why.

To configure a Remediation Portal IP, use the same steps as above.

Connecting to Active Directory

Authentication credentials are often stored in an Active Directory server. Active Directory can be used to validate credentials with the following CGX Access features:

- Employee Device Registration (see Configuring Device Registration)
- Sponsoring Guest accounts (see Configuring Guest Access)
- Permissions for administrators to access the management GUI (see Advance Configuration)

Configure Active Directory server settings on CGX Access

- In CGX Access GUI go to Configuration → General Settings.
- Click on Active Directory Servers

The screenshot shows the 'Edit Setting' dialog box for configuring an Active Directory server. The dialog has a title bar with 'Edit Setting' and a close button. Below the title bar is a button labeled 'Add New Active Directory Server'. The main content area is titled 'Server 1' and contains the following fields and sections:

- Host or IP:** 10.160.0.200
- Account Suffix:** @easynac.demo
- LDAP Query User Name:** event
- LDAP Query Password:** [Redacted]
- Encryption:** None
- Group Query From:** Domain Groups
- Query Timeout:** 60
- Computer Query Settings:**
 - Query Covers:** Entire Directory
 - Test Computer Query:** [Button]
- Test LDAP Connection:** [Button]

At the bottom of the dialog are three buttons: 'Save', 'Cancel', and 'Help'.

- Under "Active Directory Server", enter the host or IP address of the AD domain controller and the Account suffix in the "Account Suffix" field. A Username and Password is often required.
- Use the "Test LDAP Connection" button to test the settings

Note: the @ symbol should be included in the Account Suffix

Note: up to 20 AD servers can be configured per appliance

AD Integration

Tip: For faster deployments, AD integration can be enabled. When enabled, devices joined to the domain will be tagged as AD-managed, and automatically granted full access to the network.

- In CGX Access GUI go to Configuration → Integration
- Click on Active Directory Integration

Edit Action

Active Directory Integration

Enable Integration
 Check the hostname inconsistency

Server Configuration

Query Interval (Seconds)

Policy

CONDITION
 Tag devices that are domain computers

TAG

AD-managed

Single AD Server

Tag devices with no user login in days
 stale-login

Multiple AD Servers

Tag device with no user login in days
 stale-login

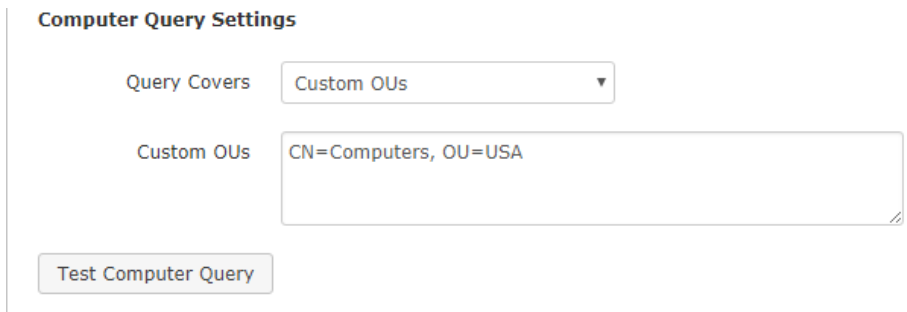
Note: With multiple AD servers, lastLogin timestamp is updated only after it's 14 days or older, so the check period should be at least 15 days.

Save Cancel Help

- Check "Enable Integration"
- Check "Tag devices that are domain computers"
- DNS can sometimes be useful to increase the number of devices tagged as AD-managed. However, if DNS information is stale, it can lead to false positives. To use DNS enable, Configuration → Integration → Setting Shared by All the Integrations

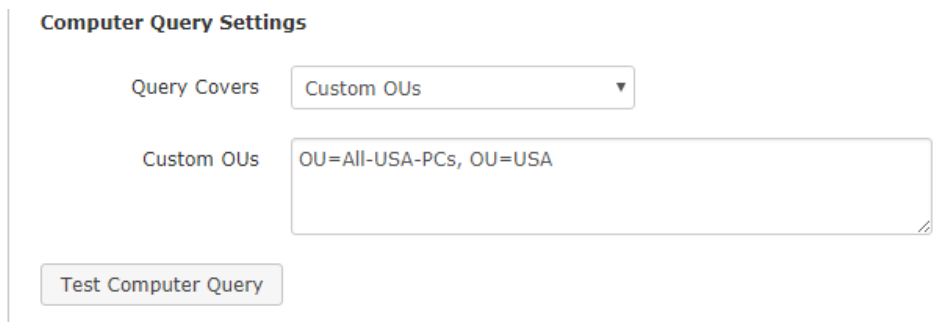
Note: In some cases, AD computer objects may be stored in a non-default OU. In these cases, it may be necessary to adjust the OUs that need to be queried. Custom OUs can be specified in the Active Directory Server section under Configuration → General Settings

Example 1 - An Active Directory of domain CGX.ACCESS has an OU called “USA” and computer accounts for the OU is stored under “Computers”. The custom OU query should look like CN=Computers, OU=USA



The screenshot shows the 'Computer Query Settings' configuration page. It features a dropdown menu for 'Query Covers' set to 'Custom OUs'. Below it is a text input field for 'Custom OUs' containing the query 'CN=Computers, OU=USA'. A 'Test Computer Query' button is located at the bottom left of the form.

Example 2 - An Active Directory of domain CGX.ACCESS has an OU called “USA” and computer accounts for the OU is stored under another child-OU named “All-USA-PCs”. The custom OU query should look like OU=All-USA-PCs, OU=USA



The screenshot shows the 'Computer Query Settings' configuration page. It features a dropdown menu for 'Query Covers' set to 'Custom OUs'. Below it is a text input field for 'Custom OUs' containing the query 'OU=All-USA-PCs, OU=USA'. A 'Test Computer Query' button is located at the bottom left of the form.

Tip: It may be easier to set the Query to cover the Entire Directory.

Notifications: Email, SMS, Syslog, Slack, Teams and WhatsApp

CGX Access can send notifications when all types of events occur. The notifications can be sent with:

- Auto Trust Policy
- Roles & Access Policy
- Monitoring Policies
- Device Profiling Policies
- Guest registration Templates

To configure the E-mail server or other notification servers used by CGX Access:

- Go to Configuration → General Settings
- Select E-mail Server, Syslog Server or Other Servers
- Select appropriate notification server

The screenshot shows a configuration window titled "Edit Setting" with a close button (X) in the top right corner. The window is divided into two main sections: "Outbound Mail Server" and "Inbound Mail Server".

Outbound Mail Server:

- Credential Type: SMTP (dropdown menu)
- Host or IP: E.g. smtp.gmail.com or smtp.gmai (text input)
- User Name: (text input)
- Password: (password input with eye icon)
- Encryption: MSA/STARTTLS (Port 587) (dropdown menu)
- Ignore Certificate Validation
- Send Email (button)

Inbound Mail Server:

- Same as Outbound
- Host or IP: E.g. imap.gmail.com or imap.gmail (text input)
- User Name: (text input)
- Password: (password input with eye icon)
- Encryption: IMAP (Port 143) (dropdown menu)
- Test Inbound Server (button)

Email Accounts Used to Send Reports, Guest Confirmations or Password Resets:

- Sender: (text input)
- BCCed: (text input)

At the bottom right of the window are three buttons: Save, Cancel, and Help.

The example shown above is for an E-mail Server

- Enter the information needed and click 'Save'.
- Enter an email address used as sender address and optionally one or more addresses that will be Bcc'd on guest registration emails
- The Inbound Mail Server is for use with Orchestration integrations with E-mail

Note: For Slack or Teams notifications please request the separate integration guide from your InfoExpress representative.

Note: For setup of WhatsApp notifications please see [Appendix E](#).

Notification Contacts:

- Go to Configuration → General Settings and click on the “Contact Information for Notifications” section.

#	Name	E-mail Address	SMS Number	WhatsApp Contact	Slack Channel/User ID	Teams Channel/User ID	Action
1	Admin	admin1@mycompany.com					Edit Delete
2	Second Admin2	admin2@mycompany.com					Edit Delete

Prev 1 Next Pages: 1

For Email
Notification Subject Line: EasyNAC Notification

Syslog Notification
Destination Syslog Server: [Dropdown]
Log Format: [Dropdown]

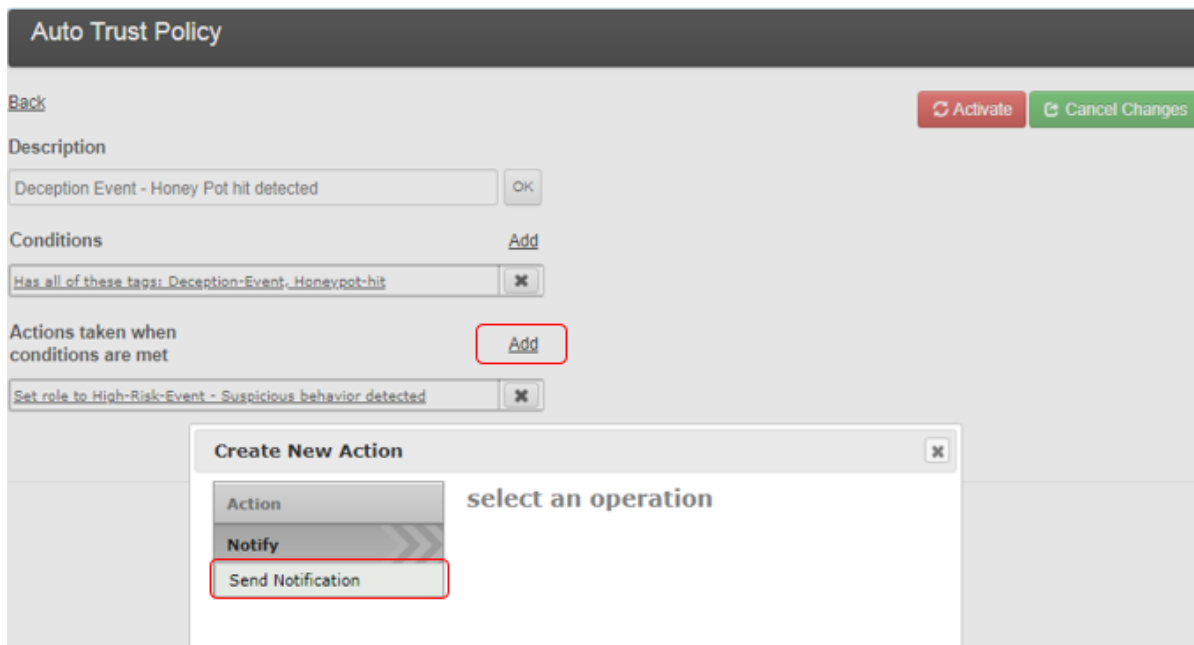
Save Cancel Help

- Fill in the info for at least one administrative contact that should get notified when notifications are sent.

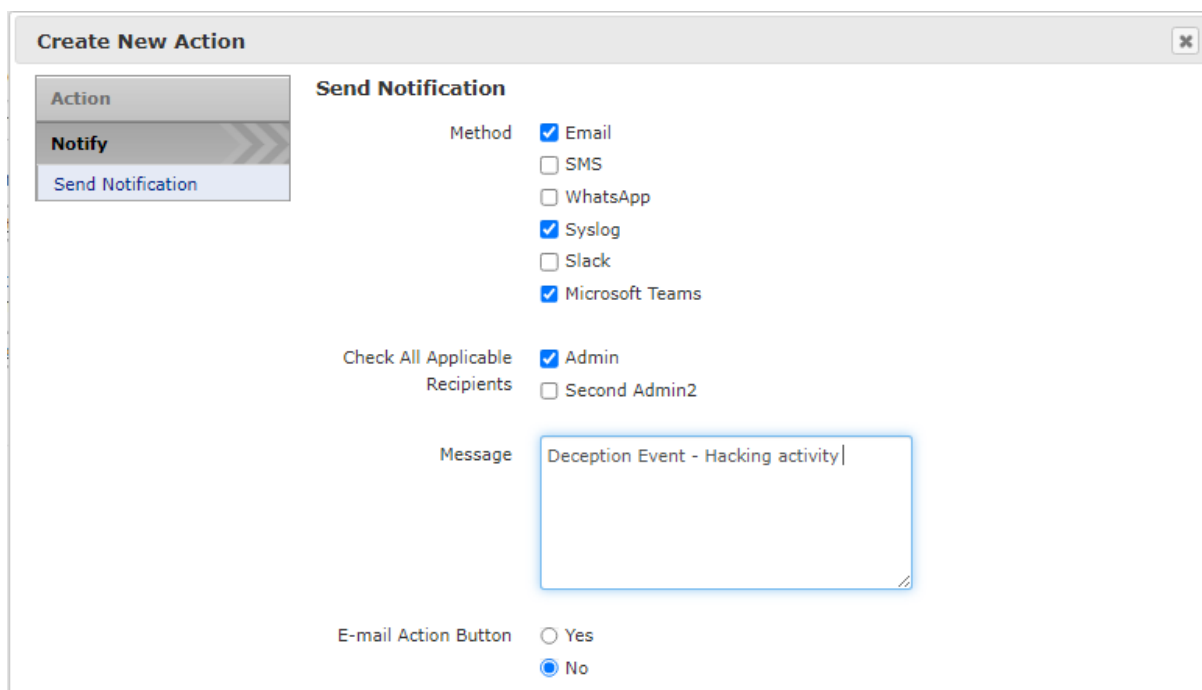
Configuring Notifications

Notifications can be configured and sent using Auto Trust Policy, Roles & Access Policy, Monitoring policies, and Device Profiling policies. Different actions are available when matching condition are met.

The example shown below is for the Auto Trust Policy...



- Next to Actions taken... → click Add
- Click “Send Notifications”
- Select Method of alert, Recipients, and preferred message



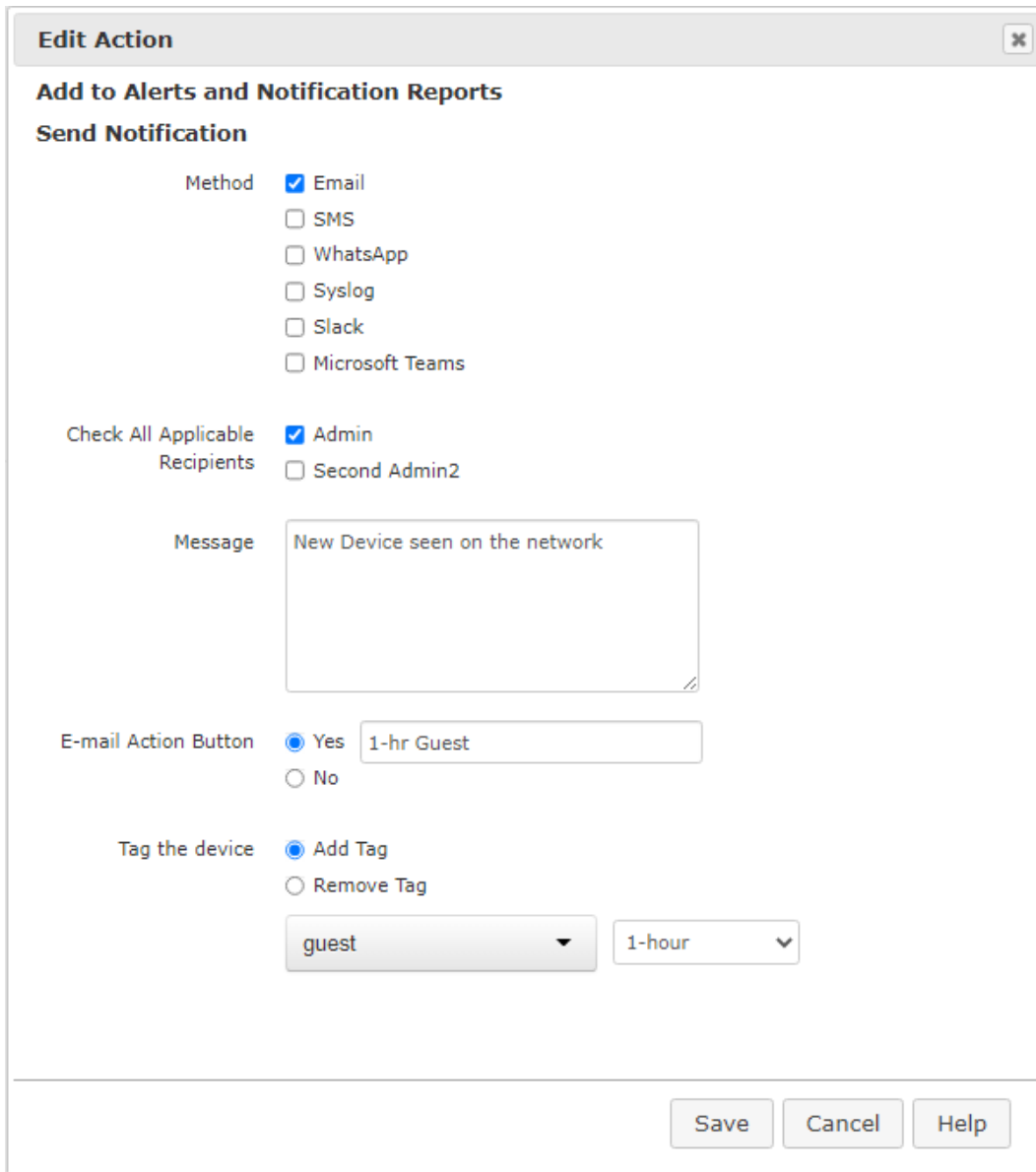
- Select Method of alert, Recipients, and preferred message
- Click “Save”
- Click the “Activate” button for the changes to take effect



E-mail Action Button

When sending E-mail based notifications, an Action Button, can be configured so quick actions can be taken from within email itself. In the example below, a Monitoring policy can send an email when a new device is seen on the network for the 1st time.

The Action Button is configured to add the “guest” tag to the the device for a period of 1 hour, if the email recipient(s) clicks the Action Button within the email sent.



The screenshot shows a web-based configuration window titled "Edit Action". The window has a close button in the top right corner. Below the title bar, there is a section "Add to Alerts and Notification Reports" with a sub-section "Send Notification".

Under "Send Notification", the "Method" section has several options: "Email" (checked), "SMS", "WhatsApp", "Syslog", "Slack", and "Microsoft Teams".

The "Check All Applicable Recipients" section has "Admin" (checked) and "Second Admin2".

The "Message" field contains the text "New Device seen on the network".

The "E-mail Action Button" section has "Yes" (checked) and "No". The "Yes" option is associated with a text input field containing "1-hr Guest".

The "Tag the device" section has "Add Tag" (checked) and "Remove Tag". Below these options are two dropdown menus: the first is set to "guest" and the second is set to "1-hour".

At the bottom right of the window are three buttons: "Save", "Cancel", and "Help".

Note: For this feature to work as expected, the email recipient would need to have network connectivity to the Management IP address of the appliance. They would not need login credentials. The Auto Trust Policy would also need to be configured to assign Guest Access when a device has the guest tag.

Protecting Additional Subnets

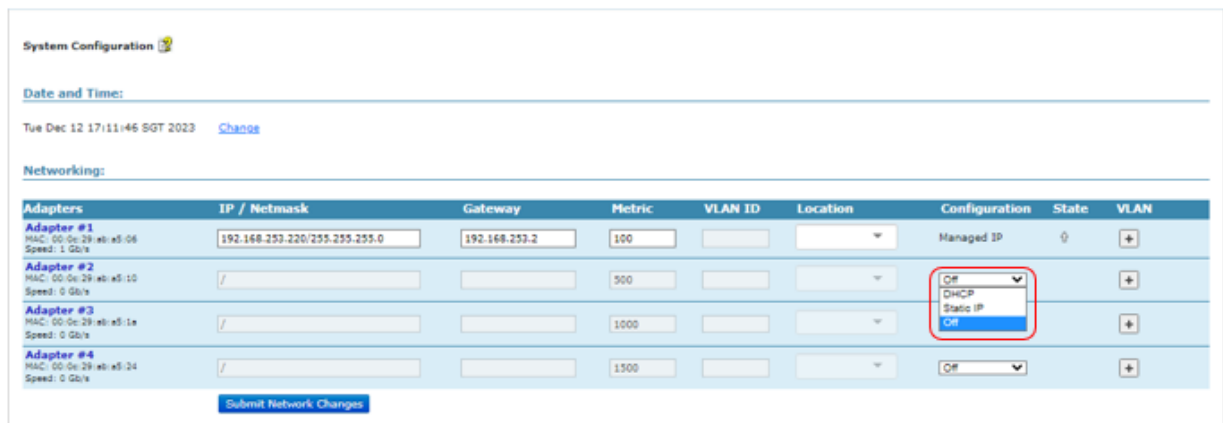
With the use of ARP enforcement, CGX Access requires layer-2 visibility of ARP broadcast traffic to detect and restrict devices. There are two methods that can be used to extend visibility to multiple subnets.

- **Method 1 – Physical connection:** Add additional network adapter and plug-in to a normal switch access port to extend protection to additional subnet. The physical appliances support up-to 6 adapters and the virtual appliance can support up to 10 adapters. Hyper-V supports 8 adapters.
- **Method 2 – 802.1q trunk:** Use 802.1q trunk ports so multiple VLANs can be protected with just one or more adapters. With the use of trunk ports up to 200 VLANs can be protected. Multiple adapters are recommended if there is extensive traffic from devices being restricted with ACLs.
 - **Virtual CGX Access appliances** also supports 802.1q. Please note that additional configuration in the ESX/ESXi or Hyper-V server would be required.

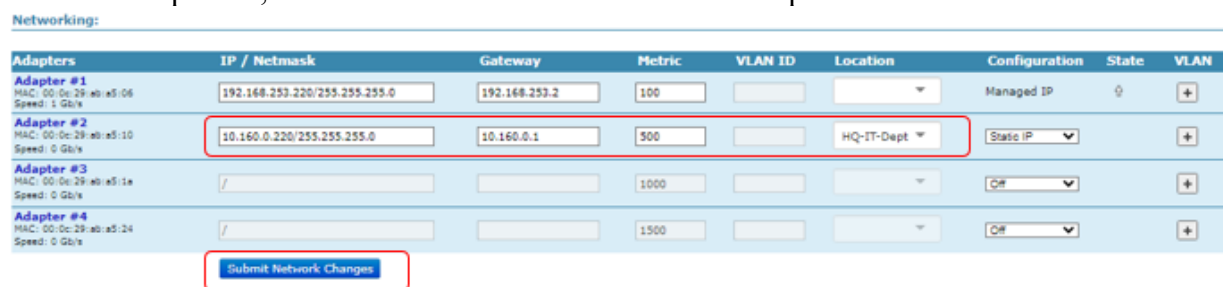
Adding Network Adapters

If using VMware, the virtual appliance is pre-configured with 10 virtual adapters. To configure adapters inside the virtual appliance, go to:

- In CGX Access GUI go to Configuration → Appliance Settings
- Select the method the IP address will be assigned to the adapter



- Complete IP address information if a static IP address will be used. DHCP can also be used.
- Metric field will be automatically configured
- Location is optional, and is recommended for location-based policies



- To confirm the network changes, click the “Submit Network Changes” button

Note: When adding adapters to the CGX Access virtual appliance, the adapter must first be provisioned within the VMware host and then connected to the virtual appliance.

Using 802.1q trunk ports

If the network is configured to support VLAN tagging, then adding additional VLANs is simple.

Note: One or more adapters connected to the CGX Access appliance must be attached to a switch port(s) configured as a trunk port.

- In CGX Access GUI go to Configuration → Appliance Settings
- Click “+” button on the adapter attached to a trunk port

Networking:

Adapters	IP / Netmask	Gateway	Metric	VLAN ID	Location	Configuration	State	VLAN
Adapter #1 MAC: 00:0c:29:ab:a5:06 Speed: 1 Gb/s	192.168.253.220/255.255.255.0	192.168.253.2	100			Managed IP	0	+
Adapter #2 MAC: 00:0c:29:ab:a5:10 Speed: 0 Gb/s			500			OFF		+
Adapter #3 MAC: 00:0c:29:ab:a5:1a Speed: 0 Gb/s	/		1000			OFF		+
Adapter #4 MAC: 00:0c:29:ab:a5:24 Speed: 0 Gb/s	/		1500			OFF		+

- Complete VLAN ID and static IP address information, if necessary. DHCP can be used.

The screenshot shows a dialog box titled "Add Vlan" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- VLAN ID (1-4094):** A text input field containing the value "100".
- DHCP:** A dropdown menu currently set to "DHCP".
- IP / Netmask:** An empty text input field.
- Gateway:** An empty text input field.
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

- To confirm the network changes, click the “Submit Network Changes” button...

Networking:

Adapters	IP / Netmask	Gateway	Metric	VLAN ID	Location	Configuration	State	VLAN
Adapter #1 MAC: 00:0c:29:abe5:1e06 Speed: 1 Gb/s	192.168.253.220/255.255.255.0	192.168.253.2	100			Managed IP	⬆	+
			500			Off		+
Adapter #2 MAC: 00:0c:29:abe5:1e10 Speed: 0 Gb/s			5100	100	Floor 1	DHCP		⊗
			5102	102	Floor 2	DHCP		⊗
			5200	200	Finance	DHCP		⊗
Adapter #3 MAC: 00:0c:29:abe5:1e1a Speed: 0 Gb/s	/		1000			Off		+
Adapter #4 MAC: 00:0c:29:abe5:1e24 Speed: 0 Gb/s	/		1500			Off		+

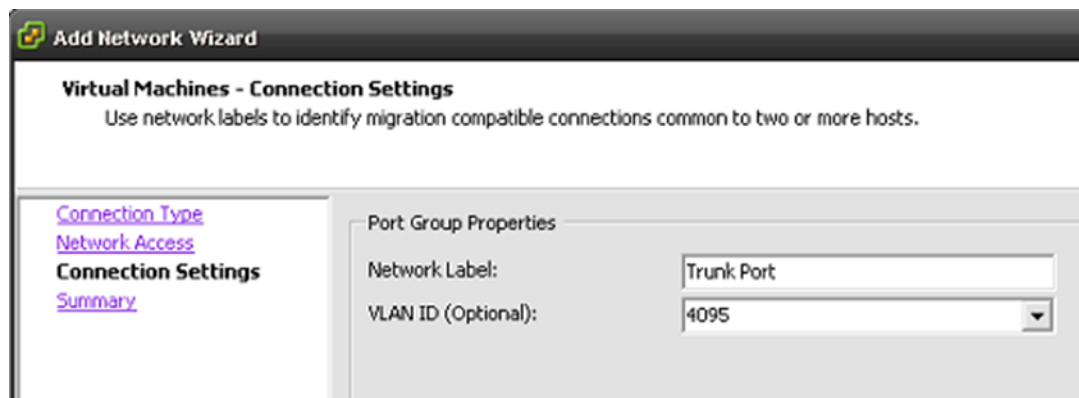
[Submit Network Changes](#)

Note: One or more adapters connected to the CGX Access appliance must be attached to a switch port configured as a trunk port.

Additional 802.1q configuration in VMware ESX / ESXi

In order for CGX Access virtual appliances to support the 802.1q, a port group that supports 802.1q VLAN tagging is needed. To configure it in your VMware virtual switch in ESX/ESXi, please follow the steps below:

1. Edit host networking
2. Navigate to Host → Configuration → Networking → vSwitch → Properties.
3. Click Ports → Portgroup → Edit.
4. Click the General tab.
5. Set the VLAN ID to All (4095) to trunked all VLANs.
6. Click OK



7. Assign the CGX-Access virtual appliance to use the Trunk Port created as in follows:



The physical network adapter would be required to connect to the trunk port on the physical networking switch.

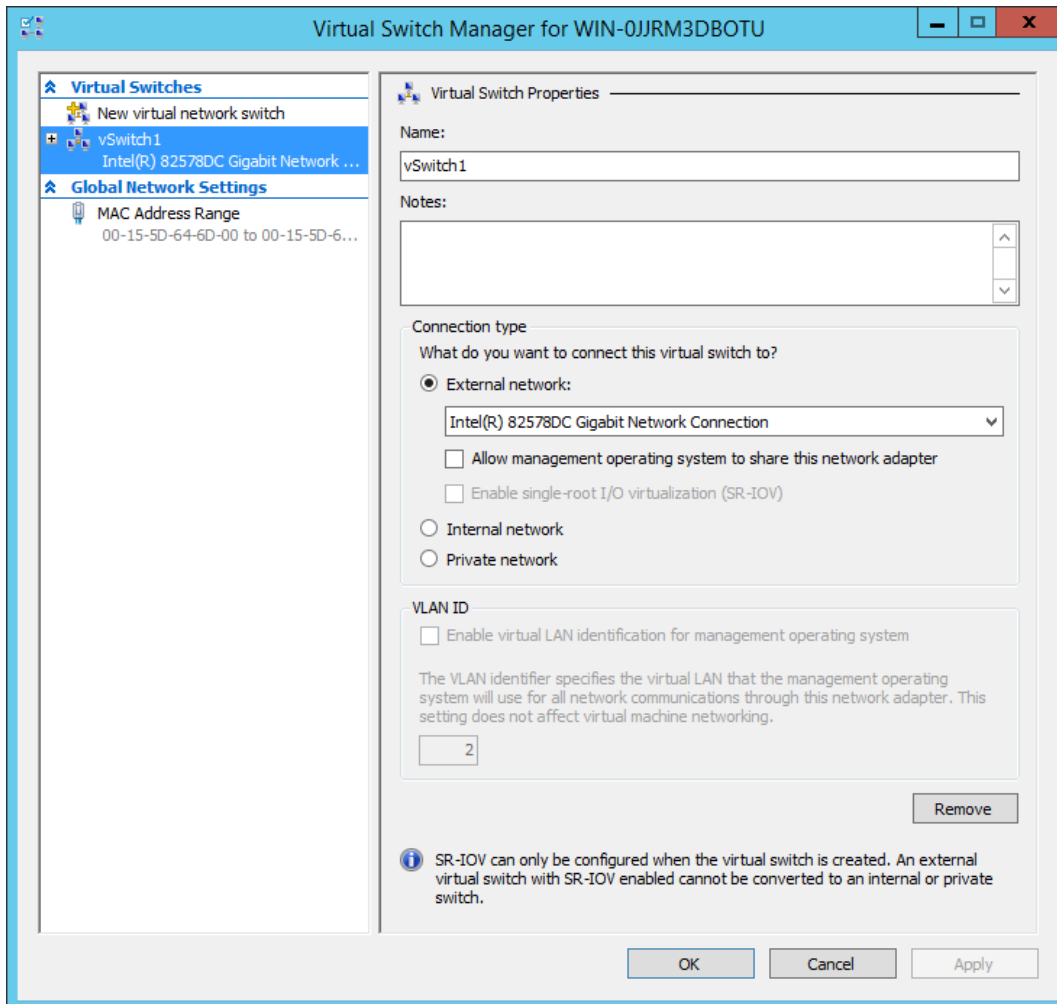
If your environment is using “Vmware Distributed switch”, you can add a “Distributed Port group” specifying a VLAN range (or complete VLAN range 0-4094). Assign this port group to the CGX-Access trunk port.



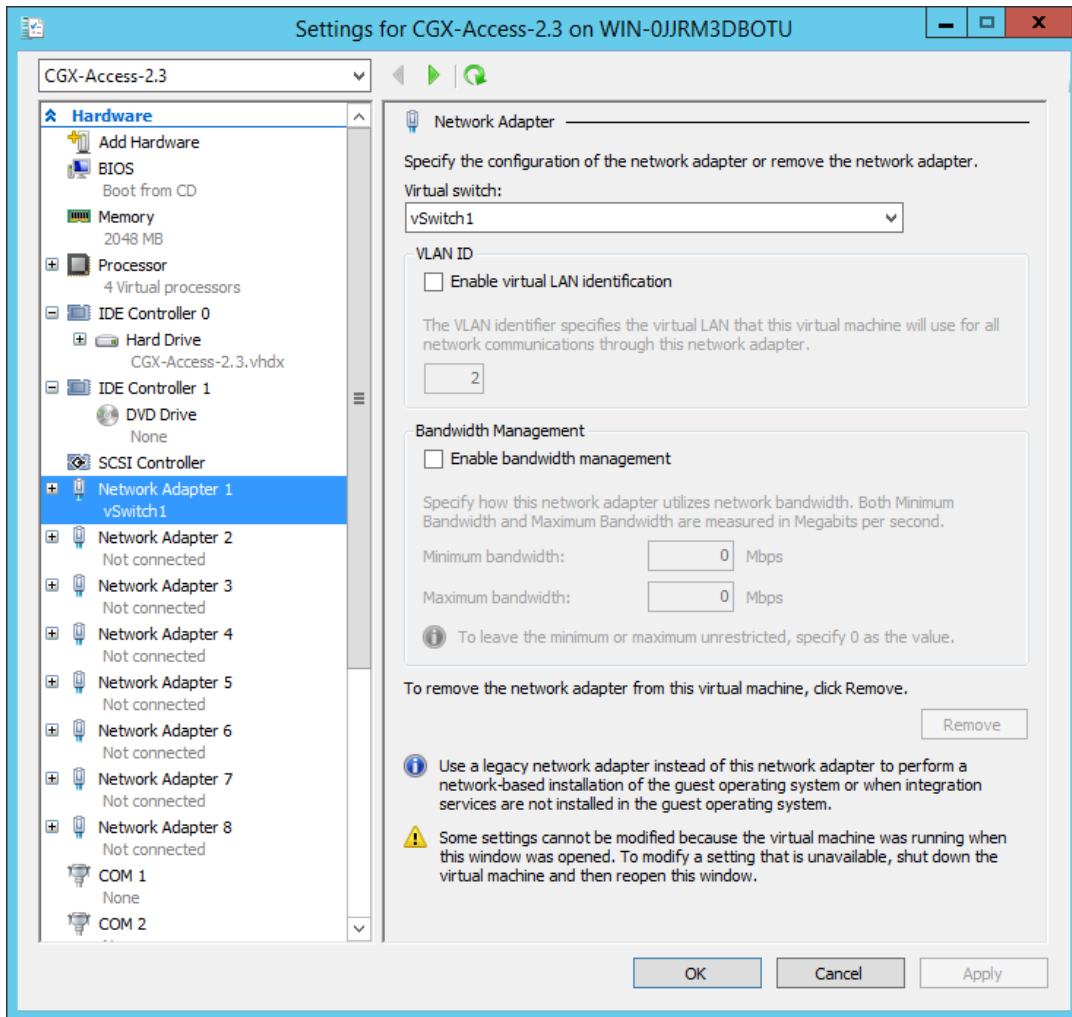
Additional 802.1q configuration in Hyper-V server

For CGX Access virtual appliances to support the 802.1q, Hyper-V's network adapters should be configured to tag frames. To enable trunking, some commands need to be entered from Windows PowerShell. The following screenshots show pre-requisite configuration.

- Hyper-V physical network adapter should support 802.1q tagging
- Switch port on which CGX Access trunk port is connected should support 802.1q tagging.
- From Virtual switch manager, configure virtual switch as “External Network”



- Select VM CGX-Access-3.0 (or vmname) and from right hand pane, click on settings. Assign virtual switch to the network adapter on CGX Access.



- Start Windows PowerShell and enter following command to configure “Network Adapter 1” as trunk port with allowed vlans 0,2,3,5,100 and Native Vlan as 0 (1 on cisco)

```
Set-VMNetworkAdaptervlan -VMName CGX-Access-3.0 -VMNetworkAdapterName "Network Adapter 1" -Trunk -AllowedVlanIdList "0,2,3,5,100" -NativeVlanId 0
```

- To verify enter following command.

```
Get-VMNetworkAdaptervlan -VMName CGX-Access-3.0
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Set-VMNetworkAdapterVlan -VMName CGX-Access-2.3 -VMNetworkAdapterName "Network Adapter 1" -Trunk -AllowedVlanIdList "0,2,3,5,100" -NativeVlanId 0
PS C:\Users\Administrator>
PS C:\Users\Administrator> get-vmnetworkadaptervlan -vmname CGX-Access-2.3

VMName      VMNetworkAdapterName Mode      VlanList
-----
CGX-Access-2.3 Network Adapter 1    Trunk    0,0,2-3,5,100
CGX-Access-2.3 Network Adapter 2    Untagged
CGX-Access-2.3 Network Adapter 3    Untagged
CGX-Access-2.3 Network Adapter 4    Untagged
CGX-Access-2.3 Network Adapter 5    Untagged
CGX-Access-2.3 Network Adapter 6    Untagged
CGX-Access-2.3 Network Adapter 7    Untagged
CGX-Access-2.3 Network Adapter 8    Untagged

PS C:\Users\Administrator>
```

Configuration required on Switch port. (cisco switch configuration used in example)

In this example, we will allow vlans 2,3,5,100 with native vlan 1 (Cisco vlan1 = HyperV-vlan0)

Switch#configure terminal

Switch(config)#interface fastEthernet 0/3

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

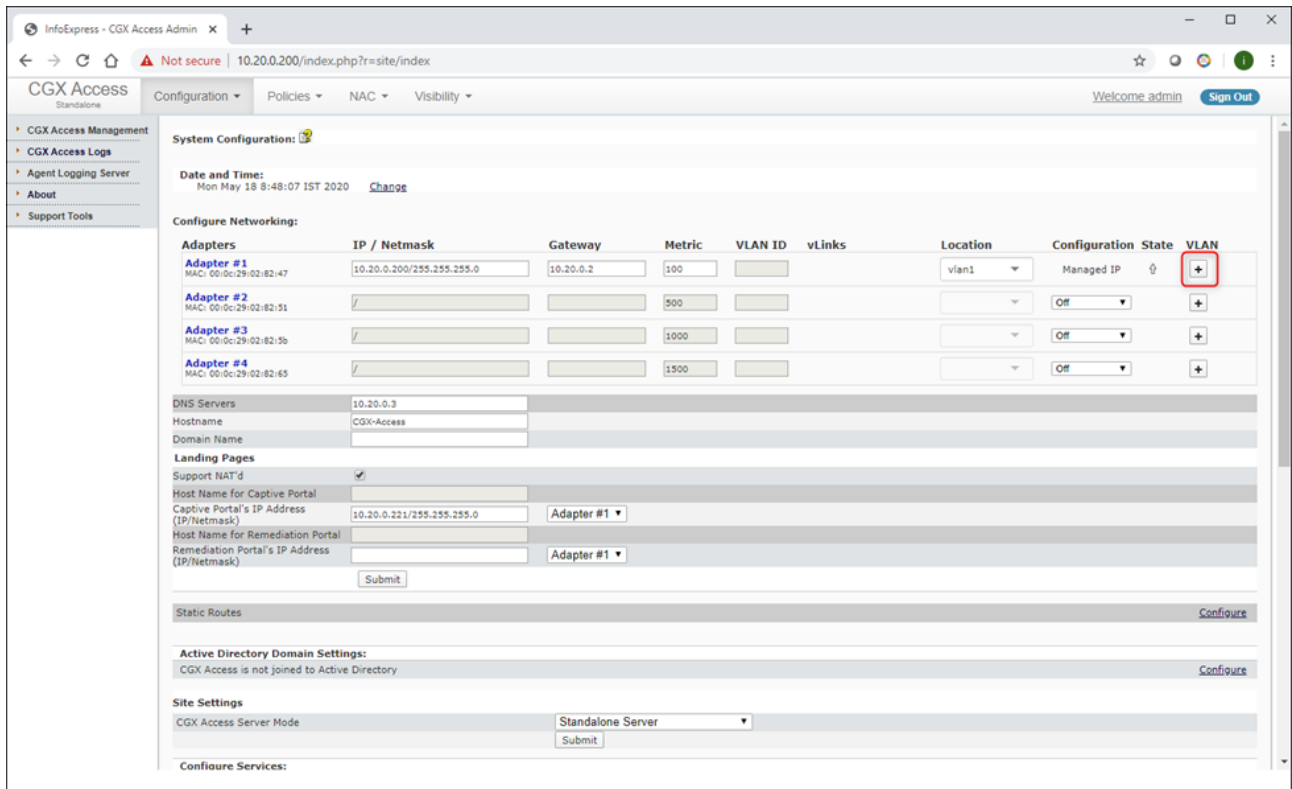
Switch(config-if)#switchport trunk allowed vlan 2,3,5,100

Switch(config-if)#switchport trunk native vlan 2 [in case you want a native vlan other than 1]

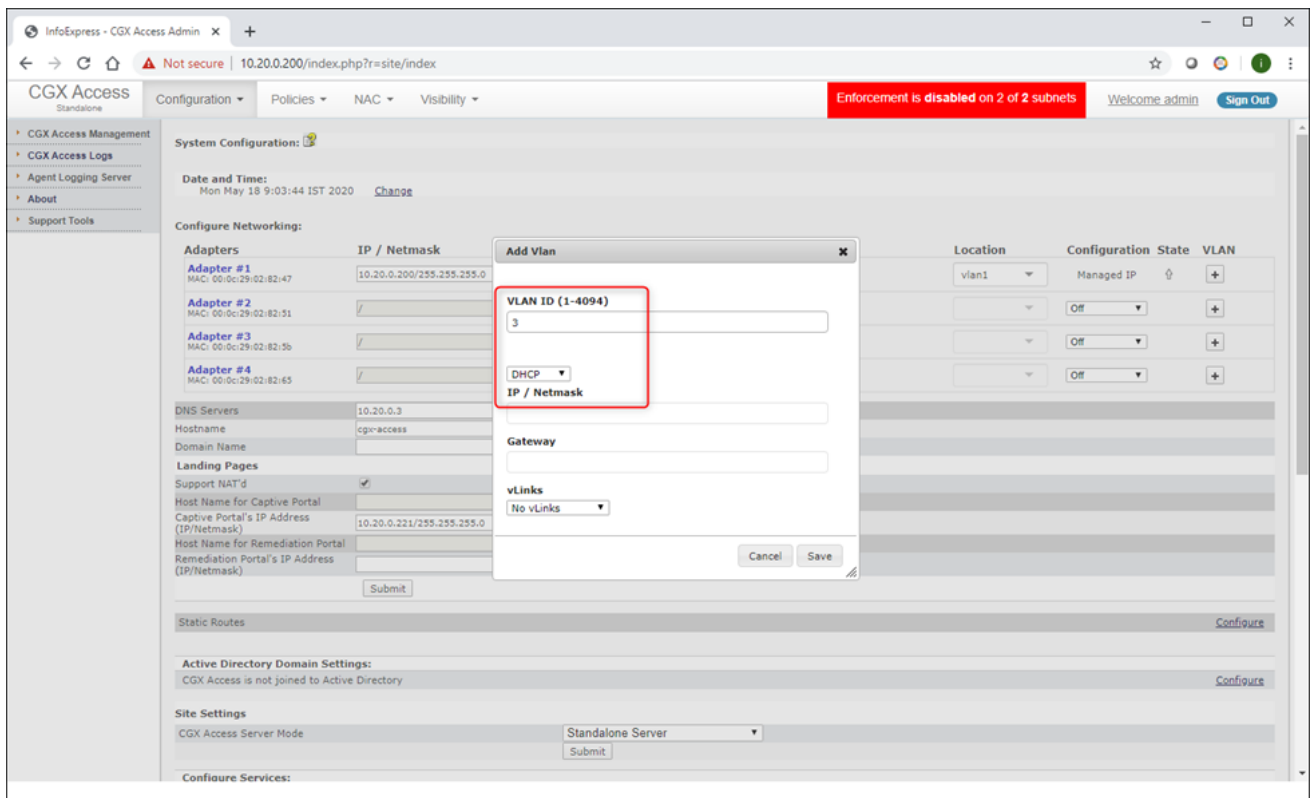
Switch(config-if)#exit

Configuring CGX Access Network adapters with VLANs

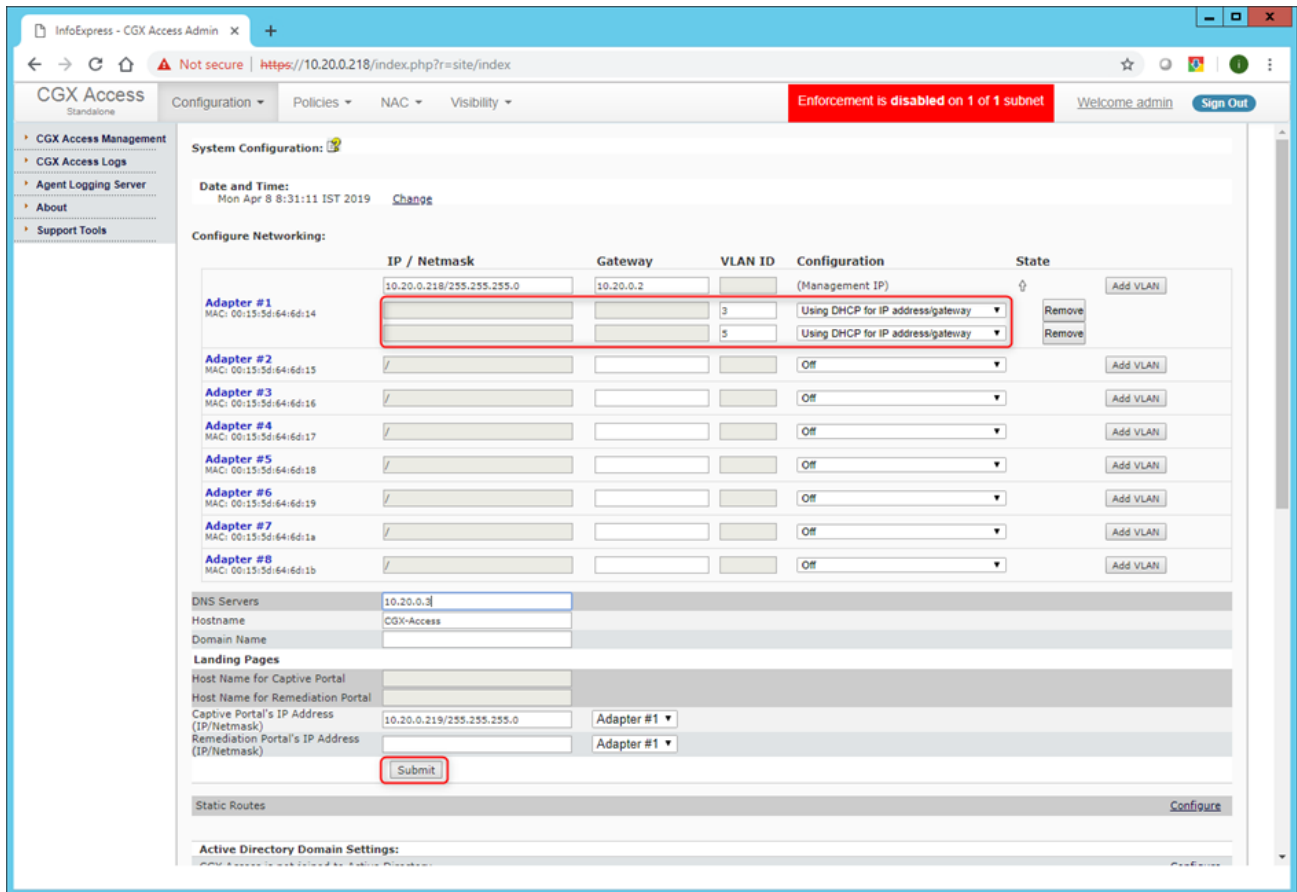
- Start CGX Access VM
- In CGX Access GUI go to Configuration → Appliance Settings
- Click “Add VLAN” button on the adapter attached to a trunk port



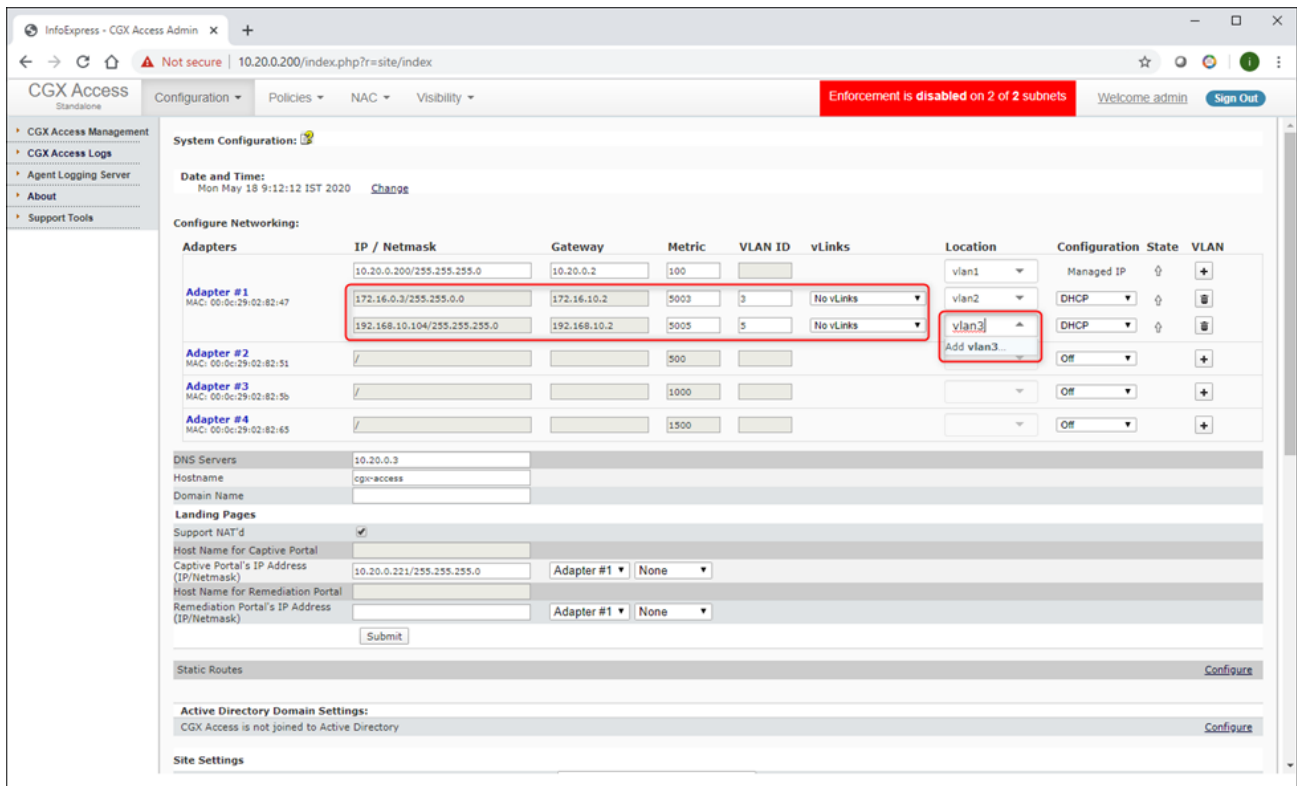
- Complete VLAN ID and IP address information. Static IP addresses or DHCP can be used.



- Repeat above step for adding more VLANs then click on submit



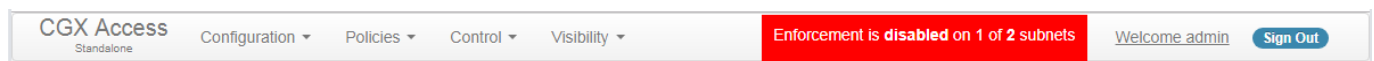
- If DHCP is configured, you should see IP address assignments to VLAN NICs



Enforcement Overview

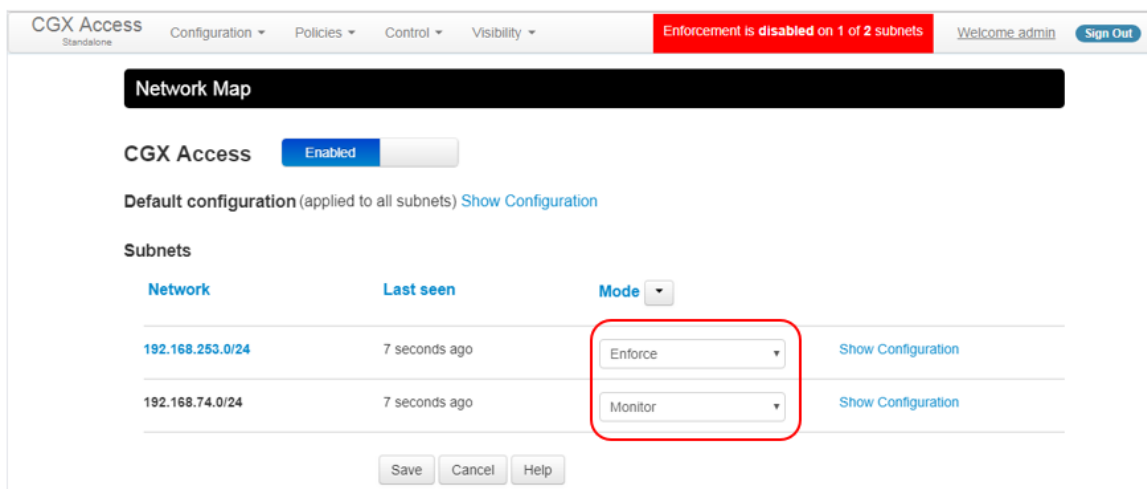
Easy NAC uses ARP enforcement to restrict access with landing page redirection. The use of ARP enforcement greatly simplifies the deployment of Network Access Control, as no network changes are required. ARP enforcement is also used to provide role-based control. To provide role-based control, CGX Access supports Access Groups (ACLs), such as: restricted, limited, full-access, guest-access, consultant, and byod-access, etc. Each Access Group (ACL) is configurable to allow for the role-based control to be customized.

By default, subnets are placed in monitoring mode. It is recommended that the basic setup be completed, ACLs fine-tuned, integrations enabled, and Allow-listing of devices be performed before enabling enforcement. When one or more subnets are in monitoring mode a status message is clearly visible across the top of the management console.



When ready, enforcement can be enabled in the Network Map. Enforcement can be delayed a few minutes when first enabled.

- Go to Control → Network Map



Note: VRRP and HSRP Redundancy

For CGX Access to function properly, it needs to know the MAC/IP of routers/gateways on the subnet. In case VRRP or HSRP is used, it is required that router's virtual and actual MAC addresses be configured in the "routerlist" under subnet configuration in "Network Map".

- Go to Control → Network Map
- Find the desired subnet and click on the “[Show Configuration](#)” link

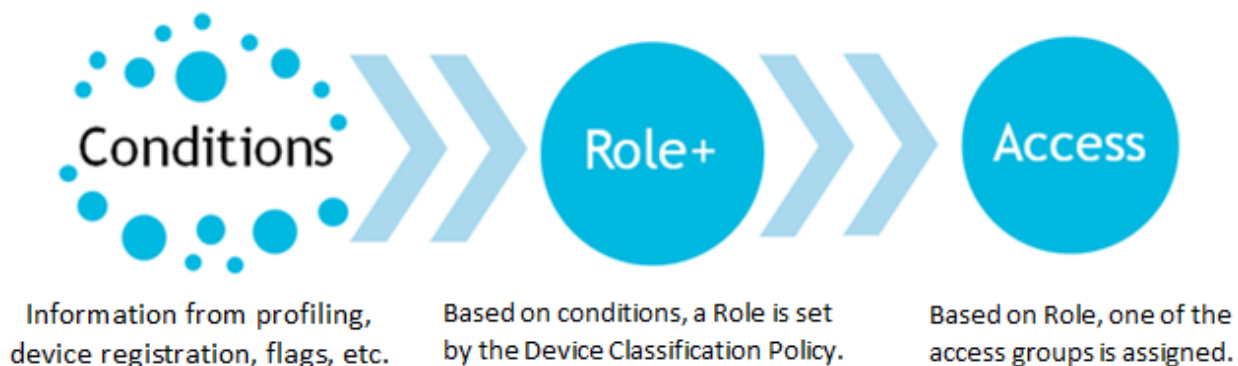
Configuring Access Policies

CGX Access includes default Access Groups (ACLs). Customized Access Groups (ACLs) can also be configured. The defaults are:

1. restricted (with redirection to captive portal)
2. full-access (complete access)
3. guest-access (default is internet only)
4. byod-access (full access by default, but can be changed to limit access to internal resources)
5. consultant (full access by default, but can be changed to limit access to internal resources)
6. limited (full access by default but can be changed. This access group is recommended for remediation purposes, but can be used for a variety of use-cases)
7. Restrict-Azure - Provides access to Microsoft while restricted to enable BYOD authentication using MS Azure credentials.
8. Restrict-Agent – Restricts a device failing an agent audit to remediation resources only
9. High-Risk – Restricts a device with redirection to remediation portal

Every device joining a protected subnet will be assigned an Access Group (ACL). Restricted access is the default for new and untrusted devices.

Access Groups are assigned in a two-step process where conditions are first evaluated in the Auto Trust Policy so a Role can be assigned. Second, Roles are then assigned one of Access Groups (ACLs), depending on time and location.



Auto Trust Policy

In CGX Access GUI:

- Go to Policies → Auto Trust

CGX Access has a set of preconfigured policies which will address typical requirements but can be modified to suit the enterprise's needs.

Auto Trust Policy

Activate

Cancel Changes

Add Rule







Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Deception Event - Honey Pot hit detected Has all of these tags: Deception-Event, Honeypot-hit	Set role to High-Risk-Event - Suspicious behavior detected Send message to: Admin via Email	  
Fingerprint Mismatch Has any of these tags: FP-mismatched	Set role to High-Risk-Event - Device failed fingerprint check	  
Malware Lateral Spread Risk - Scan Detected Has all of these tags: Dark-IP-scan, Scan-detected	Set role to High-Risk-Event - Excessive network scanning activity was detected	  
Orchestration Event Has any of these tags: SIEM-Event, IPS-Event, infected, FW-Event, APT-Event	Set role to High-Risk-Event - Malware or suspicious behavior has been detected	  
Passed Agent Audit Passed Agent Audit	Set role to full-access - Passed agent audit	  
Failed Agent Audit Failed Agent Audit	Set role to failed-agent-audit - Failed agent audit	  
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	  
Patch Non-Compliance (agent-less checks) Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant - Device is NOT compliant with the corporate patch management policy	  
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	  
Trusted IOT Device Has any of these tags: enforcer, network-infrastructure, printer, switch, VoIP	Set role to full-access - Assigned trusted IOT device tag	  
BYOD Registration Has any of these tags: byod	Set role to BYOD - Device registered with authorized credentials	  
Consultant Registration Has any of these tags: consultant	Set role to consultant - Device registered as consultant	  
Guest Registration Completed Guest or Device Registration	Set role to guest - Device registered by guest	  

Note: If none of the above conditions are met, a device will be assigned to the Untrusted Role

The conditions rules are evaluated top-down. The device role is assigned by the first rule with all matching conditions. If a rule has multiple conditions, all condition must match.

Rules can be arranged in the desired order by dragging rules up or down in the list as required. If a device does not match all the conditions in any rule, then the device will be assigned the Untrusted Role which is restricted by default.

Individual rules can be enabled or disabled with a click of a button. Disabled rules will not be evaluated.

Passed Agent Audit Passed Agent Audit	Set role to full-access - Passed agent audit	  
Failed Agent Audit Failed Agent Audit	Set role to failed-agent-audit - Failed agent audit	  

If changes are made, click the “Activate” button for the changes to take effect.

Activate

Roles & Access Policy

In CGX Access GUI:

- Go to Policies → Roles & Access

Easy NAC has a set of preconfigured Roles & Access policies which will address typical customer requirements but can be modified as necessary.

Roles & Access Policy

[New Role](#) Activate Cancel Changes

High-Risk-Event role: High-Risk during anytime from anywhere	
excluded role: excluded during anytime from anywhere	
restricted role: restricted during anytime from anywhere	
full-access role: full-access during anytime from anywhere	
untrusted role: restricted during anytime from anywhere	
guest role: guest-access during anytime from anywhere	<input type="checkbox"/>
BYOD role: byod-access during anytime from anywhere	<input type="checkbox"/>
consultant role: consultant during anytime from anywhere	<input type="checkbox"/>
non-compliant role: limited during anytime from anywhere	<input type="checkbox"/>
failed-agent-audit role: restrict-agent during anytime from anywhere	<input type="checkbox"/>

In the default Roles & Access policies above, notice how both restricted role and untrusted role would be assigned the restricted access group. For management and reporting purposes, it can sometimes be helpful to setup multiple roles even if these different roles get the same Access Group (ACL).

It is also possible to set time and locations when Access Groups (ACLs) would be assigned. One example of how this would be helpful is with guest access. It is possible to configure the guest role to only be assigned during office hours and from approved locations. Time and locations must be first be defined to use this feature. To define time and locations go to Policies → Time/Location/List

If changes are made, click the “Activate” button for the changes to take effect.



Access Group (ACLs)

Each of the access groups has a customizable ACL that is associated with it.

In CGX Access GUI:

- Go to Control → Access Control Lists

Access Groups (ACLs) Policy

Rules to enforce NAC access groups Activate Cancel Changes

[New Rule](#)

Access Group restricted	
Access Group full-access has complete access	
Access Group guest-access	
Access Group byod-access has complete access	
Access Group consultant has complete access	
Access Group limited	
Access Group restrict-Azure	
Access Group restrict-agent	

To make changes to any of the ACLs, click on the access group you would like to change, and edit the ACL in the dialog box.

Edit Action

Configure NAC rules for access group

Access group: restricted

Condition: Apply ACL

ACL rules:
ALLOW WHEN PROTO=='UDP' AND PORT==67
ALLOW WHEN PROTO=='TCP' AND PORT==67
ALLOW WHEN PROTO=='TCP' AND PORT==11698
DNSREDIRECT(CaptivePortal)
DENY WHEN TRUE

Color:

Save Cancel Help

The above restricted ACL allows DHCP traffic and NAC agent traffic on TCP port 11698. It will automatically redirect DNS traffic to the CGX Access captive portal. All other traffic is denied.

ACL Examples

1) ALLOW WHEN TRUE or ALLOWALL

Allows all the traffic.

2) DENY WHEN TRUE or DENYALL

Blocks all the traffic.

3) ALLOW WHEN PROTO=='TCP' AND PORT==80

Allows HTTP traffic to flow.

4) ALLOW WHEN PROTO=='TCP' AND PORT==11698

Allows NAC agent (TCP 11698) traffic to flow

5) ALLOW WHEN (PROTO=='TCP') AND PORT==80 AND ADDR=='192.168.100.200'

Allows HTTP traffic to the 192.168.100.200 IP Address.

6) ALLOW WHEN (PROTO=='UDP' OR PROTO=='TCP') AND PORT==21 AND ADDR=='192.168.0.0/24'

Allows FTP traffic to the 192.168.0.0/24 subnet.

7) HTTPREDIRECT <http://company.com> WHEN PROTO=='TCP' AND (PORT==80 OR PORT==443)

Redirects all the HTTP traffic to '<http://company.com>' URL.

8) HTTPREDIRECT(CaptivePortal)

The above is a special truncated syntax for HTTPREDIRECT rule which supports CGX landing pages automatically. This redirection URL will automatically use the CGX Access Captive Portal IP.

8) DNSREDIRECT(CaptivePortal)

The above is a special truncated syntax for DNSREDIRECT rule which supports CGX landing pages automatically. DNS-reply packets be modified to automatically use the CGX Access Captive Portal IP.

9) ALLOWSITE("microsoft.com")

This command allows both DNS replies and traffic to the Microsoft site. It should be placed above the DNSREDIRECT rule

10) ALLOWSUBSITE("microsoft.com")

This command allows both DNS replies and traffic to the Microsoft site and its subdomains. It should be placed above the DNSREDIRECT rule

11) DNSREPLACE(CaptivePortal)

This command is useful for environments without DNS servers. Will reply to DNS requests with the CGX Access Captive Portal IP.

12) ALLOW WHEN (PROTO=='TCP' OR PROTO=='UDP') AND LOCALPORT==3389

Allows RDP (mstsc) access on restricted endpoint. LOCALPORT is used to specify port on restricted device.

13) ALLOW WHEN PROTO=='TCP' AND LOCALPORT==3389 AND LOCALADDR=='192.168.10.20'

Allows Remote desktop to only one restricted endpoint *192.168.10.20* from all other protected end points

14) ALLOW WHEN PROTO=='TCP' AND LOCALPORT==3389 AND REMOTEADDR=='192.168.10.0/24'

Allow Remote desktop to restricted devices from subnet *192.168.10.0/24*

15) ALLOW WHEN PROTO=='TCP' AND (PORT==20 OR PORT==21) AND ADDR=='10.20.0.5'

Allow FTP from restricted devices to FTP server *10.20.0.5*

ACL Syntax

Each ACL rule has the following syntax:

<ACTION> WHEN <CONDITION>

<ACTION> can be one of the followings:

- ALLOW
Means the packet will be allowed to pass if <CONDITION> matches
- DENY
Means the packet will be blocked if <CONDITION> matches
- HTTPREDIRECT <url>
Means the packet will be modified with HTTP <url> redirection content inserted when <CONDITION> matches
- DNSREDIRECT <IP-address>
Means the DNS-reply packet be modified with <IP-address> if <CONDITION> matches
- DNSALLOW
Means the DNS-reply packet will be allowed to pass if <CONDITION> matches

<CONDITION> is a <SIMPLE-CONDITION>

or any combination of <SIMPLE-CONDITION> using parenthesis and AND|OR OPERATORS.

<SIMPLE-CONDITION> can be one of the followings:

- ETHTYPE <OPERATOR> <type>
Check for packet Ethernet type, <type> can be one of these strings: IP, ARP
- DIRECTION <OPERATOR> <direction>
Check for packet direction, <direction> can be one of these strings: IN, OUT
Packets can be captured in both directions:
IN direction means the packet flows from the protected to the rogue
OUT direction means the packet flows from the rogue to the protected

- **PROTO <OPERATOR> <proto>**
Check for IP protocol type. <proto> can be one of these strings: ICMP, TCP, UDP, IGMP
- **LOCALPORT <OPERATOR> <no>**
Check for TCP/UDP port against the number <no> in the case of IP/TCP/UDP packet.
This is always the port on restricted device.
- **REMOTEPORT <OPERATOR> <no>**
Check for TCP/UDP port against the number <no> in the case of IP/TCP/UDP packet.
This is the destination port for outgoing packet and source port for incoming packet.
- **PORT <OPERATOR> <no>**
Check for TCP/UDP port against the number <no> in the case of IP/TCP/UDP packet.
This is the destination port for outgoing packet and source port for incoming packet.
- **LOCALADDR <OPERATOR> <addr_or_subnet>**
Check for IPv4 address or subnet against string <addr_or_subnet>.
This is always the IP address of restricted device(s).
- **REMOTEADDR <OPERATOR> <addr_or_subnet>**
Check for IPv4 address or subnet against string <addr_or_subnet>.
This is the destination IP address for outgoing packet and source IP address for incoming packet
- **ADDR <OPERATOR> <addr_or_subnet>**
The same as REMOTEADDR
- **HOSTNAME <OPERATOR2> <site_name>**
Check if DNS hostname inside DNS-reply packet matches <site_name>
- **TRUE**
This condition is always true
- **FALSE**
This condition is always false

<OPERATOR> can be ==, != for strings and ==, !=, >, <, <=, >= for numbers.

Also, ! prefix-OPERATOR can be used to negate the [SIMPLE-CONDITION], like this:

!(PROTO=='TCP')

<addr_or_subnet> can contain IP-address range, like '192.168.0.1-192.168.0.100'

All strings should be quoted using single-quotes: 'example'

Tagging Devices and Allowlisting

In NAC deployments, it is a common requirement to grant access (Allowlist) specific devices that are not normally registered by end-users. Typical examples include printers, network infrastructure, VoIP phones and other types of devices.

An easy way to grant access is by using the concept of Tagging. The CGX Access solution supports the ability for administrators to create and set tags on specific devices. Then using Auto Trust Policy, devices with specific tags can be granted full-access, restricted or assigned some other access.

By default, devices with any of these tags: AD-Managed, AV-Managed, managed-device, patch-managed, XDR-managed, enforcer, network-infrastructure, printer router, switch, and VoIP, will automatically be granted full-access. This list can be modified to address unique requirements.

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕
Trusted IOT Device Has any of these tags: enforcer, network-infrastructure, printer, switch, VoIP	Set role to full-access - Assigned trusted IOT device tag	⊙ ↻ ✕

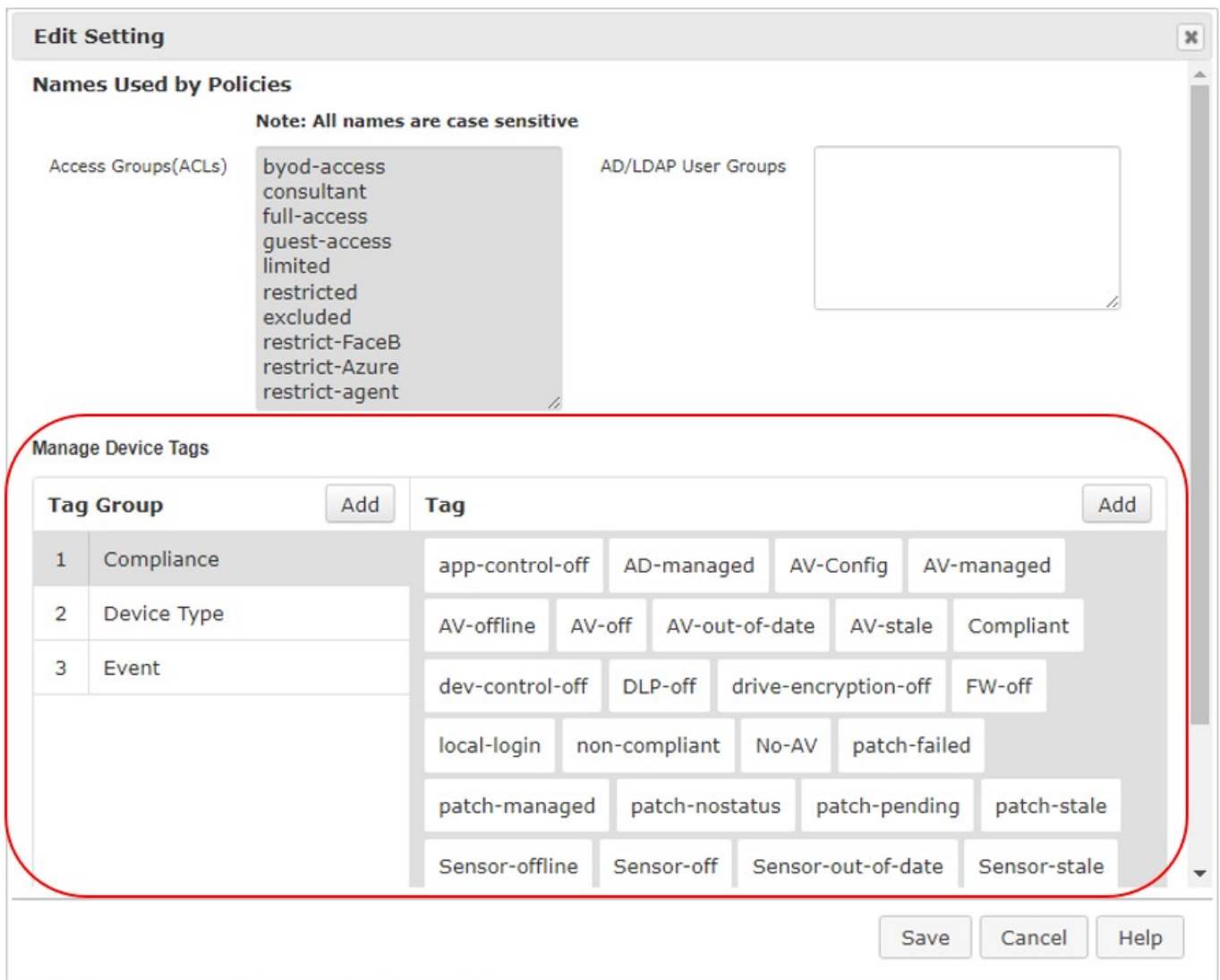
Note: The above policy order was changed for illustration purposes. Typically, these rules would be lower in priority, so non-compliant devices or high-risk devices can be assigned a restrictive role.

With the Device Profiler feature, CGX Access automates the process of tagging. The Easy NAC solution can automatically tag a device based on the results of device profiling. If CGX Access detects that a device is a printer, it will tag the device as a printer. If using the default Auto Trust Policy, the printer would then be granted full-access. The same is true for network infrastructure like routers.

Tags

CGX Access supports pre-defined tags and custom tags. Pre-defined tags are organized into three separate groups: Compliance, Device Type and Event. Customers can also add their own custom groups and custom tags.

- Go to Configuration → General Settings - Click on “Names Used by Policies”:



Tags can be leveraged to address many unique requirements. For example, if printers need to be physically checked before access is granted. Then a policy can be set to send an alert to the administrator when a device was automatically tagged as a printer shows up on the network. Once the printer has been verified, the administrator can then assign a custom tag, i.e., approved-printer, which would allow it access to the network.

Setting Tags

To manually assign tags to devices via the Device Manager.

- Go to Visibility → Device Manager

If the list of devices is long, show the Report Filters at the top of the screen to narrow down the results.

Setting the tags manually can be done for one or more devices in a few steps.

- 1. Select the device(s) where a tag is desired
- 2. Select an Action → Set tag and → Select Tag
- 3. Confirm tag is Permanent or select an expiration period
- 4. Click “Apply to selected devices”

The screenshot shows the 'Device Manager' interface with the following elements:

- Header:** 'Device Manager' and 'All Unique Devices Identified by CGX Access'. Navigation links: 'Back Refresh Export Help'. Updated at: 'Wed Dec 13 2023 09:57:22'.
- Filters:** 'Cover Devices Active in: Past 24 Hours' and 'Show Report Filter'.
- Form Elements:**
 - 'Set tag' dropdown menu (highlighted with a red box and '2').
 - 'Select Tag' dropdown menu (highlighted with a red box and '3') showing options: COMPLIANCE, DEVICE TYPE, byod, consultant, enforcer, full-access, guest.
 - 'Permanent' dropdown menu (highlighted with a red box and '3').
 - 'Apply to selected devices' button (highlighted with a red box and '4').
- Table:**
 - Total # of Devices: 2
 - Table with columns: MAC, Hostname, Acc Grc, Vendor, Tags / Lists, IP Address / IPv6, Last Seen, Comment, Access Status, Grant Access.
 - Row 1: MAC 00:50:56:87:9B:97, Hostname -----, Acc Grc full, Vendor Embedded, Tags network-infrastructure virtual routerlist, IP Address 10.160.0.1, Last Seen 2023-12-13 09:56:57, Comment -----, Access Status blue dot, Grant Access (ON, OFF, Auth, Fingerprint).
 - Row 2: MAC 00:50:56:05:F3:77, Hostname c6793554255, Acc Grc restricted untrusted demo, Vendor VMware, Inc., Tags virtual, IP Address 10.160.0.223, Last Seen 2023-12-13 09:47:45, Comment -----, Access Status red dot, Grant Access (ON, OFF, Auth, Fingerprint).

Allowlist \ Blocklist \ Excludelist \ Routerlist

CGX Access also supports adding a device(s) to a manual Allowlist, Blocklist or Exclude-list.

- Allowlist – Device will always have Full Access and be protected, regardless of policy.
- Blocklist – Device will always be Restricted, regardless of policy
- Excludelist – Device is ignored by EasyNAC. It will not be restricted or protected from rogue devices. Excluded devices do not consume a license.
- Routerlist – Default gateways will automatically have Full Access and be protected. For ARP enforcement to work as expected VRRP and HSRP routers would need to be add manually.

The examples below will assume Allowlist, but other lists will work the same way.

In the Network Map, devices can be added by MAC Address or IP Address to the Default configuration Allowlist or to an Allowlist specific to a subnet. If entered into the Default configuration, the Allowlist would be configured for all subnets. When adding devices to the Default configuration, it’s best to use MAC addresses, so it can be relevant to all subnets.

- Go to Control → Network Map → [Show Configuration](#)

Network Map

CGX Access

Enabled

Default configuration (applied to all subnets) [Hide Configuration](#)

Show timed-out subnets

Routerlist

Allowlist

Blocklist

Excludelist

Eg: 10.2.0.1
08:00:27:CA:AB:6E

The Network Map can also be used to configure IP addresses or MAC addresses that should only be Allowlisted on a specific subnet(s).

- Go to Control → Network Map
- Find the desired subnet and click on the “[Show Configuration](#)” link

Subnets

Network

Last seen

Mode

Action

192.168.253.0/24

18 seconds ago

Enforce

[Show Configuration](#)

Once the “[Show Configuration](#)” link has been clicked, the view will expand to show the Allowlist box specific to this subnet. Both IP Addresses and MAC Addresses can be added.

192.168.253.0/24

22 seconds ago

Enforce

[Hide Configuration](#)

Routerlist

Allowlist

Blocklist

Excludelist

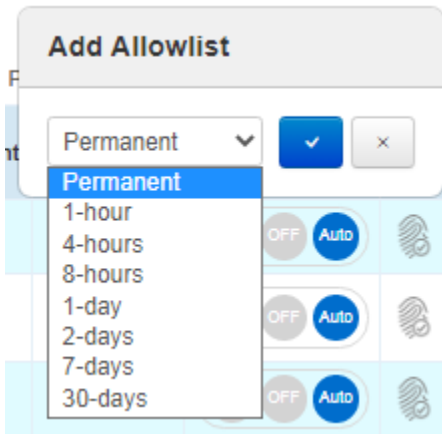
Eg: 10.2.0.1
08:00:27:CA:AB:6E

Adding Devices to the Allowlist or Blocklist

For quick additions to the Allowlist or Blocklist you can click the ON | OFF controls in the Device Manager. ON is the technical equivalent of being on the Allowlist, while OFF is the equivalent of being on the Blocklist. Auto means access is set automatically following the policies defined under Auto Trust Policy.



When you click the ON button you will be given the option to select an expiration period. Permanent is the default value.



When adding multiple devices to the Allowlist it can be convenient to add devices via the Device Manager.

- 1. Select the device(s) to be added to Allowlist
- 2. Select the action → Add to list → Select Allowlist
- 3. Confirm the list is Permanent or select an expiration period
- 4. Click “Apply to selected devices”

Device Manager

Back Refresh Export Help
Updated at Wed Dec 13 2023 11:20:32

Cover Devices Active in: Past 24 Hours

Show Report Filter

Add to list

allowlist

Permanent

Apply to selected devices

Total # of Devices: 4

1
Make it a Custom Report
Devices per Page 100 Page 1 of 1. First << [1] >> Last

MAC	Hostname	Access Group	Roles	OS	Vendor	Tags / Lists	IP Address / IPv6	Last Seen	Comment	Access Status	Grant Access
<input type="checkbox"/>	00:50:56:EF:68:25	full-access	full-access	VMware Player virtual NAT device	VMware	network-infrastructure virtual routerlist	192.168.253.2	2023-12-13 11:20:20	-----	●	ON OFF Auto
<input checked="" type="checkbox"/>	00:50:56:F0:9F:9F	restricted	untrusted	Unknown	VMware	virtual	192.168.253.254	2023-12-12 13:52:51	-----	●	ON OFF Auto
<input checked="" type="checkbox"/>	00:0C:29:4C:8C:B1	win-eh9kpk2tksh	restricted	Windows Server 2008 R2 Enterprise 7601 Service Pack 1	VMware	webserver virtual	192.168.253.100	2023-12-12 13:53:25	-----	●	ON OFF Auto
<input checked="" type="checkbox"/>	00:50:56:C0:00:08	laptop-jonathan	restricted	Windows 10	VMware	virtual	192.168.253.1	2023-12-12 13:53:55	-----	●	ON OFF Auto

Note: Devices that are in the Allowlist will be shown as ON. Devices in the Blocklist will be shown as OFF. Their respective list will also be shown in the Tags / Lists column.

The Excludelist

Devices added to the Exclude list will be completely unprotected by the Easy NAC solution. Its typical use would be for handling a compatibility issue. Issues are rare, but one known example is with the Cisco wireless AP. If the AP is not excluded, it would cause DHCP to fail.

The Exclude list feature can also be used for short-term license management. Devices added to the Excludelist do not consume a license, so if an organization is exceeding the license, this could be a short-term way to manage the issue. This feature should be used with care, as excluded devices will also not be protected from rogue, non-compliant or infected devices.

Note: If the device license is exceeded by more than 10%, new devices joining the network would be automatically added to this Excludelist and would therefore not be enforced or protected.

The Routerlist

The Routerlist is used to add non-default gateways to the settings. It commonly used if a customer is using VRRP or HSRP. With redundant gateways, it is required that router's virtual and actual MAC addresses be added in the "routerlist" for enforcement to work properly.

Device Discovery

Easy NAC use a combination of active and passive detection mechanisms to discover new endpoints when they join the network.

DHCP

When a new DHCP based endpoint connects to the network for example, it will send out a DHCP DISCOVER request. This broadcast packet will be seen by endpoints on the same subnet, including the CGX Access appliance. Once an IP address is assigned by your DHCP server, it will need to send out ARP requests on the network which is similar to the process described below in the static IP address devices.

Static IP

Statically addressed endpoints will send out layer-2 ARP requests, which are broadcast traffic, to locate endpoints and routers with whom they wish to communicate. CGX Access, being in the same broadcast domain, would be able to pick up the ARP request packets and immediately detect newly joined network devices. CGX Access will also periodically scan the network to detect systems that are stealthy connected to the network but without any DHCP nor ARP requests.

Device Profiling

Once CGX Access detects a new endpoint on the network, it will profile the device to determine which operation system (OS) it is running, and which network ports are open by using both active and passive profiling techniques. Active Profiling includes network scanning such as NMAP, UPnP, NBTScan which would detect an endpoint's OS, its open ports and grab the web server banner when it is detected on an endpoint.

Passive Profiling is accomplished by detecting the DHCP DISCOVER request broadcast packets and comparing them to the internal DHCP fingerprinting records to match up with the OS's unique identifier.

Note: Device Profiling information is also obtained from optional agents or integration modules such as Active Directory or End Point Protection software.

DHCP Profiling

DHCP Profiling is enabled by default, and CGX Access maintains an internal database for common end-user operating systems such as Windows, Mac OSX, iOS, Android, and Linux. For DHCP profiling of IOT devices, it's recommended to leverage Fingerbank, a cloud-based DHCP database of 35,000+ devices, which greatly enhances the accurate profiling of IOT devices.

Fingerbank

The Fingerbank Cloud API is operated by Inverse Inc., based in Canada. Easy NAC customers can leverage this cloud API for DHCP profiling of devices. Inverse allows companies to register for a free API license for up to 300 queries per hour. To register an account please visit:

<https://api.fingerbank.org/users/register>

To add this API to CGX-Access:

- Go to Configuration → General Settings
- Click on Device Profiler and select Fingerbank tab

Edit Setting

Device Profiler

NMAP scan | DHCP | **Fingerbank** | UPnP scan | Web scan | SNMP scan | NetBios | POF | LLTD | Mac -> Vendor

Fingerprint

Enable Fingerbank

API Key

Use the built-in DHCP profiling for typical end-user computing devices.
Recommended to maximize the free API license

Test Connection

- Paste the API key and Click the Test Connection
- If successful, click Save.

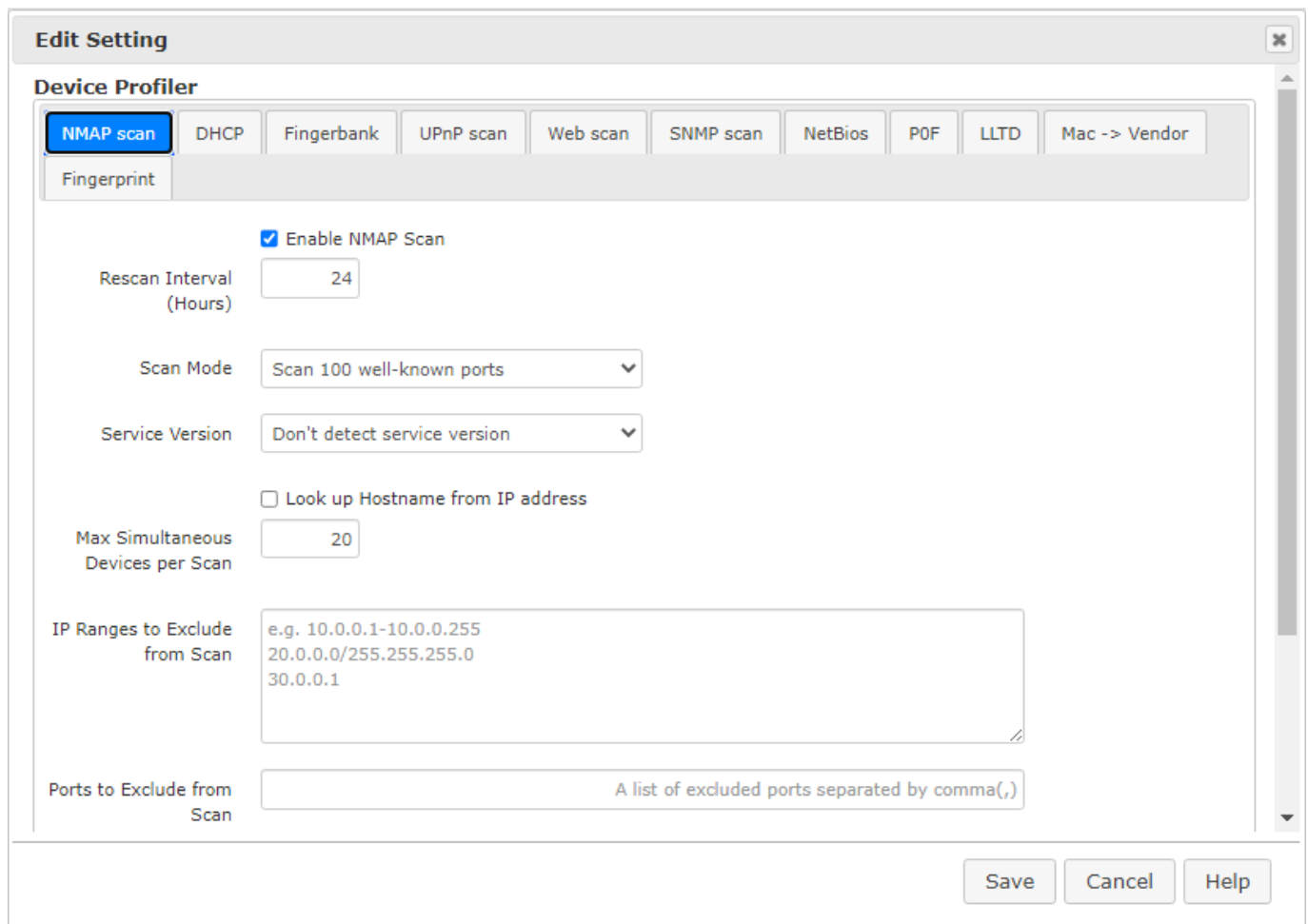
Note: It's recommended to use Easy NAC's built-in DHCP profiling for typical end-user computing devices. This would save the free API queries for IoT devices, where it's needed.

Note: Connection is made to api.fingerbank.org:443

NMAP Profiling

NMAP Profiling is enabled by default, and is used for both profiling of devices and detection of open ports. NMAP profiling is performed every 24 hours, which is the recommend frequency. NMAP scanning is optional and can be disabled. To review or make changes to the NMAP default settings:

- Go to Configuration → General Settings
- Click on Device Profiler and select NMAP scan



The screenshot shows the 'Edit Setting' window for the 'Device Profiler' section, specifically the 'NMAP scan' tab. The window has a title bar with 'Edit Setting' and a close button. Below the title bar, there are several tabs: 'NMAP scan' (selected), 'DHCP', 'Fingerbank', 'UPnP scan', 'Web scan', 'SNMP scan', 'NetBios', 'POF', 'LLTD', and 'Mac -> Vendor'. Under the 'NMAP scan' tab, there is a 'Fingerprint' sub-tab. The main configuration area includes:

- Enable NMAP Scan
- Rescan Interval (Hours): 24
- Scan Mode: Scan 100 well-known ports
- Service Version: Don't detect service version
- Look up Hostname from IP address
- Max Simultaneous Devices per Scan: 20
- IP Ranges to Exclude from Scan: e.g. 10.0.0.1-10.0.0.255, 20.0.0.0/255.255.255.0, 30.0.0.1
- Ports to Exclude from Scan: A list of excluded ports separated by comma(,)

At the bottom right, there are three buttons: 'Save', 'Cancel', and 'Help'.

Note: NMAP scan can be disabled entirely or on a subnet-by-subnet basis. To disable on specific subnet, go to:

- Go to Control → Network Map
- Find the desired subnet and click on the “[Show Configuration](#)” link

Network Map

CGX Access

Enabled

Default configuration (applied to all subnets) [Show Configuration](#)

Show timed-out subnets

Subnets

Network

Last seen

Mode

192.168.253.0/24

3 seconds ago

Enforce

[Hide Configuration](#)

Routerlist

Allowlist

Blocklist

Excludelist

192.168.253.2/00:50:56:EF:68:25 (auto-detected)

Eg: 10.2.0.1
08:00:27:CA:AB:6E
10.2.0.2/08:00:27:CA:AB:6F

Devices to protect in addition to routers

Allowlist

All devices with full access

Enable bidirectional capturing

Yes No

Disable NMAP Scanning

Yes No

Disable ARP Scanning

Yes No

- Select Yes on the “Disable NMAP Scanning”, and it will be disabled on this subnet only.

UPnP Profiling

UPnP Profiling is enabled by default, and can be a source of Operating System and hostname information from IoT devices enabled for UPnP. UPnP scanning is light weight and is performed every ~5 minutes. To review or make changes to the UPnP default settings:

- Go to Configuration → General Settings
- Click on Device Profiler and select UPnP scan

Edit Setting

Device Profiler

NMAP scan | DHCP | Fingerbank | **UPnP scan** | Web scan | SNMP scan | NetBios | POF | LLTD | Mac -> Vendor

Fingerprint

Enable UPnP Scan

Rescan Interval (Seconds)

Detect Device Description

Detect Device's Host Name

SNMP Scan

SNMP scanning is disabled by default. When enabled, SNMP would query the network devices for the switch and port a device is connected to. This information can then be used to enhance our ability to detect and prevent [MAC spoofing](#).

Supported Brands: Cisco, Aruba, Juniper, F5, HP, Palo Alto, SonicWALL, TP-Link, Fortinet, and VMware.

To enable and configure SNMP Scan settings:

- Go to Configuration → General Settings
- Click on Device Profiler and select SNMP scan

Edit Setting

Device Profiler

NMAP scan | DHCP | Fingerbank | UPnP scan | Web scan | **SNMP scan** | NetBios | POF | LLTD | Mac -> Vendor

Fingerprint

Enable SNMP Scan

Switches or Routers to scan

SNMPV2c RO Community Strings

SNMPV3 Username

SNMPV3 Security Level

Rescan Interval(secs)

Max concurrent scans

Use CDP/LLDP to discover other network devices

Detect the indirect and closest switch to an endpoint

SNMP Trap Port

SNMP Trap Community String

Configuring Device Profiler Policies

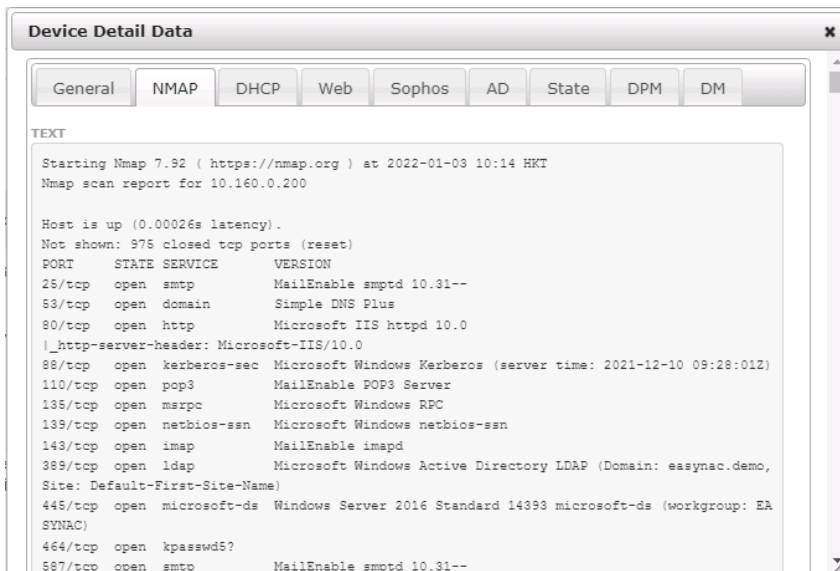
Easy NAC collects a lot of profiling information about devices. It can be helpful to use this information to create custom device profiling policies to automate the tagging of devices.

Device Detail Data

To review the information collected about a device:

- Open Device Manager
- Click on MAC address of the device

<input type="checkbox"/>	MAC	Hostname	Access Group	Roles	Location	OS	Vendor	Flags / Lists	IP Address	Last Seen	Comment	Access Status	Grant Access	
<input type="checkbox"/>	00:50:56:05:F3:77	c6793554255	restricted	untrusted	Cloud demo	Linux OS	VMware, Inc.	virtual	10.160.0.223	2022-01-03 10:19:27	-----	●	<input type="radio"/> ON <input type="radio"/> OFF <input type="radio"/> Auto	
<input type="checkbox"/>	00:50:56:0C:EA:32	c7543585455	full-access	full-access	Cloud demo	Windows Server 2016 Standard	VMware, Inc.	network-infrastructure webserver virtual AD-managed AV-managed whitelist	10.160.0.200	2022-01-03 10:19:27	AD Server	●	<input type="radio"/> ON <input type="radio"/> OFF <input type="radio"/> Auto	
<input type="checkbox"/>	00:50:56:87:9B:97		full-access	full-access	Cloud demo	Fortinet FortiGate 100D firewall	VMware, Inc.	network-infrastructure virtual routerlist	10.160.0.1	2022-01-03 10:19:27	-----	●	<input type="radio"/> ON <input type="radio"/> OFF <input type="radio"/> Auto	
<input type="checkbox"/>	00:50:56:AF:A3:D8	desktop-8fjp5su	limited	non-compliant	Cloud demo	Windows 10 Enterprise	VMware, Inc.	virtual AD-managed AV-managed AV-off	10.160.0.222	2022-01-03 10:19:27	AD Client	●	<input type="radio"/> ON <input type="radio"/> OFF <input type="radio"/> Auto	



Tip: The information contained in the Device Detail Data can be useful when creating custom Device Profiling Policies.

Device Profiling Policies

In CGX Access GUI:









- Go to Policies → Device Profiler

Device Profiling Policy

Mark devices based on profiling data

[Activate Policies](#) [Restore Policies](#)

Add Rule

Conditions	Actions	
Web data matches 'Apache or Microsoft-IIS'	Flag the device as 'webserver'	 
Device vendor matches 'Microsoft Hyper-V or VMWare'	Flag the device as 'virtual'	 
Device's NMAP scan data contains 'OS CPE.*laserjet'	Flag the device as 'printer'	 
Device type matches 'Switch or Router'	Flag the device as 'network-infrastructure'	 
Check if the port is open - Port: '5060', protocol: 'tcp'	Flag the device as 'VoIP'	 

CGX Access has a few of preconfigured Device Profiling Policies, these can be disabled or modified.

- Click Add Rule to create a custom profiling rule

Device Profiling Policy

[Back](#) [Activate Policies](#) [Restore Policies](#)

Conditions [Add](#)

Actions [Add](#)

- Click Add to create one or more Conditions

Create New Condition

Device [select an operation](#)

- Check Device Type
- Check Dhcp Data
- Device Flag
- Check Host Name
- Check MAC Address
- Check Vendor
- Check NMAP Scan
- Device OS
- Check Network Port
- Check Radius Data


[Cancel](#)

- Click Add to create one or more Actions

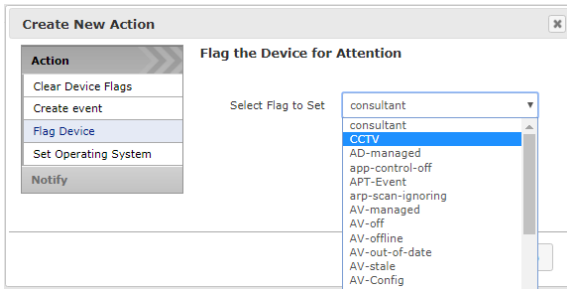
Device Profiling Policy

[Back](#) [Activate Policies](#) [Restore Policies](#)

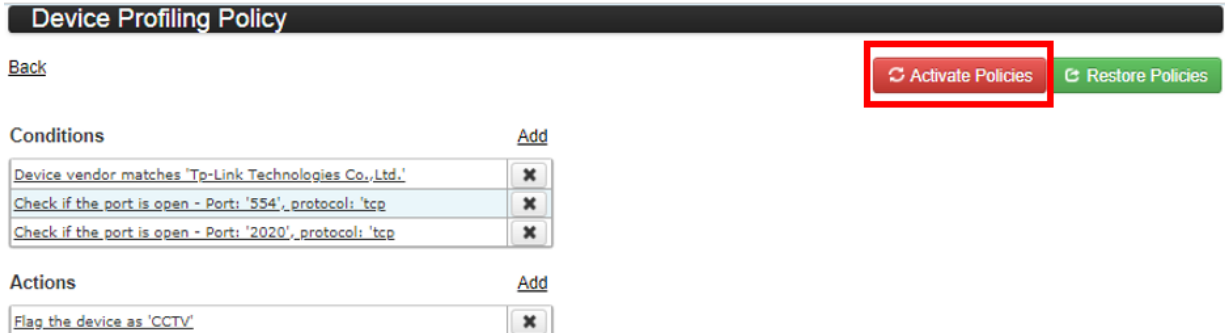
Conditions [Add](#)

Device vendor matches 'Tp-Link Technologies Co., Ltd.'	
Check if the port is open - Port: '554', protocol: 'tcp'	
Check if the port is open - Port: '2020', protocol: 'tcp'	

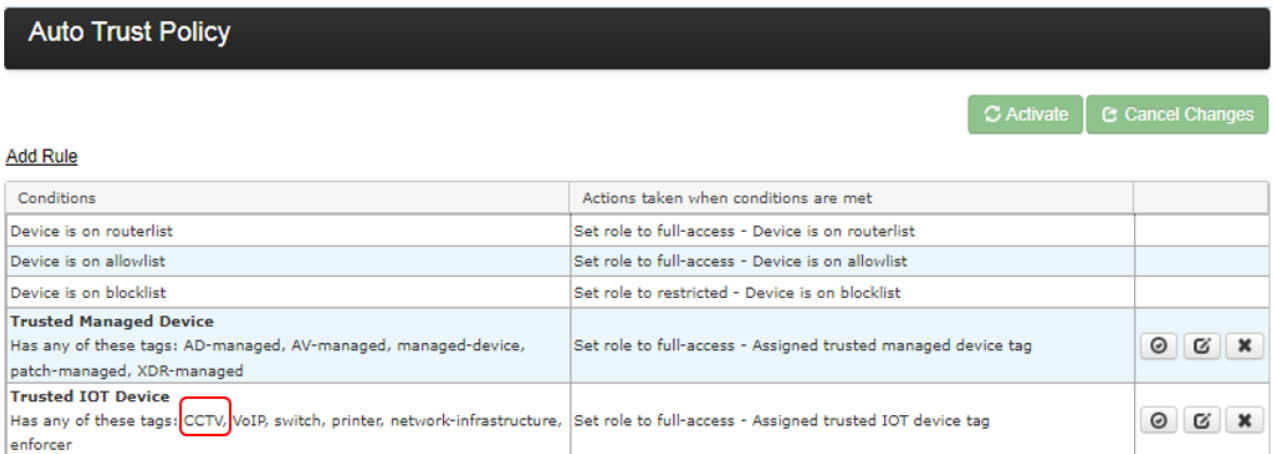
Actions [Add](#)



- Click “Activate Policies”



Devices matching the all three conditions will be Tagged as CCTV. Then adjusting the [Auto Trust Policy](#), these devices can be assigned full access to the network.



Note: The above policy order was changed for illustration purposes. Typically, these rules would be lower in priority, so non-compliant devices or high-risk devices can be assigned a restricted role.

Anti-spoofing Protection

Easy NAC provides a fingerprint feature to protect against MAC address spoofing. All devices on the network are automatically profiled for their MAC address, IP, DHCP or static assignment, Operating System, Hostname, and open ports). This information can then be used to set a unique fingerprint for the device. Once a fingerprint has been set, the device(s) will be protected from spoofing. For example, a printer can include the host name, IP address, open ports, and Embedded/IoT/Linux as its OS type. If a Windows or Apple device tries to spoof its MAC address, the spoof would be detected, and the device can be restricted.

Setting Fingerprints

Fingerprints can be set using the Device Manager

- 1. Select the device or devices where a fingerprint is desired
- 2. Select the Action → Set fingerprint
- 3. Click “Apply to selected devices”

The screenshot shows the 'Dashboard' section of the Easy NAC Device Manager. At the top, it says 'Devices Assigned full-access' and 'Updated at Sat Jan 01 2022 09:35:47'. Below this, there's a 'Cover Devices Active in:' dropdown set to 'Past 5 Minutes' and a 'Show Report Filter' link. A table of devices is displayed with columns: Roles, OS, Flags / Lists, IP Address, Last Seen, Comment, User, Location, Access Status, Grant Access, and an edit icon. A dropdown menu is open over the table, showing actions like 'Set flag', 'Clear flag', 'Add to list', etc. The 'Set fingerprint' option is highlighted with a red box and labeled '2'. The 'Apply to selected devices' button is also highlighted with a red box and labeled '3'. The first three rows of the table have their selection checkboxes highlighted with red boxes and labeled '1'. The first row in the table is: Roles: full-access, OS: Fortinet FortiGate 100D firewall, Flags / Lists: network-infrastructure virtual routerlist, IP Address: 10.160.0.1, Last Seen: 2022-01-01 09:35:42, Comment: -----, User: -----, Location: Cloud demo, Access Status: ON, Grant Access: ON, OFF, Auto, and an edit icon.

- 4. Confirm details to be included in the fingerprint → Save

The screenshot shows the 'Set device's fingerprint' dialog box. It has a title bar with a close button. Below the title, it says 'Check all the fields to be included in the fingerprint'. There are several sections: 'MAC Address' with a checked checkbox; 'IP Address' with an unchecked checkbox; 'OS' with a checked checkbox and a dropdown menu set to 'Embedded/IoT/Linux'; 'Hostname' with a checked checkbox; 'Ports' with 'Switch Port' unchecked and 'Open Port' checked, with a text input field containing 'tcp:22'; and 'Multi-Factor Authentication' with 'User Name' and 'Agent serial number' unchecked. At the bottom, there are 'Cancel' and 'Save' buttons. A red box labeled '4' highlights the 'OS' checkbox.

Note: To include Switch Port info in the fingerprint, SNMP scanning or the [RADIUS Proxy](#) feature needs to be configured.

Devices with set fingerprints will have a blue fingerprint icon displayed in the Device Manager. Clicking on the fingerprint will show the information included in its unique fingerprint.

MAC	Hostname	Roles	OS	Flags / Lists	IP Address	Last Seen	Comment	User	Location	Access Status	Grant Access	
00:50:56:87:85:70		full-access	Fortinet FortiGate 100D firewall	network-infrastructure virtual	10.160.0.1	2022-01-01 10:10:12	-----		Cloud demo			
00:50:56:0C:EA:32	c7543585455	full-access	Windows Server 2016 Standard	network-infrastructure webserver virtual AD-managed whitelist	10.160.0.200	2022-01-01 10:09:41	AD Server		Cloud demo			
00:50:56:AF:A3:D8	desktop-6fjp5su	full-access	Windows 10 Enterprise	virtual AD-managed	10.160.0.222	2022-01-01 10:09:41	AD Client		Cloud demo			
00:50:56:05:F3:77	c6793554255	full-access	Linux OS	virtual whitelist	10.160.0.223	2022-01-01 10:09:41	-----		Cloud demo			

Fingerprint Detail

- + OPENPORT : tcp:22
- + HOSTNAME : C6793554255
- + MAC : 00:50:56:05:F3:77
- + OS : linux,iot

Change Delete Close

Tip: The gray fingerprint icon can also be clicked to quickly set or change a fingerprint.

MAC Spoofing Detection

Once a fingerprint has been set, any changes in the fingerprint details will cause a mismatch and actions can be taken. In the example below, a Windows XP device had spoofed the MAC address of the printer. Since the Operating System and the hostname didn't match the fingerprint. The fingerprint icon was changed to red and device was assigned a FP- mismatched tag so actions can be taken.

MAC	Hostname	Access Group	Roles	Location	OS	Flags / Lists	IP Address	Last Seen	Access Status	Grant Access	
00:0C:29:4C:8C:B1	WIN-EH9KPK2TKSH	full-access	full-access		Windows Server 2008 R2 Enterprise 7001 Service Pack 1	network-infrastructure webserver virtual	192.168.253.100	2018-01-14 21:23:36	●		
38:59:F9:6F:AC:37	Sales-Mike	restricted	restricted		Microsoft Windows XP	printer FP-mismatched	192.168....		●		
00:0C:29:4B:70:2E	MANAGED01	full-access	full-access		Windows 7 Professional	virtual AD-managed	192.168....		●		
00:0C:29:51:DB:AA	SALES-MIKE	restricted	untrusted		Windows XP	virtual	192.168....		●		
C0:25:E9:03:7E:B0		full-access	full-access		Linux 2.6.23 - 2.6.38	network-infrastructure webserver	192.168....		●		

Fingerprint Detail

- + OS : others
- + MAC : 38:59:F9:6F:AC:37
- + HOSTNAME : BRW3859F96FAC37

Mismatched values:

- + OS : windows,winxp
- + HOSTNAME : Sales-Mike

Change Delete Close

IP Spoofing Detection

The fingerprint can also set and monitor the IP address allocation of the endpoints. Options include checks for: 1) Static IP 2) DHCP assigned IP address or 3) DHCP assigned IP in a specific subnet scope. Device changing how their IP address is assigned will be tagged as a FP-mismatched.

Set device's fingerprint

Check all the fields to be included in the fingerprint

MAC Address (default)

IP Address(es)

Operating System

In the example below, the device's fingerprint was set for a DHCP assigned address in the 10.160.0.0/24 subnet. When it's IP changed to a static IP address, even in the same subnet, it was tagged FP-mismatched.

The screenshot shows the 'Dashboard' for 'Devices Assigned High-Risk'. A 'Fingerprint Detail' window is open, displaying the following information:

- + HOSTNAME : DESKTOP-6FJP5SU
- + MAC : 00:50:56:AF:A3:D8
- + IP : dhcp-subnet 10.160.0.0/24
- + OS : windows
- Mismatched values:**
- + IP : 10.160.0.88

The main table below shows the device details:

MAC	Hostname	Roles	Location	OS	Last Seen	Comment	First Seen	Vendor
00:50:56:AF:A3:D8	desktop-6fjp5su	High-Risk-Event	Cloud demo	Windows 10 Enterprise 6.3 Build 19045 Service Pack None	2023-12-13 18:42:27	AD Joined Client	2022-04-23 12:28:55	VMware, Inc.

At the bottom right of the device row, there are two IP addresses: 10.160.0.88 and 10.160.0.222. The first IP is circled in red, and a fingerprint icon is also circled in red, indicating a mismatch.

Using Policies → Auto Trust rules, actions can be taken when a FP-mismatched is detected. The policy below shows the device will be assigned the High-Risk-Event role and alerts will be sent to the network administrator via e-mail and Teams.

Auto Trust Policy

Activate
Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met
Device is on routerlist	Set role to full-access - Device is on routerlist
Device is on allowlist	Set role to full-access - Device is on allowlist
Device is on blocklist	Set role to restricted - Device is on blocklist
Fingerprint Mismatch Failed Fingerprint Check	Set role to High-Risk-Event - Device failed fingerprint check Send message to: EasyNAC Admin via Email, Microsoft Teams

Fingerprint Rescan Interval

Some device profiling features, like NMAP scanning are run with a default 24-hour frequency. For faster fingerprint mismatch detection, a faster rescan interval can be set. It's recommended to only increase the rescan interval for devices with Fingerprints.

In CGX Access GUI:

- Go to Configuration → General Settings → Device Profiler
- Select Fingerprint tab

Edit Setting

Device Profiler

NMAP scan
 DHCP
 Fingerbank
 UPnP scan
 Web scan
 SNMP scan
 NetBios
 POF
 LLTD
 Mac -> Vendor

Fingerprint

Enable Rescanning Devices with Fingerprint

Rescan Interval(secs)

Multi-Factor Authentication

The Fingerprinting feature can also provide 2FA (Something you know (password) and something you have a (specific device). User credentials will be captured with the use of agents, WMI or 802.1x, and then associated with a specific device.

Set device's fingerprint

Check all the fields to be included in the fingerprint

MAC Address
 IP Address
 OS
 Hostname

Ports

Switch Port
 Open Port

Multi-Factor Authentication

User Name
 Agent serial number

Windows

easynacbobby
easynaccharles

Cancel Save

- Click “User Name” and then select the from a list of available accounts. Up to 5 accounts can be included in a Fingerprint.
- If using agents, click “Agent Serial number”; If it can’t be selected then the device doesn’t have and agent installed.
- Save Changes to Fingerprint

Note: If you are unable to select “User Name” then no user names have been detected for this device. User names are sourced from the use of Agents, WMI, or 802.1x authentication when using the Radius Proxy feature.

Mismatched Authentication

Once a fingerprint has been set, any changes in the fingerprint details will cause a mismatch and actions can be taken. In the example below, Bobby was the authorized Username, but the account Charles was logged into device. Since there was an authentication mismatch, the fingerprint icon was changed to red and device was assigned a FP- mismatched tag so actions can be taken.

<input type="checkbox"/>	MAC	Hostname	Access Group	Roles	Location	OS	Vendor	Flags / Lists	IP Address	Last Seen	Comment	Access Status	Grant Access	
<input type="checkbox"/>	00:50:56:AF:A3:D8	desktop-6fjp5su	restricted	restricted	Cloud demo	WinX64 10 Enterprise 6.3 Build 19043 Service Pack None	VMware, Inc.	virtual AD-managed FP-mismatched	10.160.0.222	2022-01-01 14:23:57	AD Client	●	<input type="button" value="ON"/> <input type="button" value="OFF"/> <input type="button" value="Auto"/>	
<input type="checkbox"/>	00:50:56:05:F3:77	c6793554255	full-access	full-access	Cloud demo	Linux OS	VMware, Inc.	virtual whitelist	10.160.0.223	2022-14-23			<input type="button" value="Change"/>	
<input type="checkbox"/>	00:50:56:87:85:70		full-access	full-access	Cloud demo	Fortinet FortiGate 100D firewall	VMware, Inc.	network-infrastructure virtual routerlist	10.160.0.1	2022-14-23			<input type="button" value="Change"/>	
<input type="checkbox"/>	00:50:56:0C:EA:32	c7543585455	full-access	full-access	Cloud demo	Windows Server 2016 Standard	VMware, Inc.	network-infrastructure webserver virtual AD-managed whitelist	10.160.0.200	2022-14-23			<input type="button" value="Change"/>	

Fingerprint Detail

+ USERNAME : easynac\bobby
 + AGENTSERIAL : 253519870731101
 + HOSTNAME : DESKTOP-6FJP5SU
 + MAC : 00:50:56:AF:A3:D8
 + OS : windows

Mismatched values:
 + USERNAME : EASYNAC\charles

If both Bobby and Charles are authorized users, the change button could be clicked, and both usernames could be added to the fingerprint.

Change device's fingerprint

Check all the fields to be included in the fingerprint

MAC Address
 IP Address
 OS Windows
 Hostname

Ports

Switch Port
 Open Port

Multi-Factor Authentication

User Name easynac\bobby easynac\charles
 Agent serial number

Rogue DHCP Server Detection

With personal Wi-Fi routers and misconfigured virtual machines, it is not uncommon for rogue DHCP servers to show up on the network. CGX Access can be configured to detect rogue DHCP servers, so they can be quickly identified and removed from the network.

- Go to Configuration → General Settings.
- Click on “Other Servers”
- Under DHCP Servers, input the IP addresses of all the authorized DHCP servers on the network.
- Select “Detect Rogue DHCP Servers”

Edit Setting
✕

RADIUS Server

Radius Clients

DHCP Servers

Web Proxy Server

SMS Gateway

WhatsApp Provider

Slack App

Teams App

Detect Rogue DHCP Servers

IP Addresses of Authorized DHCP Servers

192.168.253.100
 192.168.253.101

Note: Any DHCP server not on the authorized IP list will be tagged as DHCP-rogue.

Using Policies → Auto Trust Policy, actions can be taken when DHCP-rogue is detected. The policy below shows the device will be assigned a restricted role and alerts will be sent to the network administrators.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Rogue DHCP Server Has any of these tags: DHCP-rogue	Set role to High-Risk-Event - Device acting as DHCP server Send message to: EasyNAC Admin via Email Send message to Syslog	⊙ ↗ ✕

Time \ Location \ List Policies

It can be useful to use time, location or lists of IP addresses to help determine what access should be granted. For example, the default settings will allow guests to access the internet at any time, and from any part of the network. If we wanted to limit where and when they can access the internet, we can use the Location and Time Policies.

Location Policy

Option 1: Location names can be set by adapter or VLAN under Configuration → Appliance settings

Networking:

Adapters	IP / Netmask	Gateway	Metric	VLAN ID	Location	Configuration	State	VLAN
Adapter #1 MAC: 00:0c:29:ab:a5:06 Speed: 1 Gb/s	192.168.253.220/255.255.255.0	192.168.253.2	100			Managed IP	0	+
Adapter #2 MAC: 00:0c:29:ab:a5:10 Speed: 0 Gb/s	10.160.0.220/255.255.255.0	10.160.0.1	300		HQ-IT-Dept	Static IP		+
Adapter #3 MAC: 00:0c:29:ab:a5:1a Speed: 0 Gb/s	/		1000			Off		+
Adapter #4 MAC: 00:0c:29:ab:a5:24 Speed: 0 Gb/s	/		1500			Off		+

Submit Network Changes

Option 2: Define location names by IP range.

- Go to Policies → Time/Location/List and click on Location-policy.

Edit Action

Set Device's Location

Location name: Guest WiFi

Device's IP within these ranges: 192.168.254.1-192.168.254.254

One per line (e.g. 192.168.39.1 - 192.168.39.255)

Location definitions can be based on IP address ranges. Once the Location name has been saved, it can now be added as a condition for Guest Access in the Roles & Access policy.

- Go to Policies → Roles & Access

The above Roles & Access policy now has two possible Access Groups for for guests. If on the Guest WIFI access is granted, if at any other location, access is restricted. If we wanted to limited access to office hours, we could set a third condition based on time.

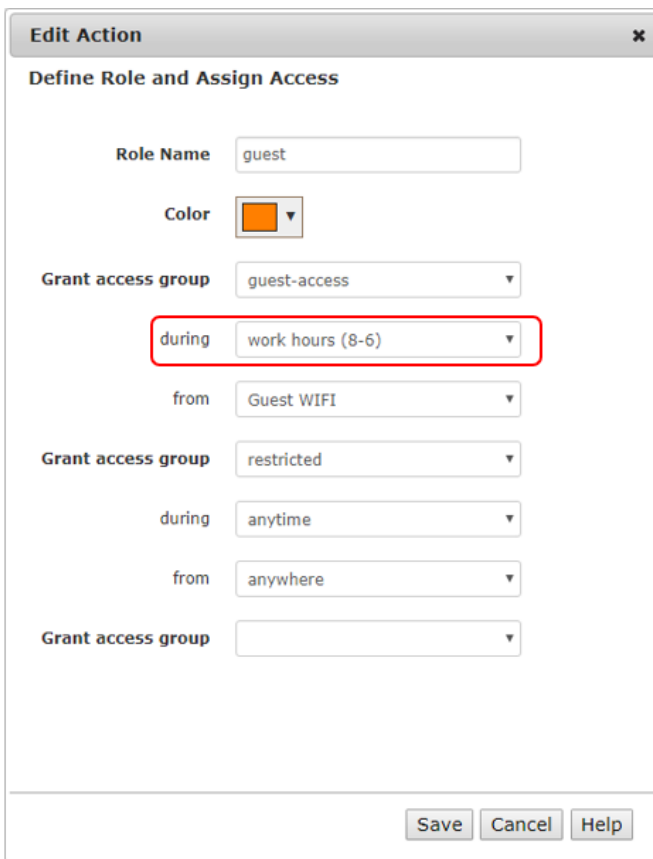
Time Policy

- Go to Policies → Time/Location/List and click on Time-policy.

Time definitions can be adjusted, or new ones created. Below is an example of how work hours might be defined:

Once the Time Period name has been saved, it can now be added as a condition in the Role & Access policy.

- Go to Policies → Roles & Access



The screenshot shows a dialog box titled "Edit Action" with a close button (X). Below the title is the section "Define Role and Assign Access". The form contains several fields:

- Role Name:** A text input field containing "guest".
- Color:** A color selection dropdown menu showing an orange square.
- Grant access group:** A dropdown menu with "guest-access" selected.
- during:** A dropdown menu with "work hours (8-6)" selected. This field is highlighted with a red rectangular border.
- from:** A dropdown menu with "Guest WIFI" selected.
- Grant access group:** A dropdown menu with "restricted" selected.
- during:** A dropdown menu with "anytime" selected.
- from:** A dropdown menu with "anywhere" selected.
- Grant access group:** An empty dropdown menu.

At the bottom of the dialog are three buttons: "Save", "Cancel", and "Help".

The above Role & Access policy now has both time and location conditions for guest access to be granted.

Device-Lists Policy

Device-Lists Policies provides an easy method to define a list of IP addresses or MAC addresses to help determine what access should be granted. It is commonly used to define a group of IP address that needs to be Allowlisted.

- Go to Policies → Time/Location/List and click on Device-lists.

Device Lists can be adjusted, or new ones created. Below is an example of how to create a device list for a server farm using IP addresses:

Create New Action
✕

Define IP Address List

Define IP Address List

Define MAC Address List

List name

Server Farm

IP addresses or ranges

10.0.0.100-10.0.0.150
 10.0.0.200-10.0.0.250

e.g. 10.0.0.1, 10.0.0.1-10.0.0.255

Save

Cancel

Help

Once the Device-List has been saved, it can now be added as a condition in the Auto Trust Policy.

- Go to Policies → Auto Trust

Auto Trust Policy

↻ Activate

↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Server Farm Device is on Server Farm	Set role to full-access - Server segment	<div style="display: flex; gap: 5px;"> ⊙ ↻ ✕ </div>

The above Auto Trust policy will assign the Server Farm to have full-access.

Configuring Guest Access

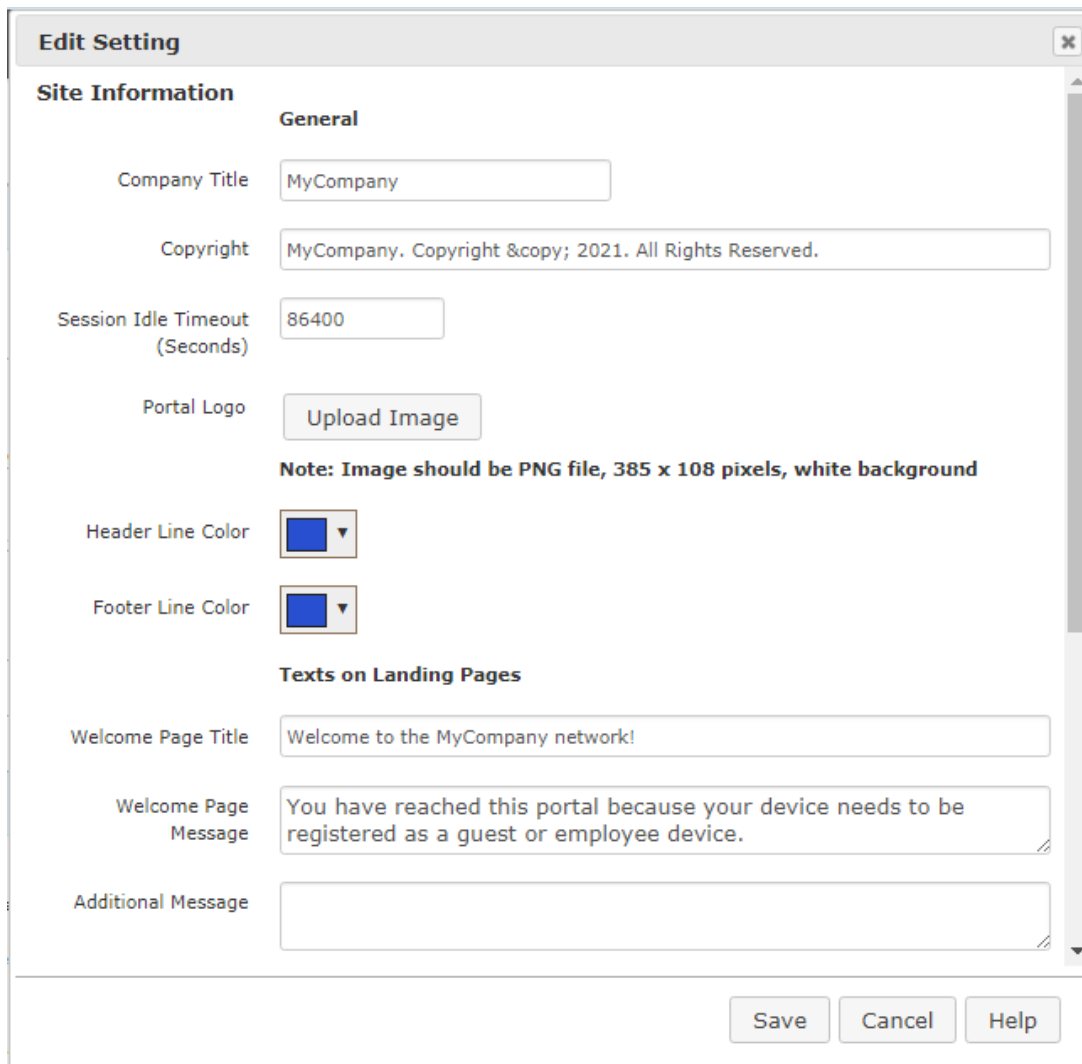
CGX Access supports multiple login methods for guest registration. Typical options include self-service registration, sponsor registration, or self-service registration with sponsor approval. CGX Access can support all these methods simultaneous, so different registration processes can be used for different use cases. Guest Access is a standard feature that is enabled by default, but a few steps are recommended to customize or enhance the guest experience.

Customize Captive Portal

Go to Configuration → General Settings and click on “Site Information”

- Adjust the Company Title, Welcome Page Title, and any other details as desired.
- Upload a corporate image* and adjust the header and footer colors

***Note:** Image must be PNG file and be 385 x 108 pixels. MS paint can be used to create.



The screenshot shows a window titled "Edit Setting" with a close button (X) in the top right corner. The window is divided into two main sections: "Site Information" and "Texts on Landing Pages".

Site Information

General

- Company Title: MyCompany
- Copyright: MyCompany. Copyright © 2021. All Rights Reserved.
- Session Idle Timeout (Seconds): 86400
- Portal Logo: Upload Image

Note: Image should be PNG file, 385 x 108 pixels, white background

- Header Line Color: Blue
- Footer Line Color: Blue

Texts on Landing Pages

- Welcome Page Title: Welcome to the MyCompany network!
- Welcome Page Message: You have reached this portal because your device needs to be registered as a guest or employee device.
- Additional Message: (Empty text area)

At the bottom of the window, there are three buttons: Save, Cancel, and Help.

Customize Guest Portal

Go to Configuration → General Settings and click on “Guest Registration”:

- Edit the title and message boxes as desired.
- Enable or disable terms and conditions
- Set the number of days to keep guest history details

Edit Setting

Guest Registration

Show Terms of Use

Login Page Title: Welcome to Guest Registration!

Login Page Message: You have reached this portal because your device needs to be validated for guest access.

Pending Approval Message Title: Default: Guest Access is Pending

Pending Approval Message: Default: Please wait for Approval

Get Guest's IP from Proxy Header or Client Side

Miscellaneous

How Long to Keep Guest History (Days): 30

Guest Login

Allow Guest Login by Access Code

Allow Guest Login by Credential

Allow Self-serve Guest Registration

Self-serve Guest Template: 1 day guest

Save Cancel Help

- Scroll down to enable your organizations preferred login methods

Edit Setting

the guest history

Guest Login

Allow Guest Login by Access Code

Allow Guest Login by Credential

Allow Self-serve Guest Registration

Self-serve Guest Template: 1 day guest

Allow guest login by access code – Enabled by default, this option allows for a guest to use a sponsor-provided access code to self-register a guest account. Based on Guest Templates, different access codes can require different registration information or grant different access to the guest \ consultant. Approval can also be required after the guest registers.

The screenshot shows a 'Guest Login' form with a light green header. Below the header, the text 'Please select your login type.' is followed by three radio button options: 'I have an access code.' (which is selected), 'I have guest login credentials.', and 'Register for Guest Access.'. A horizontal line separates this section from the next. Below the line, the text 'Please enter your provided Access Code.' is followed by a text input field labeled 'Access Code:'. At the bottom of the form is a blue 'Submit' button.

Allow guest login by credential – Enabled by default, this option allows for a guest to use their guest credentials to login. Guest Credentials can be created and provided by a sponsor or created by the guest as part of an earlier self-registration process.

The screenshot shows a 'Guest Login' form with a light green header. Below the header, the text 'Please select your login type.' is followed by three radio button options: 'I have an access code.', 'I have guest login credentials.' (which is selected), and 'Register for Guest Access.'. A horizontal line separates this section from the next. Below the line, the text 'Username:' is followed by a text input field. Below that, the text 'Password:' is followed by a text input field. At the bottom left of the form is a red link that says 'Forgot Your Password?'. At the bottom right is a blue 'Login' button.

Allow self-service guest registration – Enabled by default, this option allows a guest to provide their contact information required and get immediate guest access without requiring an access code. Based on the guest template used, approval can be required, and the information they must provide can be customized.

It also possible to provide the guest with an option to provide their sponsor's e-mail address for the approval process and on how long their registration should be active.

Guest Login

Please select your login type.

I have an access code.

I have guest login credentials.

Register for Guest Access.

Your Sponsor's Email

Full Name * :

Email Address * :

Cell Phone * :

Company * :

Expire after: 12h 12h 1d 2d

Request Access

Automated Guest Registration – CGX Access supports an optional automated guest account creation feature. Using syslog, third-party systems can send guest information to the appliance. For example, when a guest registers at reception, the front desk system can send guest details to CGX Access, which will create a guest account for the user. Contact InfoExpress or your authorized partner for more information on this enhanced feature.

Guest Registration Templates

As outlined above, Easy NAC supports multiple registration methods to support a variety of guest registration experiences. To customize these different methods, templates can be used to address unique registration requirements. For example, some guest templates can require basic guest info and grant internet access for 1 day. While other templates may require more in-depth information and require approval before granting 3 days of server access.

A few registration templates are pre-configured on Easy NAC. These templates can be modified, and new templates can be created. The default templates include:

- **Consultant Registers Themselves**
 - Consultant register themselves using an access code

- Account expiration set for 1 week, with authentication every 12 hours
- A consultant tag is assigned, so that the guest would be given consultant access
- Approval is not required, but can be enabled
- Limited to 1 device
- **1-day guest – no approval necessary**
 - A random password \ username is created automatically once user inputs their details
 - Account is valid for (12-hours)
 - No approval is necessary, but can be enabled
- **Automated Guest Registration**
 - Used only when the custom Automated Guest Registration Feature has been configured. This feature allows 3rd party servers to send guest accounts details to the CGX Access appliance.
 - Controls the length of time a user is allowed guest access and how often they must re-authenticate

Customizing Device Registration Templates for Guests

- Go to Configuration → Device Registration Templates → Guest Registration Templates
- Select an existing template or Click “Add template” to create a new one

The above image shows various fields for the guest registration options. Here administrators can adjust the user experience, required fields, and account validity, etc.

The first step is to decide if the template is for guest Self-Registration or Sponsor Registration. With Sponsor registration, an approved employee(s) will create the account and pass the details to the visitor. When a sponsor registers a guest, there is no need for the Access Code concept, so this template has less options.

Self-Registration

Sponsor Registers Guest

Guest Template options (for Self-Registration)

Method Name – Use a name that would be meaningful for the Sponsors who may use it

Description – Optional (can be used to provide more details about the template)

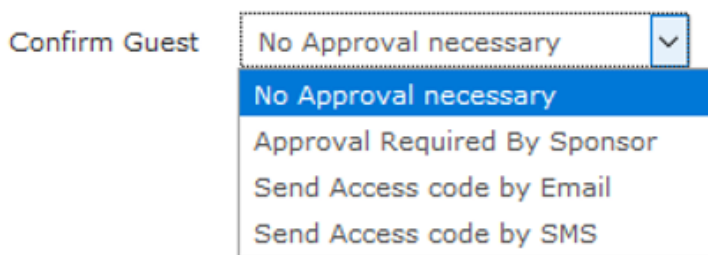
Username Created – Decide if the account name is auto generated by the system or the guest

Password Created - Decide if the account name is auto generated by the system, or the guest

Show guest credentials on registration – After a guest completes the registration process their browser will show a successful web page. If selected, this checkbox will remind or inform the user of their credentials on this success page.

Select the information that the guest must enter – Select the boxes that the guests are shown during the registration process. Additional custom fields can be added under Configuration → General Settings → Registration Fields.

Confirm Guest – This dropdown box allows you to configure an additional verification check.



Approval Required by Sponsor – With this option a sponsor e-mail is configured in the template. This sponsor will receive an e-mail when a guest registers using this template. The Sponsor can 1-click a link in the e-mail to approve the guest. If outside the office, the sponsor can also reply to the e-mail with a keyword, like (approve, accept, OK, etc.) to also approve the guest. (e-mail approval requires the e-mail orchestration feature to be enabled).

When using the Self-Service Registration feature, it can be convenient to allow the guest to specify their sponsor. A group of employees or the entire company can be given permission to sponsor a guest.

Confirm Guest

Allow guest to provide sponsor email

Approval Emails

Send email to guest after approving / rejecting request

Note: WhatsApp, Slack and Teams can also be used to approve guest accounts when integration has been enabled.

Send Access code by Email – When using this method, the e-mail provided by the guest during registration will be sent a code, that must be typed into the guest portal to complete the registration process. Note: the guest will need access to his e-mail account.

Send Access code by SMS – When using this method, the phone number provided by the guest during registration will be sent a code, that must be typed into the guest portal to complete the registration process. Note: an SMS gateway must be configured to use this feature.

Tag Guest – When checked, a Tag can be selected and assigned to the guest’s device. This tag is useful for assigning a specific type of access to this guest. For example, if assigned a consultant tag, they will be assigned consultant access. For more details on tags, see the section titled Tagging Devices and Allowlisting.

Access Code Type – Access codes are useful when using different templates for different types of guests. This optional setting allows you to configure if the access codes created can be used more than once (Group use) or one-time only. Group use can be more convenient, while one-time use offers more security for when access is being provided to sensitive resources.

Code Expires after – This setting allows you to configure how long an Access code, once created, will still be valid. For Group use codes, you may want to change them on a regular basis. You can provide a default value, but also choose to let sponsors change this value, when the Access code is first generated.

Access Code Prefix – By default, access codes are randomly generated, with a prefix that can be used to help you remember what the code is for. For example, if you create a template designed for events, you may want to use a prefix EV. Then all access codes generated using this template will start with EV. A simpler approach is to check the box to allow the sponsors to create any code they prefer manually. With this approach, they can create access code called Dec20-event. This would be easier for both sponsors and guests to remember.

Account Expires After – Sets the duration of the account once it has been created using this template. Once the account expires, the guest will need to complete the registration process again, if necessary. Using the checkboxes provided, the administrator can choose to allow sponsors or guests to adjust the length of time their account should last.

Max Devices per Guest – Sets the max number of devices that a guest can use with their account.

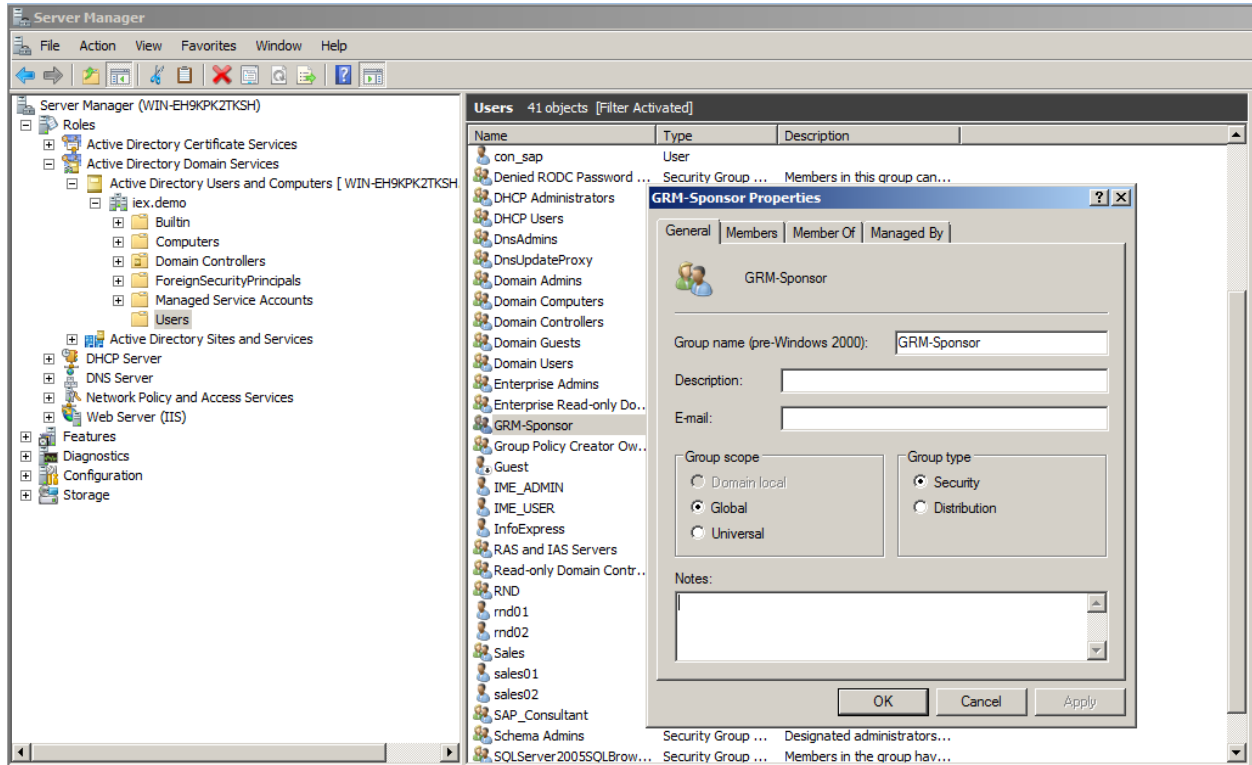
Setting up Sponsors

Easy NAC can query the Active Directory server to validate permissions for sponsors to access the management UI. Approved sponsors would only be given access to guest management functionality.

Using the "Active Directory Users and Computers" MMC:

- Add the group “GRM-Sponsor”

Note: upper/lower case is significant when creating AD groups.



Once the GRM-Sponsor AD group has been created, staff can be given sponsor rights (by adding their user-id to the GRM-Sponsor group).

By default, sponsors can sponsor all types of guest accounts. To limit sponsors to only certain guest types (for example, if the reception staff is only permitted to create daily visitors), please follow these steps:

- Go to Configuration → Device Registration Methods
- Verify the types you want the sponsor to be able to administer
- Go to Configuration → Permission Manager and select the GRM-Sponsor Role (or another role you may have created)
- Select the appropriate Registration Methods the sponsor should be allowed to administer

Guests/BYOD devices	
Access to Device Registration Templates	<input checked="" type="radio"/> No access <input type="radio"/> Readonly <input type="radio"/> R/W
Allow to Sponsor	<input checked="" type="checkbox"/> All guest types
	<input type="checkbox"/> Consultant Register Themselves
	<input type="checkbox"/> 1 day guest
Access to Device Registration Manager	<input checked="" type="radio"/> No access <input type="radio"/> Readonly <input type="radio"/> R/W

Sponsoring Users

Creating a “Consultant Registers Themselves” Access Code

- A user who has either GRM-Sponsor or CGX-Admin permissions can go to Visibility → Guest Registration Manager. If a user only has sponsor access, they can log in to the main CGX Access web GUI and will have limited access to the Sponsor Guest pages.
- Choose “Consultant Registers Themselves” from the pick list and click on “Create a Sponsorship”:

The screenshot shows the CGX Access web interface. At the top, there is a header with 'CGX Access Remote Server' and a 'Visibility' dropdown. Below this is a breadcrumb trail: 'CGX Access / Registration Manager'. A navigation bar contains 'Sponsor Guest', 'Guest Accounts', 'Report', and 'Guest Request'. The main content area is titled 'Sponsor a Guest's Access to MyCompany's Network'. Underneath, it says 'Select a registration template:' followed by a dropdown menu with three options: 'Consultant Register Themselves', 'Consultant Register Themselves' (highlighted), and '1 day guest'. To the right of the dropdown is a blue button labeled 'Create a Sponsorship'.

- Complete the fields as desired and click “Save”:

The screenshot shows the same CGX Access web interface as the previous one, but now the 'Create a Sponsorship' button has been replaced by a form. The form is titled 'Sponsor a Guest's Access to MyCompany's Network' and contains the following fields:

- 'Period Valid Expire *': A text input field containing '+1 weeks'.
- 'Access Code Expire': A text input field containing '2021-05-31 08:43:38'.
- 'Authentication Interval *': A text input field containing '43200'.
- 'Access Code *': A text input field containing 'AV7days'.

 At the bottom of the form are two buttons: a blue 'Save' button and a grey 'Back' button.

To create other types of access codes, follow the process outlined above. When additional information is needed, the web UI will request them.

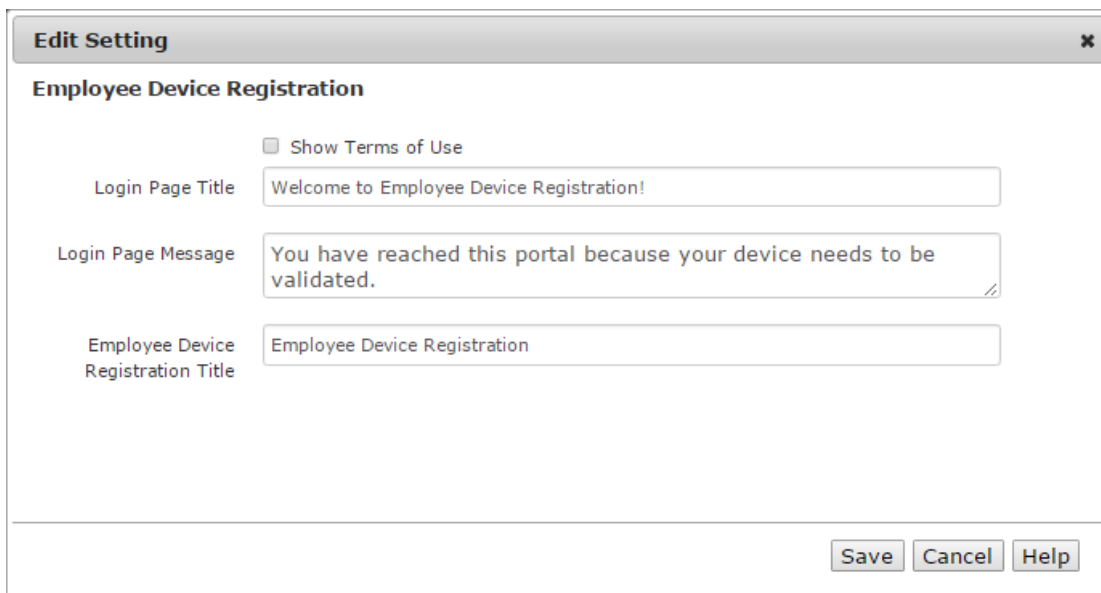
Configuring Device Registration

Easy NAC supports device registration and is commonly used to support Bring Your Own Device (BYOD) initiatives. Employee's or student devices are checked by validating their credentials against Active Directory, Azure AD, or a Radius database. When a new device joins the network, it will be redirected to the captive portal. Staff would then be able to register the device, and this registration would be valid for days, weeks, or months. Several configuration options allow administrators to have access control of the BYOD devices. Administrative options include:

- Which AD groups are allowed to register BYOD device(s)
- Quantity of BYOD devices allowed per user (by group)
- Type of BYOD devices allowed
- Role-based access granted

Customizing the Device Registration portal

- Go to Configuration → General Settings and click on “Employee Device Registration”.



The screenshot shows a dialog box titled "Edit Setting" with a close button (X) in the top right corner. The main heading is "Employee Device Registration". Below the heading, there is a checkbox labeled "Show Terms of Use" which is currently unchecked. There are three text input fields: "Login Page Title" containing "Welcome to Employee Device Registration!", "Login Page Message" containing "You have reached this portal because your device needs to be validated.", and "Employee Device Registration Title" containing "Employee Device Registration". At the bottom right of the dialog box, there are three buttons: "Save", "Cancel", and "Help".

- Edit the title and message boxes as desired.
- Opt-in or Opt-out to show Terms of Use
- Click on save to accept any changes to the configuration.

Confirm Active Directory settings

To validate AD credentials, the AD server must be configured correctly. To verify settings, use the GUI.

- Go to Configuration → General Settings.
- Click on Active Directory Servers

- Under Active Directory Server, confirm the host or IP address of the AD domain controller and the Account suffix in the "Account Suffix" field. The @ symbol should proceed the Account Suffix.


By default, all domain users with valid credentials will be able to register their BYOD devices. It is possible to limit which groups can register their devices, and to set different policies for different groups. The enable granular AD registration, the AD groups must be specified in the CGX Access server.

- Go to Configuration → General Settings.
- Click on “Names Used by Policies”

Add the Active Directory groups that would need to register their devices. Groups that are added will be shown as a configurable option when customizing Device Registration methods.

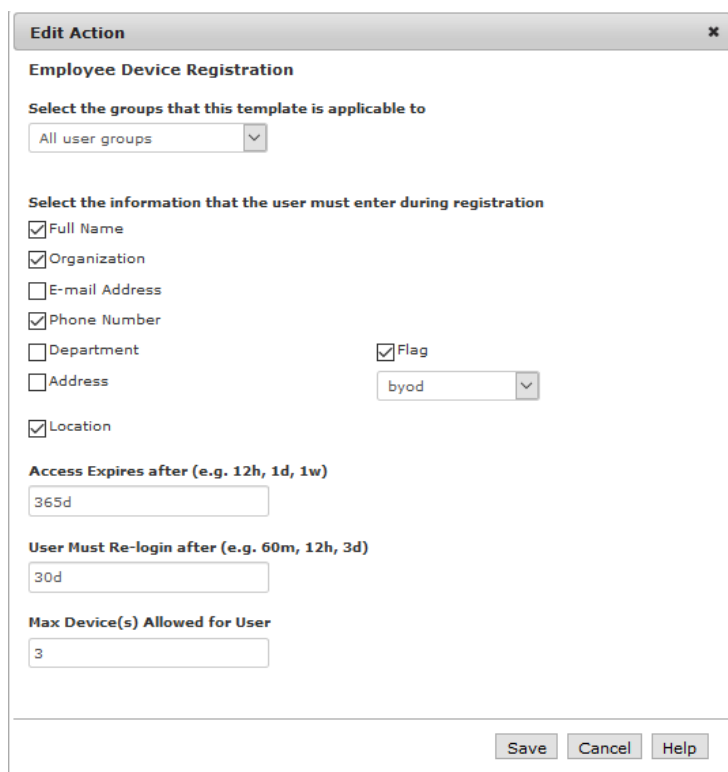
Customizing Device Registration Methods

- Go to Configuration → Device Registration Templates → Device Registration Templates

Employee Registers Personal Devices - Employee registers their own device. Must enter full name, phone #, location Access expires after 365d Users must re-login after 365d Max device(s) allowed for user is 3 Will be flagged as "byod"	
MsAzure AD Employee Registration - MsAzure AD Employee Registration Account expires after 12h Employee must re-login after 12h Max device(s) allowed for employee is 1	

There are two default templates for employee device registration, one for customers use cloud-based MS Azure AD, and another for traditional AD servers. To make changes to a typical registration...

- Click on the “Employee Registers Personal Device” registration type:



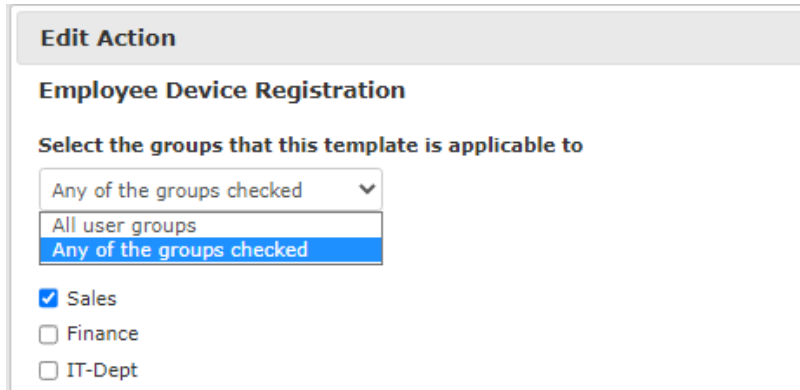
The screenshot shows a dialog box titled "Edit Action" with a close button (x) in the top right corner. The main title is "Employee Device Registration". Below the title, there is a section "Select the groups that this template is applicable to" with a dropdown menu currently set to "All user groups". The next section is "Select the information that the user must enter during registration", which includes several checkboxes: "Full Name" (checked), "Organization" (checked), "E-mail Address" (unchecked), "Phone Number" (checked), "Department" (unchecked), "Address" (unchecked), and "Location" (checked). There is also a "Flag" checkbox (checked) with a dropdown menu set to "byod". Below these sections are three input fields: "Access Expires after (e.g. 12h, 1d, 1w)" with "365d" entered, "User Must Re-login after (e.g. 60m, 12h, 3d)" with "30d" entered, and "Max Device(s) Allowed for User" with "3" entered. At the bottom right, there are three buttons: "Save", "Cancel", and "Help".

The above defines various parameters that can be customized for the device registration method. The default method is configured to apply to all users with valid credentials.

Additional device registration methods can be created for different AD groups to have different parameters. This can be useful in situations where different length of access, device quantity allowed, or different information needs to be gathered on the user.

To modify:

- Change the top pulldown box to 'Any of the groups checked'
- Select the AD groups that the template will be applied to:



Edit Action

Employee Device Registration

Select the groups that this template is applicable to

Any of the groups checked ▾

All user groups

Any of the groups checked

Sales

Finance

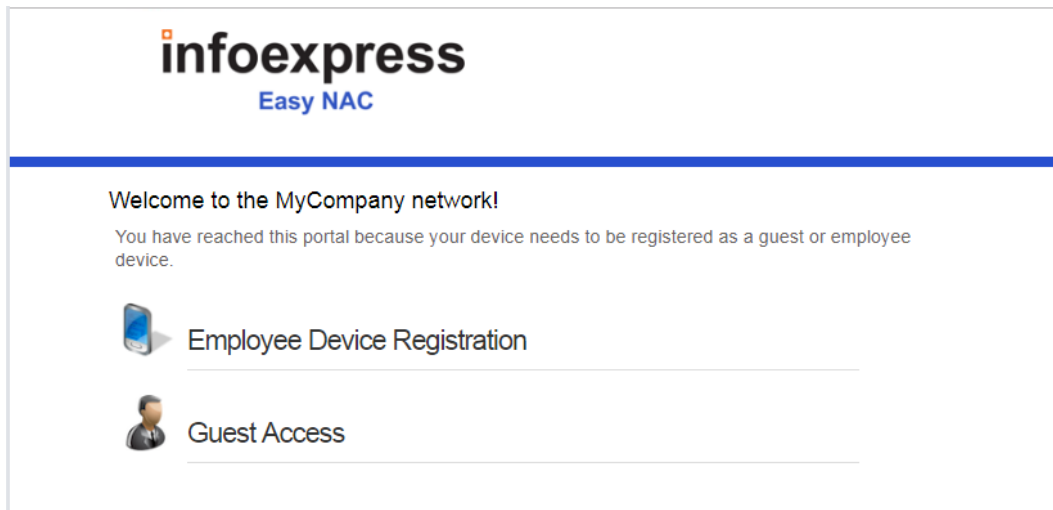
IT-Dept

- Change the parameters for information gathered, access expiration, etc.
- Click 'Save' and Activate changes.

Note: When you have multiple Device Registration Methods, they are evaluated from top to bottom. Methods can be re-arranged by dragging and dropping them in order they should be evaluated.


User Experience


When a user is connected to the network, the browser will be redirected to a page like this:



infoexpress
Easy NAC

Welcome to the MyCompany network!
You have reached this portal because your device needs to be registered as a guest or employee device.


 [Employee Device Registration](#)

 [Guest Access](#)

Users can click on the Employee Device Registration link to be presented with a login screen:

Welcome to Employee Device Registration!

You have reached this portal because your device needs to be validated.

 **Device Self-Registration Login**

Please enter your Active Directory (employee) credentials.

Username:

Password:

At this point, the employee will enter their AD credentials. Depending on the configuration they may be prompted to complete an information form such as Full Name, Organization, Location, etc. After completion the appropriate access will be assigned.

This device will be remembered by the system based on the timeout specified in the device registration template. The user will not be asked for credentials until the device ages out of the database or the timer for login requests has expired.

Note: If a user exceeds the number of devices they are allowed to registered, they will be shown their list of devices, and can choose to deregister one of more devices.

Integration: Anti-Virus \ Endpoint Management

Easy NAC supports integration with enterprise AV, XDR and endpoint management vendors. By leveraging the integration with the management server, CGX Access can enforce compliance with security policies, without the use of agents. Devices out-of-compliance can be restricted, and an administrator(s) alerted.

Supported Solutions:

- Bitdefender GalaxyZone
- Carbon Black Cb Response – 6.x +
- Carbon Black Cloud
- Cortex XDR
- CrowdStrike Falcon
- Cybereason
- ESET Antivirus - 6.5+
- Elastic XDR
- FireEye HX Integration
- HCL BigFix - 9.x +
- Ivanti Security Controls – 2019.3 +
- Kasaya VSA
- Kaspersky Antivirus - 10.x+
- Managed Engine Desktop Central
- Managed Engine Patch Manager
- Microsoft Intune
- Microsoft SCCM \ WSUS – 4.x +
- Microsoft Windows Management Instrumentation (WMI)
- Moscii StarCat 2013 and StarCat 10
- OKTA Verify
- Sophos Enterprise Console - 5.x +
- Sophos Central (cloud)
- Symantec Endpoint Protection Manager - 14.x
- Symantec Endpoint Protection Cloud
- Trend Micro OfficeScan - XG+
- Trend Micro Apex Central (cloud)
- Trellix ePO - 5.x +
- Webroot (cloud)

Bitdefender Integration

- In CGX Access GUI go to Configuration → Integration
- Click on "Bitdefender"
- Check "Enable Integration"
- Enter Access URL and API Key

Edit Action

Bitdefender

Enable integration

Configuration

Access URL:

API Key:

Query interval (seconds):

Test connection

Show query result data

Policies

CONDITIONS

Flag devices running Bitdefender Agent

Flag devices that are offline

Flag devices that have not reported in days

Flag devices with AV signature older than days

Flag devices that are infected by malware

FLAG

AV-managed

AV-offline

AV-stale

AV-out-of-date

infected

Save Cancel Help

The URL and API key can be obtained by logging into GravityZone → MyAccount → API

Notes:

1. The access URL should be lower case and match what's specified in the Control Center

Control Center API

Access URL:

2. The Network API needs to be enabled

API key

Key: ae73d4ed8165808d30396cf0e32ff4d7b8c2fbb9a485ba91a665f7467228dc57

Enabled APIs:

- Companies API
- Reports API
- Licensing API
- Accounts API
- Packages API
- Incidents API
- Network API
- Quarantine API
- Integrations API
- Event Push Service API
- Policies API

Save Cancel

- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and Bitdefender cloud have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

- Flag devices running Bitdefender Agent
- Flag devices that are offline
- Flag devices that have not reported in days
- Flag devices with AV signature older than days
- Flag devices that are infected by malware
- Flag devices if Advanced Threat Control is disabled
- Flag devices if AntiMalware is disabled
- Flag devices if Content Control is disabled
- Flag devices if Device Control is disabled
- Flag devices if Firewall is disabled
- Flag devices if Encryption is disabled

FLAG







-
-
-
-
-
-
-
-
-
-
-

There are several conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

[Activate](#) [Cancel Changes](#)

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	  
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	  

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off, AV-out-of-date, etc. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

Carbon Black Cb Response Integration

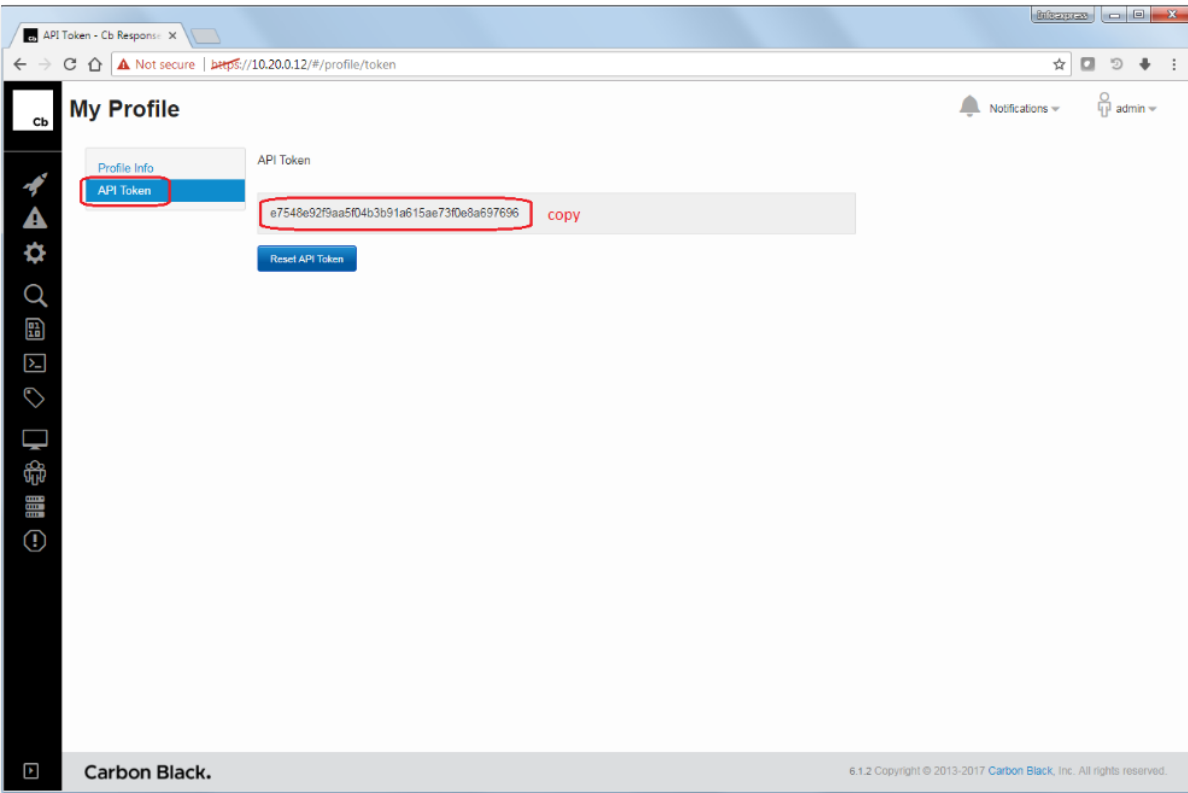
- In CGX Access GUI go to Configuration → Integration
- Click on "Carbon Black"

The screenshot shows the 'Edit Action' configuration window for Carbon Black Integration. The window is titled 'Edit Action' and has a close button in the top right corner. The main content is organized into several sections:

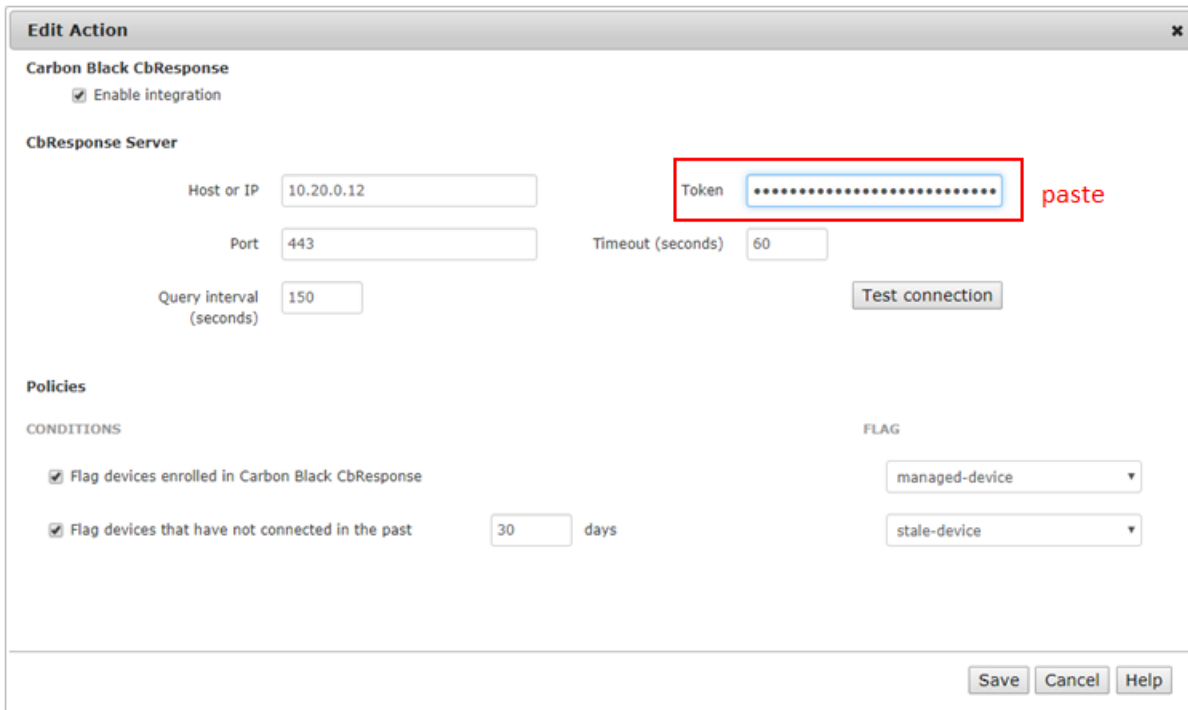
- Carbon Black Integration:** A checkbox labeled 'Enable Integration' is checked.
- Server Configuration:**
 - Version:** A dropdown menu is open, showing 'Cb Response' (selected) and 'Cloud'.
 - Host or IP:** A text input field containing 'aerehndrcenteraeproymoc'.
 - Port:** A text input field containing '443'.
 - Token:** A text input field with a toggle icon on the right.
 - Timeout (Seconds):** A text input field containing '60'.
 - Query Interval (Seconds):** A text input field containing '150'.
 - Test Connection:** A button.
 - Show Query Result Data:** An unchecked checkbox.
- Policy:**
 - CONDITION:** A checkbox labeled 'Tag devices enrolled in Carbon Black' is checked.
 - TAG:** A dropdown menu showing 'managed-device'.

At the bottom right of the window, there are three buttons: 'Save', 'Cancel', and 'Help'.

- Check "Enable Integration"
- Select Version: Cb Response
- Enter Hostname or IP / port
- In Cb Response console go to Admin → My Profile → API Token



- Copy API Token and Paste into Token field



- Use "Test connection" button to validate settings and connectivity

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and Cb Response server have been successfully tested, policies can be set to enforce endpoint devices have been installed with the Cb Response agent and connecting to the server regularly.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

Flag devices enrolled in Carbon Black Cb Response

Flag devices that have not connected in the past days

FLAG

managed-device

stale-device





When selected CGX Access will set tags and automatically grant access to devices being protected by Cb Response. While devices that have not connected in the past x days can be tagged as a stale-device.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

[Add Rule](#)

[Activate](#) [Cancel Changes](#)

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	 
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	 

The policy above shows a device will be assigned full-access if tagged as managed-device. However, it would be given a non-compliant role if it has been tagged as a stale-device. The order of the rules is important, as they are evaluated in descending order.

Tip: The managed-device tag is helpful in expediting deployments. Any device that is being protected by the Carbon Black will automatically be granted access to the network.

Carbon Black Cloud Integration

- In Carbon Black Cloud web management go Settings → API Access
 - Define a new Access Level
- Note:** only Read access for Device - General Information is required

Dialog: Edit Access Level

* Name: EasyNAC

* Description: EasyNAC API Call

Copy permissions from: [Dropdown]

CATEGORY	PERMISSION NAME	NOTATION NAME	CREATE	READ	UPDATE	DELETE	EXECUTE
> Device	Bypass	device.bypass	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> Device	General information	device	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> Device	Policy assignment	device.policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> Device	Background scan	device.bg-scan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Save, Cancel

- Add an API Key with the custom Access Level create above

Dialog: Add API Key

* Name: EasyNAC API

Description: [Text Area]

* Access Level type: Custom

* Custom Access Level: EasyNAC

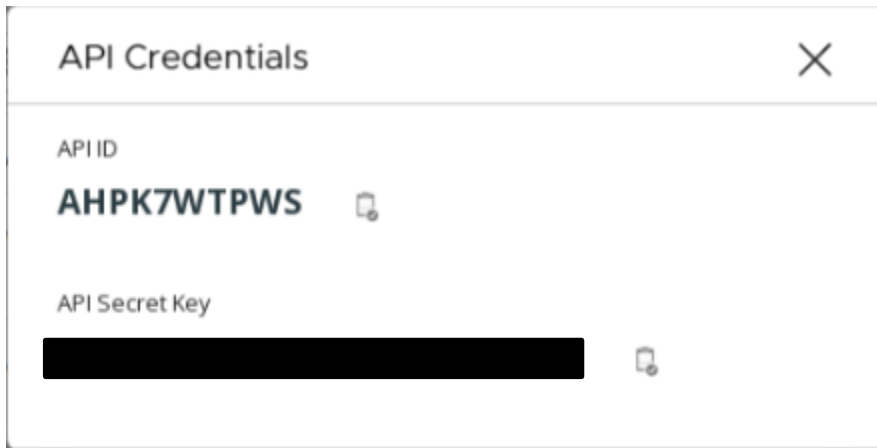
Authorized IP addresses

Specify a comma separated list of single IP address, or an IP address range in CIDR notation (for example, 203.0.113.5/32).

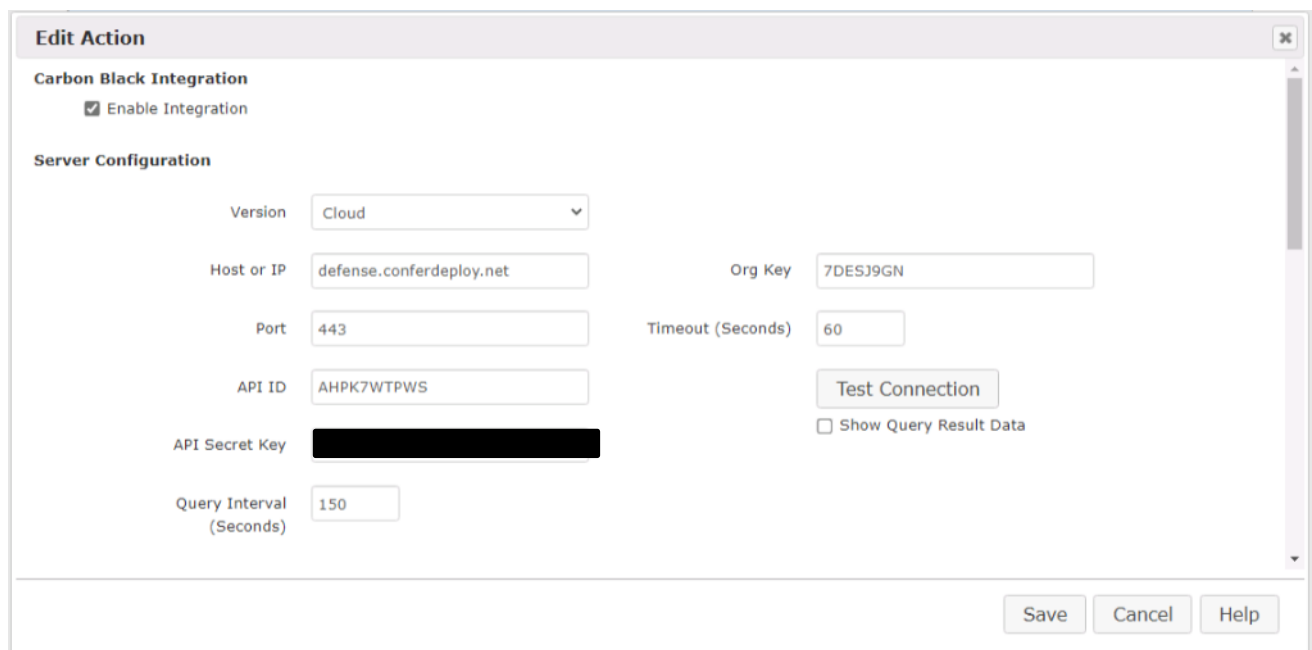
[Text Area]

Buttons: Save, Cancel

- Once API is created – Copy API ID and API Secret key



- In CGX Access GUI go to Configuration → Integration
- Click on "Carbon Black"
- Check “Enable Integration”, select Cloud version
- Enter Access URL, API ID, API Secret Key and Org Key



- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and Carbon Black Cloud have been successfully tested, policies can be set to enforce compliance with policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION

- Flag devices enrolled in Carbon Black
- Flag devices with deregistered or uninstalled sensor
- Flag devices with sensor being in bypass mode
- Flag devices with inactive sensor
- Flag devices with out-of-date sensor
- Flag devices that are in quarantine
- Flag devices that have not connected in the past days

FLAG

- ▾
- ▾
- ▾
- ▾
- ▾
- ▾
- ▾

There are multiple conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	<input type="button" value="⊙"/> <input type="button" value="↗"/> <input type="button" value="✕"/>
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	<input type="button" value="⊙"/> <input type="button" value="↗"/> <input type="button" value="✕"/>

The example above shows a device will be assigned a non-compliant role if it has been tagged as stale-device or Sensor-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The managed-device tag is helpful in expediting deployments. Any device that is being managed by the organization's Carbon Black deployment can automatically be granted access to the network.

CrowdStrike Integration

- In CrowdStrike web management go Support and Resources → API Client and Keys
- Click on “Add new API Key”

Add new API client

CLIENT NAME
Easy NAC Appliance

DESCRIPTION
Integration with Network Access Control for automated trust and compliance checks

API SCOPES

	Read	Write
Alerts	<input type="checkbox"/>	<input type="checkbox"/>
Detections	<input type="checkbox"/>	<input type="checkbox"/>
Device control policies	<input type="checkbox"/>	<input type="checkbox"/>
Hosts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Actors (Falcon X)	<input type="checkbox"/>	—
Indicators (Falcon X)	<input type="checkbox"/>	—

CANCEL ADD

Note: only Read access to Hosts in required

- Complete form and Click ADD

API client created

✓ API client created

CLIENT ID
b6732f5435e74d66872e2b01d215f6bf

SECRET
[REDACTED]

BASE URL
https://api.us-2.crowdstrike.com

Copy this to a safe place
This is the only time we'll show you this secret

DONE

Note: Once API is created – Copy Client ID, Secret, and Base URL

- In CGX Access GUI go to Configuration → Integration
- Click on "CrowdStrike"
- Check "Enable Integration"
- Enter Access URL, Client ID and Client Secret

Edit Action

CrowdStrike Integration

Enable integration

Server Configuration

Access URL:

Client ID:

Client Secret:

Query Interval (Seconds):

Test connection

Show query result data

Policies

CONDITIONS

Flag devices running CrowdStrike Agent

Flag devices that have not reported in days

Flag devices with Sensor update older than days

Flag devices with Device Control disabled

FLAG

- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and CrowdStrike cloud have been successfully tested, policies can be set to enforce compliance with policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

- Flag devices running CrowdStrike Agent
- Flag devices that have not reported in days
- Flag devices with Sensor update older than days
- Flag devices with Device Control disabled
- Flag devices with Firewall disabled

FLAG







-
-
-
-
-

There are multiple conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

[Activate](#) [Cancel Changes](#)

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	  
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	  

The example above shows a device will be assigned a non-compliant role if it has been tagged as stale-device or Sensor-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The managed-device tag is helpful in expediting deployments. Any device that is being managed by the organization's CrowdStrike deployment can automatically be granted access to the network.

Cybereason Integration

- In CGX Access GUI go to Configuration → Integration
- Click on "Cybereason"
- Check "Enable Integration"

Edit Action

EARLY RELEASE

Cybereason Integration

Enable integration

Server Configuration

Host or IP: customer.cybereason.net

Port: 443

Query Interval (Seconds): 120

Username: user@infoexpress.com

Password:

Test connection

Show query result data

Policy

CONDITION

Flag devices running Cybereason Agent

Flag devices that are offline

FLAG

AV-managed

AV_offline

Save Cancel Help

- Enter Hostname or IP (should be the same as your management console)
- Specify Username and Password (should also work on management console)
- Use "Test connection" button to validate settings
- You may leave Query interval the default or adjust
- Save this configuration

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and Cybereason have been successfully tested, policies can be set to enforce compliance with policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions. CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Policy

CONDITION

- Flag devices running Cybereason Agent
- Flag devices that are offline
- Flag devices that are isolated
- Flag devices with Device Control disabled
- Flag devices that have not connected in days
- Flag devices that have not updated in days
- Flag devices with Sensor out of date
- Flag devices with Firewall disabled
- Flag devices with Anti-Malware disabled
- Flag devices with Prevention mode disabled
- Flag devices with Anti-Ransomware disabled
- Flag devices with Anti-Exploit disabled
- Flag devices with PowerShell mode disabled
- Flag non-compliant managed devices

FLAG

- AV-managed
- AV-offline
- infected
- dev-control-off
- AV-stale
- AV-out-of-date
- Sensor-out-of-date
- FW-off
- AV-off
- AV-Config
- AV-Config
- AV-Config
- AV-Config
- non-compliant

Auto Trust Policy

[Activate](#) [Cancel Changes](#)

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ✎ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ✎ ✕

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off or AV-out-of-date. **Tip:** The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

ESET Antivirus Integration

- In CGX Access GUI go to Configuration → Integration
- Select the “ESET Antivirus”

Edit Action

ESET Antivirus

Enable integration

SQL Server Configuration

Host or IP: 10.10.0.230

Port: 1433

Database: era_db

Username: sa

Password:

Query interval (seconds): 150

Test connection

Policies

CONDITIONS

Flag devices running ESET Antivirus Agent

Flag devices with AV signature older than 10 days

Flag devices that have not connected in 7 days

FLAG

AV-managed

AV-out-of-date

AV-stale

Save Cancel Help

CGX Access communicates with the ESET Security Management Center by querying the SQL database.

- Setup the SQL Server used by ESET to support SQL queries over TCP 1433. See prerequisites below.
- Check “Enable Integration”
- Enter Hostname or IP, database port, database name, and database Username & Password
- Use "Test connection" button to validate settings → Save changes

ESET SQL Prerequisites:

- Configure the MS SQL Server on the Administration Server to enable TCP/IP and specify a port such as 1433
- Use MS SQL Server management studio to create an account with permission to read the era_db database. The default database name use by ESET is era_db.
- Configure the firewall on the ESMC to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your ESET Security Management Center.

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and ESET Security Management Console have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

- Flag devices running ESET Antivirus Agent
- Flag devices with AV signature older than days
- Flag devices that have not connected in days

FLAG

AV-managed

AV-out-of-date

AV-stale

There are a few conditions you can select to monitor. When selected, CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Activate
Cancel Changes

[Add Rule](#)

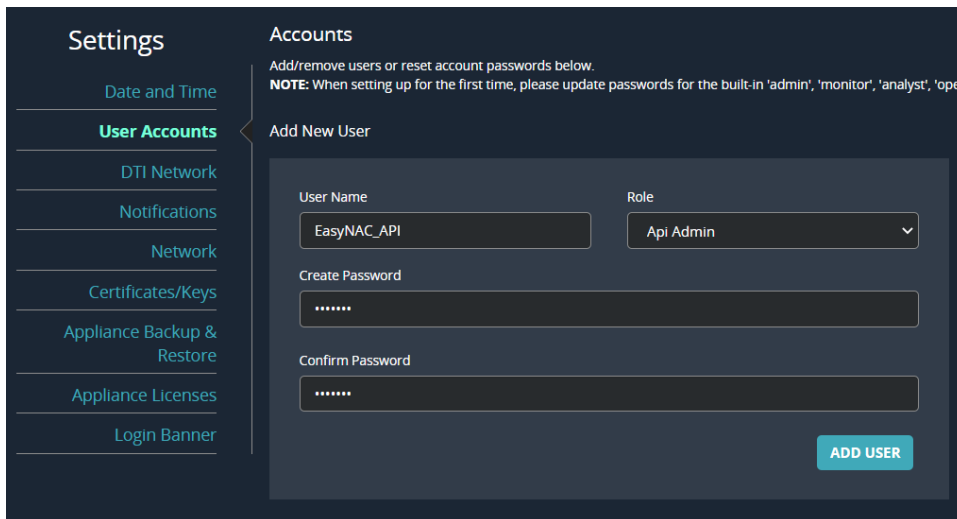
Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	<input type="button" value="⊙"/> <input type="button" value="↗"/> <input type="button" value="✕"/>
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	<input type="button" value="⊙"/> <input type="button" value="↗"/> <input type="button" value="✕"/>

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

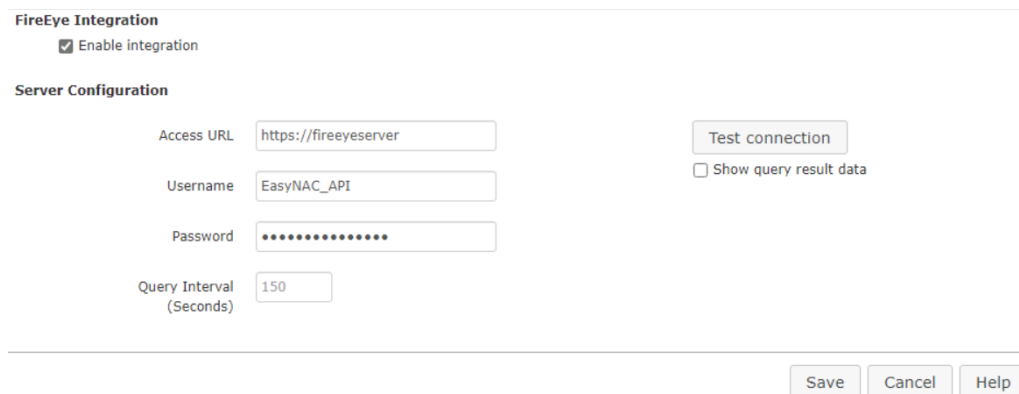
FireEye HX Integration

- In FireEye HX management console go to Admin → Appliance Settings → User Accounts
- Create a New User and select the “API Admin” role for the account.



The screenshot shows the 'Accounts' section of the FireEye HX management console. On the left is a 'Settings' sidebar with options like 'Date and Time', 'User Accounts', 'DTI Network', 'Notifications', 'Network', 'Certificates/Keys', 'Appliance Backup & Restore', 'Appliance Licenses', and 'Login Banner'. The main area is titled 'Accounts' and contains the 'Add New User' form. The form includes a 'User Name' field with 'EasyNAC_API', a 'Role' dropdown menu with 'Api Admin' selected, a 'Create Password' field, and a 'Confirm Password' field. An 'ADD USER' button is located at the bottom right of the form.

- In CGX Access GUI go to Configuration → Integration
- Click on "FireEye Integration"
- Check “Enable Integration”
- Input the Access URL. It’s the same URL used by the FireEye management console



The screenshot shows the 'FireEye Integration' configuration page. At the top, there is a section titled 'FireEye Integration' with a checked 'Enable integration' checkbox. Below this is the 'Server Configuration' section, which contains several input fields: 'Access URL' (https://fireeyeserver), 'Username' (EasyNAC_API), 'Password' (masked with asterisks), and 'Query Interval (Seconds)' (150). To the right of the 'Access URL' field is a 'Test connection' button. Below the 'Test connection' button is a checkbox for 'Show query result data'. At the bottom of the page are three buttons: 'Save', 'Cancel', and 'Help'.

- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and FireEye have been successfully tested, policies can be set to enforce compliance with policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Edit Action

CONDITION	FLAG
<input checked="" type="checkbox"/> Flag devices running FireEye Agent	AV-managed
<input checked="" type="checkbox"/> Flag devices with Antivirus update older than <input type="text" value="7"/> days	AV-out-of-date
<input checked="" type="checkbox"/> Flag devices with Malware Guard update older than <input type="text" value="7"/> days	AV-out-of-date
<input checked="" type="checkbox"/> Flag devices with Antivirus disabled	AV-off
<input checked="" type="checkbox"/> Flag devices with Malware Guard disabled	AV-off

There are multiple conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the organization’s FireEye deployment can automatically be trusted on the network.

HCL BigFix Integration

In CGX Access GUI go to Configuration → Integration

- Select “HCL BigFix”

Edit Action

HCL BigFix Integration

Enable Integration

Server Configuration

Host or IP: 192.168.253.100 Username: SA

Port: 1433 Password:

Database: BFEnterprise Test Connection

Query Interval (Seconds): 150

Policy

CONDITION	TAG
<input checked="" type="checkbox"/> Tag devices enrolled in HCL BigFix	patch-managed
<input checked="" type="checkbox"/> Tag devices that have not reported in 30 days	patch-stale
<input checked="" type="checkbox"/> Tag devices that failed an update more than 30 days ago	patch-failed
<input checked="" type="checkbox"/> Tag devices with updates pending for more than 30 days	patch-pending

Source Severity: e.g. Critical,High,... Category: e.g. Severity Update,Upgrade

Save Cancel Help

- Check “Enable Integration”
- Enter Hostname or IP / database port / database name
- Enter Username / Password to connect to database
- Use "Test connection" button to validate settings
- Save changes

BigFix SQL Prerequisites:

- Verify the MS SQL Server on the BigFix server was enabled for TCP/IP and specify a port such as 1433.
- Use MS SQL Server management studio to create an account with permission to read the BFEnterprise database. BFEnterprise is the default database name used by BigFix.
- Configure the firewall on the BigFix server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your BigFix Server.

Setting and Enforcing Patch Compliance Policies

Once the communications between the CGX Access appliance and BigFix server have been successfully tested, policies can be set to enforce compliance with patch policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION	TAG
<input checked="" type="checkbox"/> Tag devices enrolled in HCL BigFix	patch-managed
<input checked="" type="checkbox"/> Tag devices that have not reported in <input type="text" value="30"/> days	patch-stale
<input checked="" type="checkbox"/> Tag devices that failed an update more than <input type="text" value="30"/> days ago	patch-failed
<input checked="" type="checkbox"/> Tag devices with updates pending for more than <input type="text" value="30"/> days	patch-pending

Source Severity Category

There are four conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Patch Non-Compliance (agent-less checks) Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant - Device is NOT compliant with the corporate patch management policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The policy above shows a device will be assigned a non-compliant role if it has been tagged as patch-failed, patch-pending, or patch-stale. The order of the rules is important, as they are evaluated in descending order.

Tip: The patch-managed tag is helpful in expediting deployments. Any device that is being managed by the BigFix server can automatically be granted access to the network.

Ivanti Security Controls

In CGX Access GUI go to Configuration → Integration

- Select “Ivanti Security Controls”

The screenshot shows the 'Edit Action' window for Ivanti integration. The window has a title bar 'Edit Action' and a close button. Below the title bar, there is a section for 'Ivanti' with a checked checkbox 'Enable integration'. The main configuration area is titled 'SQL Server' and is enclosed in a red rounded rectangle. It contains the following fields: 'Host or IP' (10.100.20.150), 'Port' (1433), 'Database' (Protect), 'Query interval (seconds)' (150), 'Username' (SA), and 'Password' (masked with dots). A 'Test connection' button is located to the right of the password field. Below the 'SQL Server' section is a 'Policies' section with two columns: 'CONDITIONS' and 'FLAG'. The 'CONDITIONS' column has four checked items: 'Flag devices managed by Ivanti', 'Flag devices that have not reported in' (30 days), 'Flag devices with missing patches greater than' (10), and 'Flag devices with missing product levels greater than' (10). The 'FLAG' column has four dropdown menus with values: 'patch-managed', 'patch-stale', 'patch-pending', and 'patch-pending'. At the bottom right of the window are 'Save', 'Cancel', and 'Help' buttons.

- Check “Enable Integration”
- Enter Hostname or IP / database port / database name
- Enter Username / Password to connect to database
- Use "Test connection" button to validate settings
- Save changes

Ivanti SQL Prerequisites:

- Verify the MS SQL Server on the Ivanti server was enabled for remote connections and specify a port such as 1433.
- Use MS SQL Server management studio to create an account with permission to read the Protect database. Protect or SecurityControls are the default database names used by Ivanti.
- Configure the firewall on the Ivanti server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your Ivanti Server.

Setting and Enforcing Patch Compliance Policies

Once the communications between the CGX Access appliance and Ivanti server have been successfully tested, policies can be set to enforce compliance with patch policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies		FLAG
CONDITIONS		
<input checked="" type="checkbox"/> Flag devices managed by Ivanti		patch-managed
<input checked="" type="checkbox"/> Flag devices that have not reported in	30 days	patch-stale
<input checked="" type="checkbox"/> Flag devices with missing patches greater than	10	patch-pending
<input checked="" type="checkbox"/> Flag devices with missing product levels greater than	10	patch-pending

There are four conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

[Add Rule](#)

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↗ ✕
Patch Non-Compliance (agent-less checks) Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant - Device is NOT compliant with the corporate patch management policy	⊙ ↗ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↗ ✕

The policy above shows a device will be assigned a non-compliant role if it has been tagged as patch-pending or patch-pending. The order of the rules is important, as they are evaluated in descending order.

Tip: The patch-managed tag is helpful in expediting deployments. Any device that is being managed by Ivanti can automatically be granted access to the network.

Kaseya VSA Integration

- In CGX Access GUI go to Configuration → Integration
- Click on "Kaseya VSA"
- Check "Enable Integration"
- Enter Hostname or IP / port
- Enter Username / Password to login to Kaseya management console

The screenshot shows the 'Edit Action' window for Kaseya VSA Integration. It includes a checkbox for 'Enable Integration' which is checked. Under 'Server Configuration', there are input fields for 'Host or IP' (saasxx.kaseya.net), 'Port' (443), 'Username' (admin@example.com), and 'Password' (masked with dots). There is also a 'Query Interval (Seconds)' field set to 900 and a 'Matching endpoints based on' dropdown menu set to 'Hostname'. A 'Test Connection' button is located at the bottom right.

Note: Username used for integration should have System Role and System Scope

- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Patch Compliance Policies

Once the communications between the CGX Access appliance and Kaseya VSA server have been successfully tested, policies can be set to enforce compliance with patch policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION

- Flag devices enrolled in Kaseya VSA
- Flag devices that have not reported in days
- Flag devices with **missing approved + missing manual** patches greater than
- Flag devices with **pending** patches greater than

FLAG

- ▾
- ▾
- ▾
- ▾

There are four conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↗ ✕
Patch Non-Compliance (agent-less checks) Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant - Device is NOT compliant with the corporate patch management policy	⊙ ↗ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↗ ✕

The policy above shows a device will be assigned a non-compliant role if it has been tagged as patch-pending or patch-stale. The order of the rules is important, as they are evaluated in descending order.

Tip: The patch-managed tag is helpful in expediting deployments. Any device that is being managed by Kaseya VSA can automatically be granted access to the network.

Kaspersky Antivirus Integration

- In CGX Access GUI go to Configuration → Integration
- Select the “Kaspersky Antivirus”

Edit Action

Kaspersky Antivirus

Enable integration

SQL Server Configuration

Host or IP: 192.168.253.150 Username: SA

Port: 1433 Password: *****

Database: KAV Test connection

Query interval (seconds): 150

Policies

CONDITIONS	FLAG
<input checked="" type="checkbox"/> Flag devices running Kaspersky Antivirus Agent	AV-managed
<input checked="" type="checkbox"/> Flag devices with inactive on-access scanner	AV-off
<input checked="" type="checkbox"/> Flag devices with AV signature older than 10 days	AV-out-of-date
<input checked="" type="checkbox"/> Flag devices that have not connected in 7 days	AV-stale

Save Cancel Help

CGX Access communicates with the Kaspersky Administration Server by querying the SQL database.

- Setup the SQL Server used by Kaspersky to support SQL queries over TCP 1433. See prerequisites below.
- Check “Enable Integration”
- Enter Hostname or IP, database port, database name, and database Username & Password
- Use "Test connection" button to validate settings → Save changes

Kaspersky SQL Prerequisites:

- Configure the MS SQL Server on the Administration Server to enable TCP/IP and specify a port such as 1433
- Use MS SQL Server management studio to create an account with permission to read the KAV database. KAV is the default database name used by Kaspersky.
- Configure the firewall on the Kaspersky Administration Server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your Kaspersky AV Server.

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and Kaspersky Administration Server have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS	FLAG
<input checked="" type="checkbox"/> Flag devices running Kaspersky Antivirus Agent	AV-managed
<input checked="" type="checkbox"/> Flag devices with inactive on-access scanner	AV-off
<input checked="" type="checkbox"/> Flag devices with AV signature older than <input type="text" value="10"/> days	AV-out-of-date
<input checked="" type="checkbox"/> Flag devices that have not connected in <input type="text" value="7"/> days	AV-stale

There are several conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

ManageEngine Desktop Central Integration

- In CGX Access GUI go to Configuration → Integration
- Click on "ManageEngine Desktop Central"
- Check "Enable Integration"
- Enter Hostname or IP / port
- Enter Username / Password to login to ManageEngine

The screenshot shows the 'Edit Action' configuration window for ManageEngine Desktop Central. The window has a title bar with 'Edit Action' and a close button. The main content is divided into several sections:

- ManageEngine Desktop Central**: A checkbox for 'Enable Integration' is checked.
- Server Configuration**:
 - Host or IP: 10.10.200.102
 - Port: 8383
 - API Version: 1.3 (dropdown menu)
 - Username: admin
 - Password: masked with dots
 - Query Interval (Seconds): 900
 - Buttons: 'Upload QR Code image' and 'Test connection'
- Policy**:
 - CONDITIONS**: Three checkboxes are checked: 'Flag devices enrolled in ManageEngine Desktop Central', 'Flag highly vulnerable devices', and 'Flag devices that have not reported in' (with a '30' days input field).
 - FLAG**: Three dropdown menus are set to 'managed-device', 'non-compliant', and 'stale-device'.

At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

- If enabled for Multi-Factor Authentication, Upload QR Code image
- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Patch Compliance Policies

Once the communications between the CGX Access appliance and ManageEngine server have been successfully tested, policies can be set to enforce compliance with patch policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

Flag devices enrolled in ManageEngine Desktop Central

Flag highly vulnerable devices

Flag devices that have not reported in days

FLAG

managed-device

non-compliant

stale-device

There are three conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.







Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Activate

Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	  
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	  

The policy above shows a device will be assigned a non-compliant role if it has been tagged as non-compliant or stale-device. The order of the rules is important, as they are evaluated in descending order.

Tip: The managed-device tag is helpful in expediting deployments. Any device that is being managed by the ManageEngine server can automatically be granted access to the network.

ManageEngine Patch Manager Integration

- In CGX Access GUI go to Configuration → Integration
- Click on "ManageEngine Patch Manager"
- Check "Enable Integration"
- Select ManageEngine Type: On-premise or Cloud
- Enter Hostname or IP / port
- If On-premise: Enter Username / Password to login to ManageEngine
- If Cloud: Enter OAuth Client ID, Secret and Token

Edit Action

ManageEngine Patch Manager Integration

Enable Integration

ManageEngine Type: Patch Manager Plus On-Premise

Server Configuration

Host or IP:

Port: 6383

API Version: 1.3

Query Interval (Seconds): 300

Username:

Password:

Test Connection

Policy

CONDITION	FLAG
...	...

Save Cancel Help

- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Patch Compliance Policies

Once the communications between the CGX Access appliance and ManageEngine server have been successfully tested, policies can be set to enforce compliance with patch policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION	FLAG
<input checked="" type="checkbox"/> Flag devices enrolled in ManageEngine Patch Manager	patch-managed
<input checked="" type="checkbox"/> Flag highly vulnerable devices	non-compliant
<input checked="" type="checkbox"/> Flag devices that have not reported in <input type="text" value="30"/> days	patch-stale

There are a few conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Patch Non-Compliance (agent-less checks) Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant - Device is NOT compliant with the corporate patch management policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The policy above shows a device will be assigned a non-compliant role if it has been tagged as patch-stale or non-compliant. The order of the rules is important, as they are evaluated in descending order.

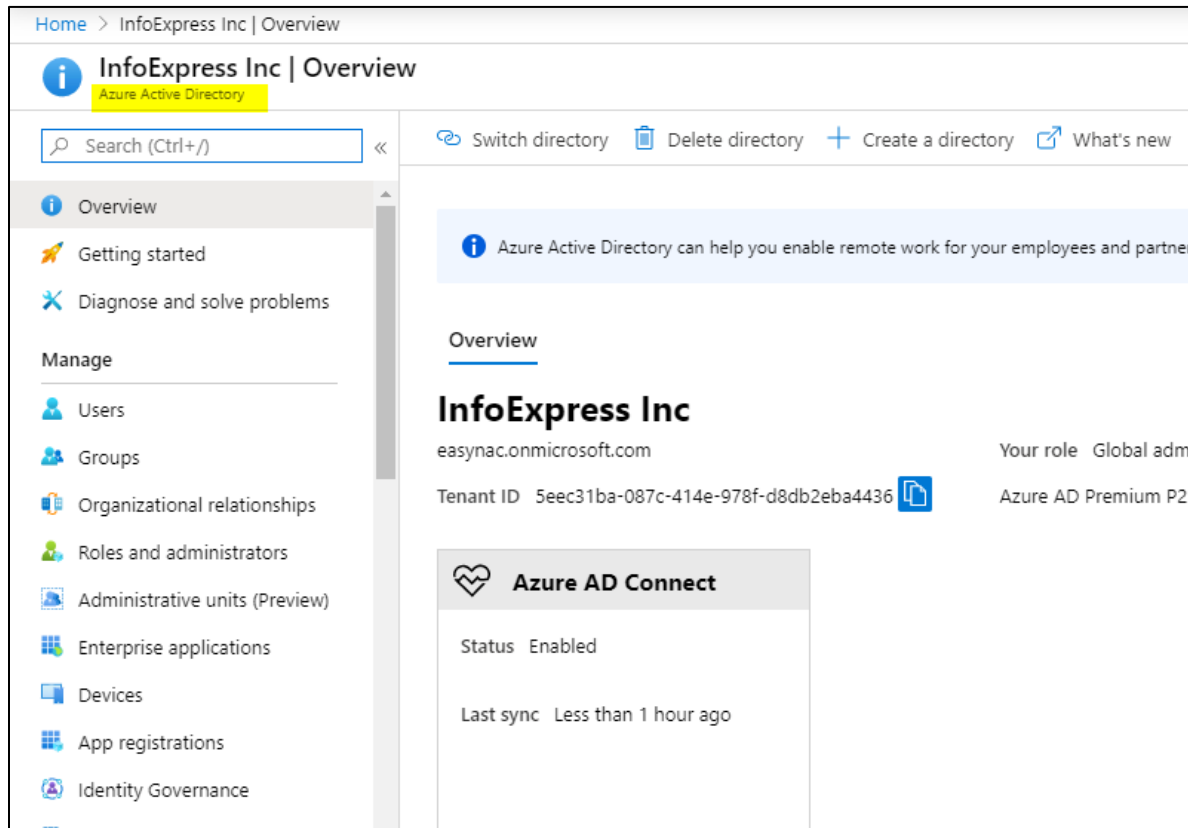
Tip: The patch-managed tag is helpful in expediting deployments. Any device that is being managed by the ManageEngine server can automatically be granted access to the network.

Microsoft Intune Integration

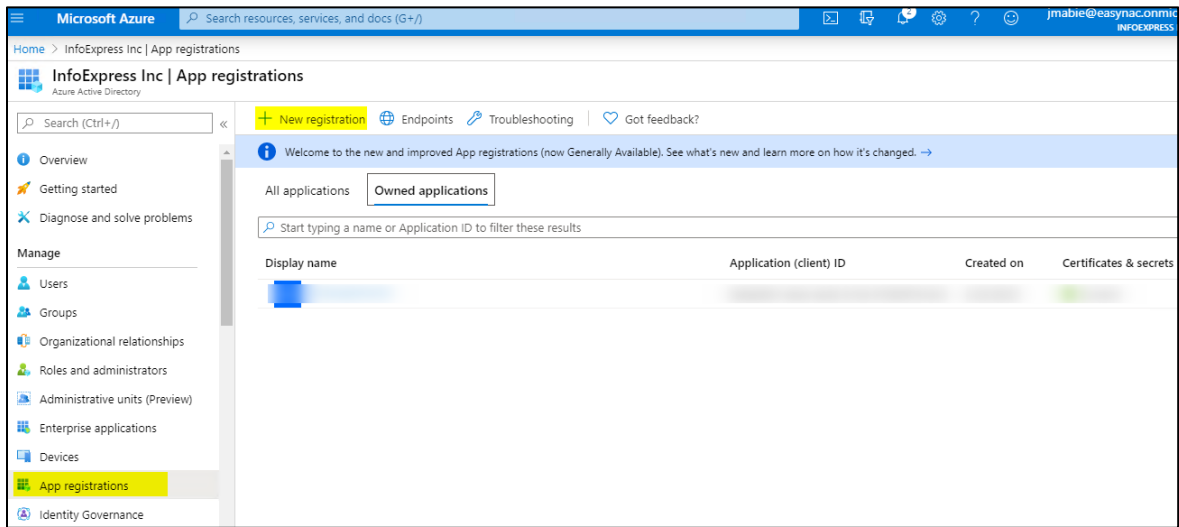
Integration with MS Intune requires an application be registered in MS Azure.

Step 1: Register a new application in Azure directory

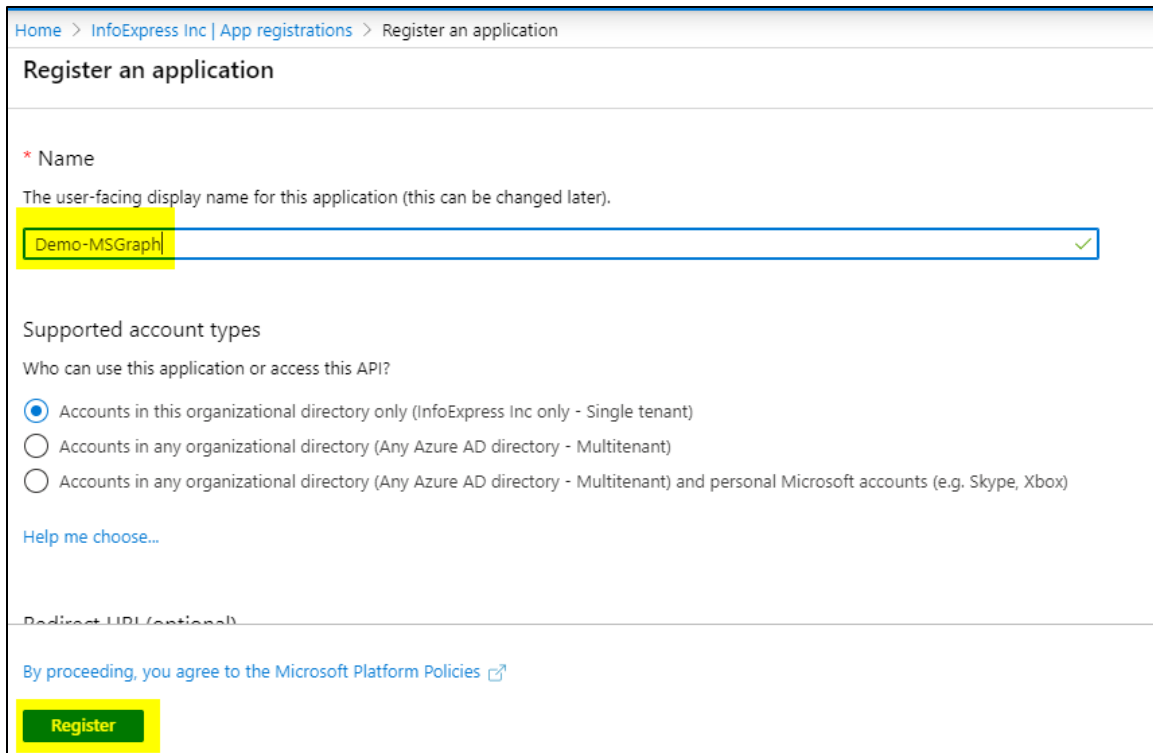
- Go to Azure Directory → App registration → New registration (Screen 1, 2 & 3)



Screen-1

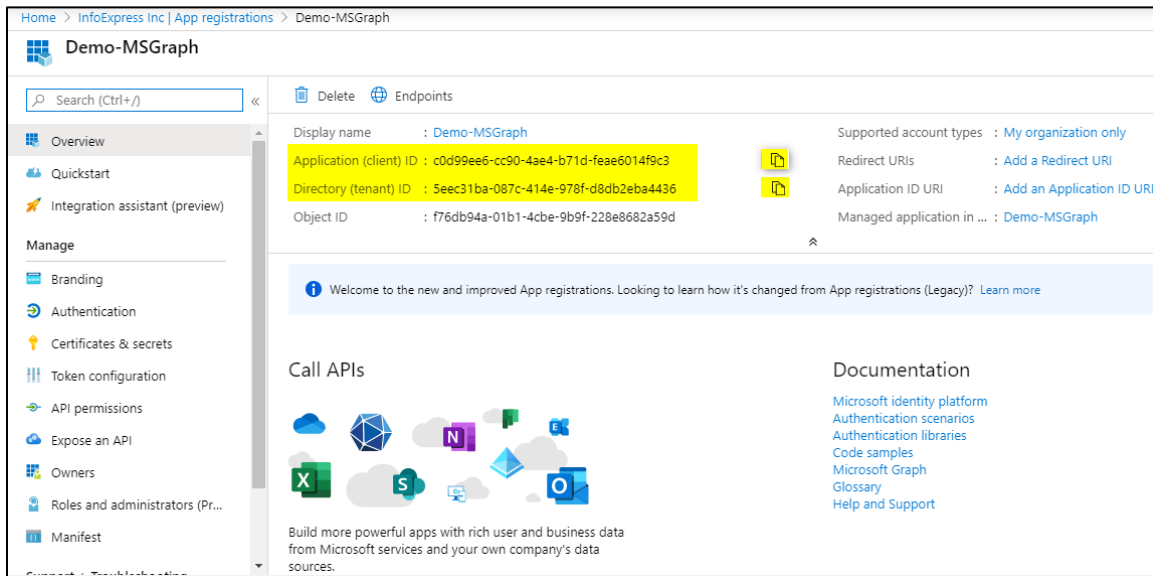


Screen-2

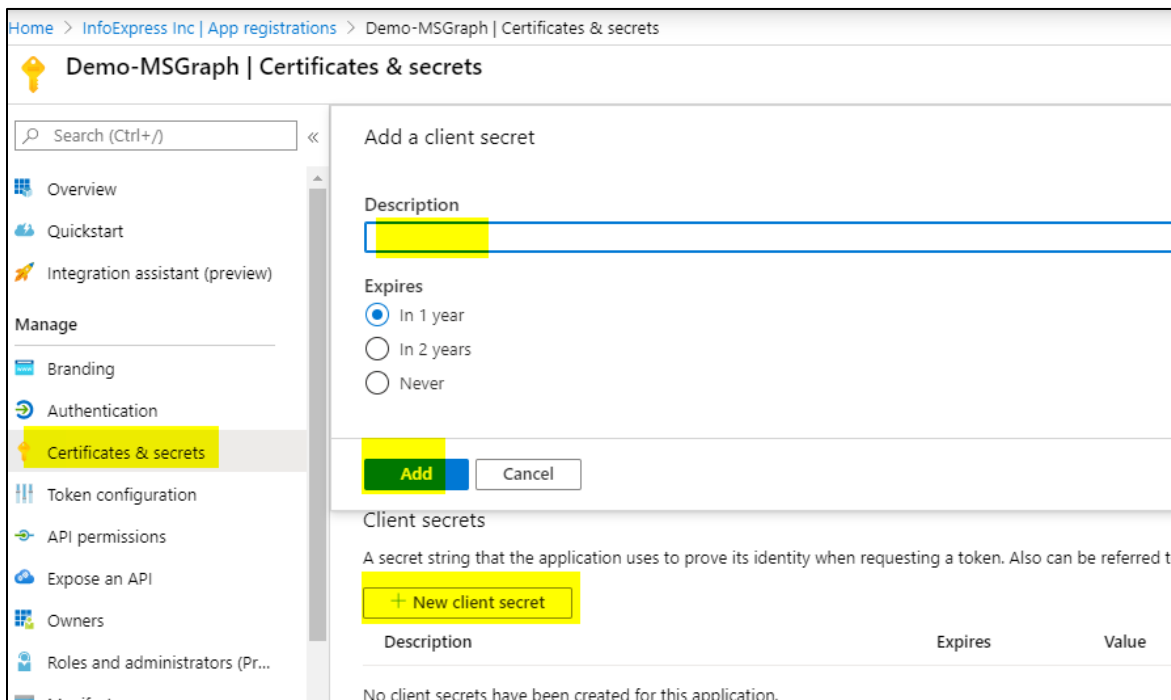


Screen-3

Step 2: Set Client secret and copy 'client ID', 'tenant ID' and 'client secret' (Screen 4, 5 & 6)



Screen-4

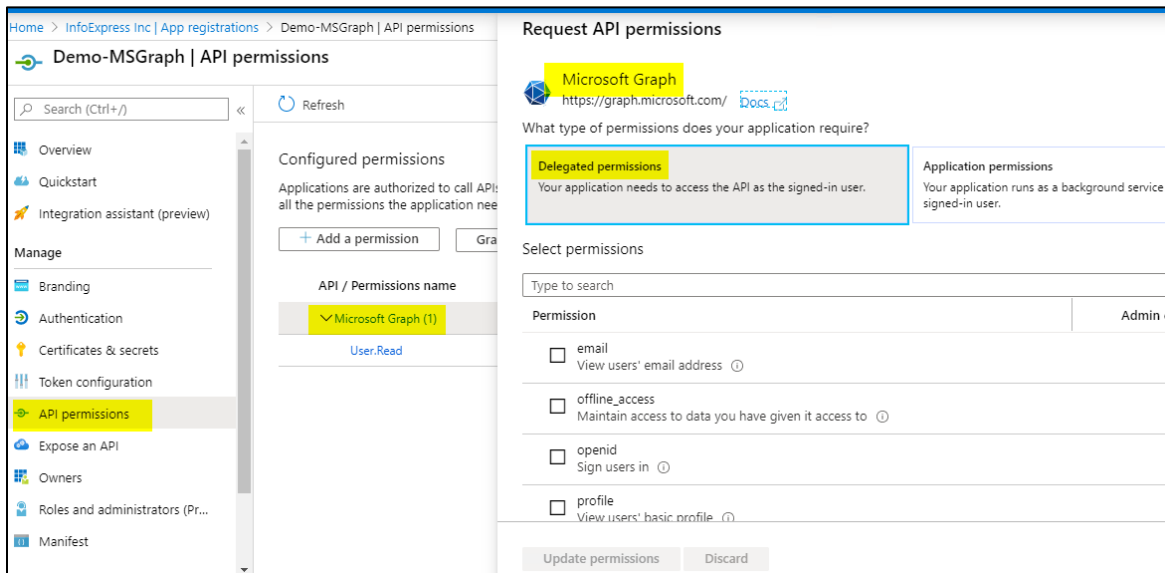


Screen-5



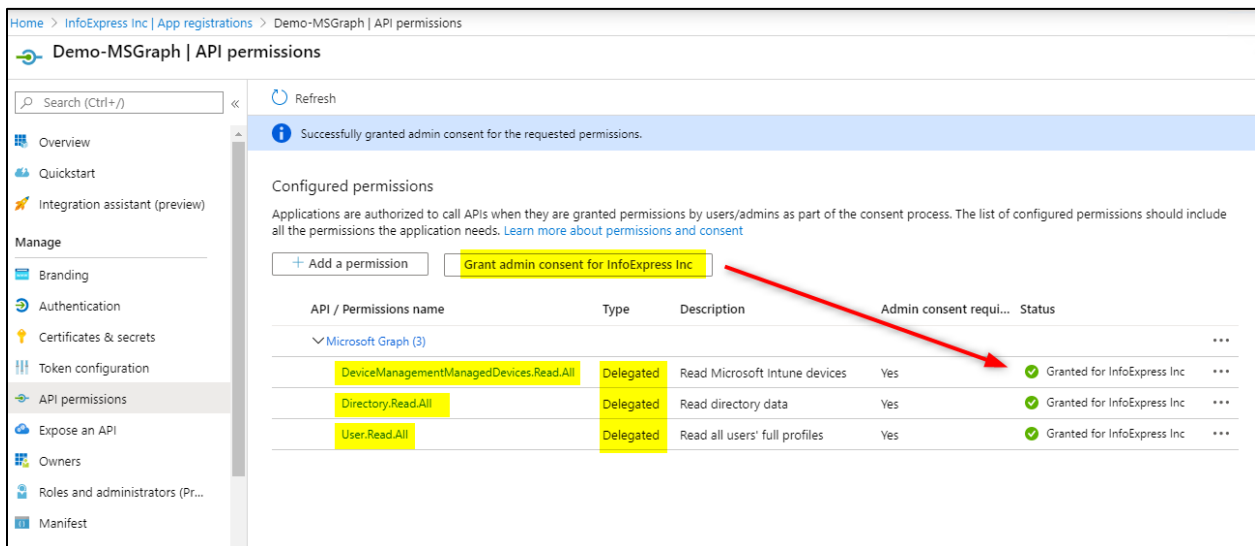
Screen-6

Step 3: Set API permissions as shown (Screen 7 & 8)



Screen-7

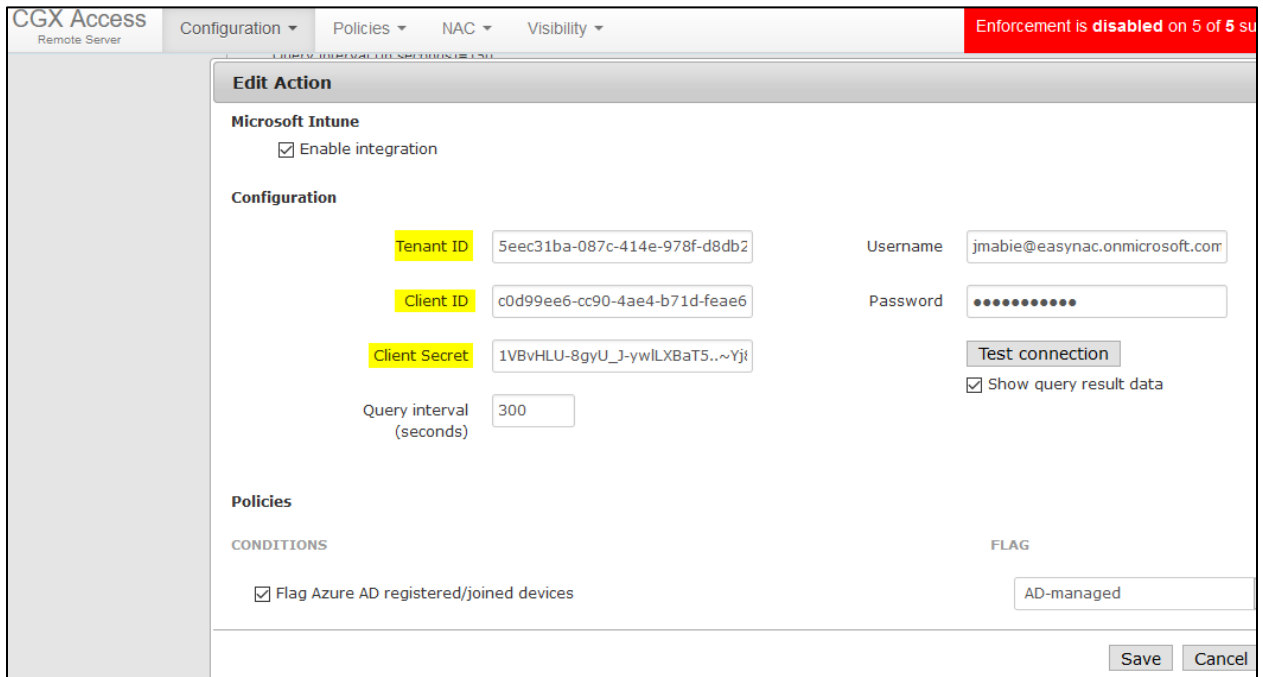
- Ensure permission name, type and Admin consent is granted for each permission



Screen-8

Step 4: Go to CGX Access → Configuration → Integration → Microsoft Intune.

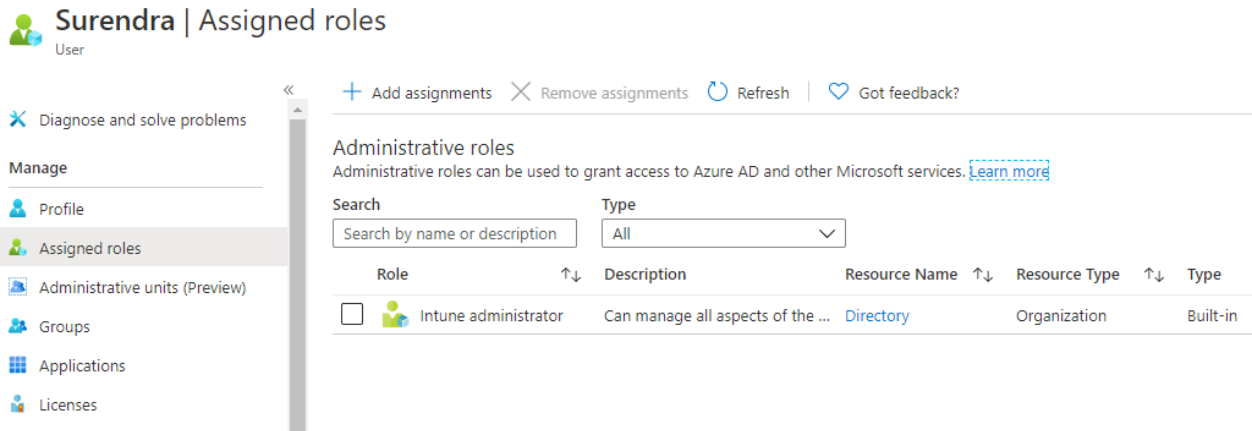
- Paste the required details, copied in step-2 above (Screen 9)



Screen-9

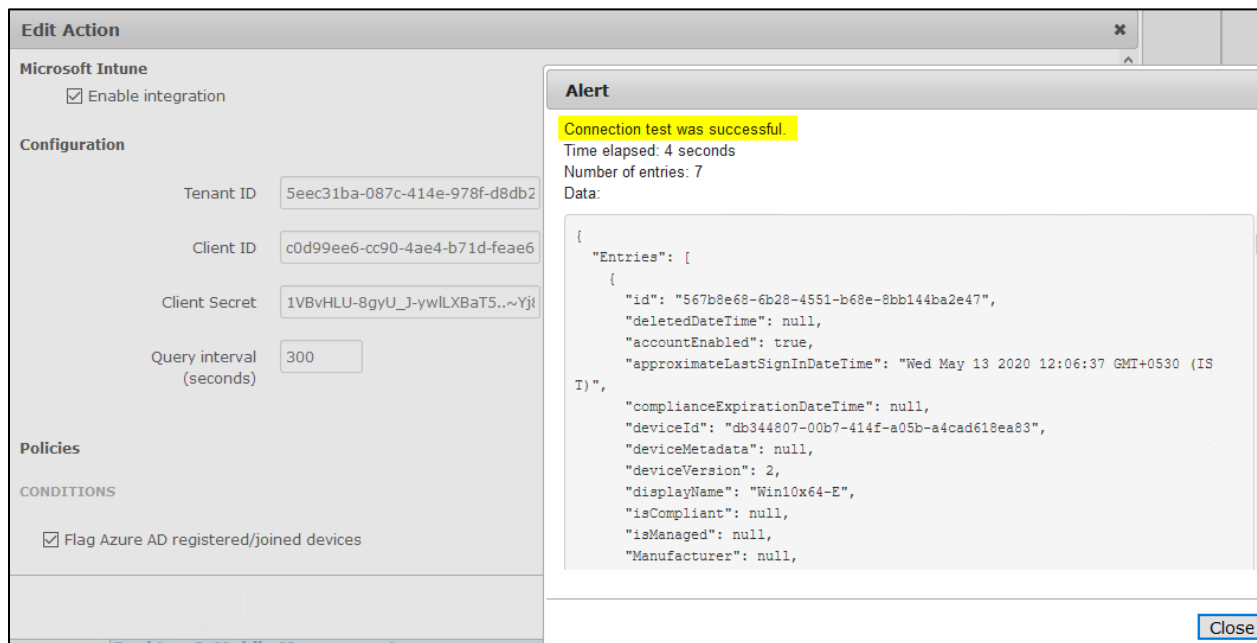
- Input Azure credentials – Account must have a role of "Intune Administrator (Screen 10)

[Home](#) > [Microsoft Intune](#) > [Users | All users](#) >



Screen-10

- Use "Test connection" button to validate settings and connectivity (Screen-11)



Screen-11

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and MS Intune have been successfully tested, policies can be set to enforce endpoint devices have been enrolled and compliant with Intune device compliance policy.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies	
CONDITIONS	FLAG
<input checked="" type="checkbox"/> Flag Azure AD registered/joined devices	<input type="text" value="AD-managed"/>
<input checked="" type="checkbox"/> Flag managed devices	<input type="text" value="managed-device"/>
<input checked="" type="checkbox"/> Flag non-compliant managed devices	<input type="text" value="non-compliant"/>

When selected CGX Access will set tags and automatically grant access to devices being managed by MS-Intune. While devices out of compliance can be tagged as a non-compliant.







Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Activate

Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	  
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	  

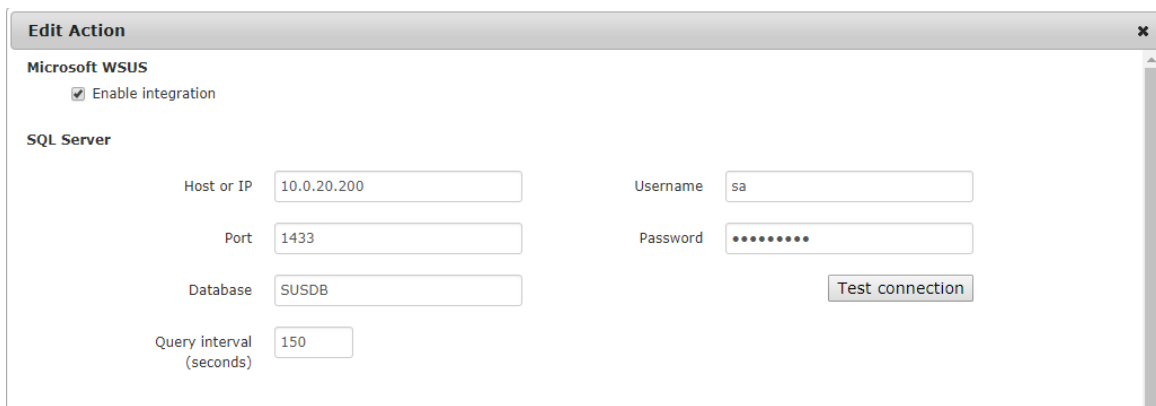
The policy above shows a device will be assigned full-access if tagged as AD-Managed or managed-device. However, it would be given a non-compliant role if it has been tagged as a non-compliant. The order of the rules is important, as they are evaluated in descending order.

Note: The AD-Managed tag is applied to both Azure AD-joined devices and AD registered devices. While the managed-device tag is only applied to Azure AD-joined devices.

Microsoft SCCM \ WSUS Integration

CGX Access communicates with the WSUS server by querying the SQL database. By default, WSUS uses the Windows Internal Database, so it may be necessary to first update the WSUS server to use SQL. See WSUS SQL prerequisites below.

- In CGX Access GUI go to Configuration → Integration
- Select the “Microsoft WSUS”



- Check “Enable Integration”
- Enter Hostname or IP / database port / database name
- Enter Username / Password to connect to database
- Use "Test connection" button to validate settings
- Save changes

WSUS SQL Prerequisites:

- By default, WSUS uses the Windows Internal Database. For integration with CGX Access, it is required to use an SQL database.
- Verify the MS SQL Server on the WSUS server was enabled for TCP/IP and specify a port such as 1433.
- Configure the firewall on the WSUS server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your WSUS Server.

Setting and Enforcing Patch Compliance Policies

Once the communications between the CGX Access appliance and WSUS server have been successfully tested, policies can be set to enforce compliance with patch policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

- Flag devices enrolled in Microsoft WSUS
- Flag devices that have not reported in days
- Flag devices with failed updates greater than days
- Flag devices with pending updates greater than days
- Flag devices with updates with errors greater than
- Flag devices with updates needed greater than
- Flag devices with updates with no status greater than

FLAG

-
-
-
-
-
-
-

There are several conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Activate
Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Patch Non-Compliance (agent-less checks) Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant - Device is NOT compliant with the corporate patch management policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The policy above shows a device will be assigned a non-compliant role if it has been tagged as patch-pending or patch-failed. The order of the rules is important, as they are evaluated in descending order.

Tip: The patch-managed tag is helpful in expediting deployments. Any device that is being managed by the WSUS server can automatically be granted access to the network.

Microsoft Windows Management Instrumentation (WMI)

CGX Access can query endpoints directly using Windows Management Instrumentation (WMI). WMI allows for Windows endpoints and Windows Servers to be queried over the network for compliance requirements.

- In CGX Access GUI go to Configuration → Integration
- Select the “Microsoft WMI”

Edit Action

Microsoft Windows Management Instrumentation (WMI)

Enable integration

Domain Admin Account: iex\administrator

Query interval (seconds): 14400

Password: [masked]

Test Device: 192.168.253.54

Test connection

Policies

CONDITIONS	FLAG
<input checked="" type="checkbox"/> Flag devices manageable by WMI	managed-device
<input type="checkbox"/> Verify device is domain joined	
<input checked="" type="checkbox"/> Flag devices with local account login	local-login

Save **Cancel** **Help**

- Check “Enable Integration”
- Enter Username and Password

The account requires permissions to perform WMI queries on client computers. A Domain Admin Account is often necessary. Use domain\username syntax for the Domain Admin account.

- Use "Test connection" button to validate settings

Alert

WMI test passed successfully.

Query result:

Name:	Microsoft Windows 7 Professional
CSName:	MANAGED01
Build Number:	7601

Close

- Save changes

WMI Troubleshooting:

Windows contains a number of security features that may prevent the use of WMI on a remote system. Therefore, it may be necessary to modify your system's Active Directory and Windows Firewall settings for WMI to work.

As WMI is a pre-installed component on Microsoft Operating systems, it's recommended you use Microsoft resources from troubleshooting WMI on your network.

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista>

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and endpoint devices have been successfully tested, policies can be set to detect compliance with policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

- Flag devices manageable by WMI
 - Verify device is domain joined
- Flag devices with local account login
- Flag devices with AV installed
- Flag devices with no AV installed
- Flag devices with inactive on-access scanner
- Flag devices with old AV-signatures
- Flag devices with personal firewall off
- Flag devices with running process

dropbox.exe, onedrive.exe, googledrivesync.exe

- Flag devices without running process

bdagent.exe

FLAG

managed-device

local-login

AV-managed

No-AV

AV-off

AV-out-of-date

FW-off

non-compliant

non-compliant

There are several conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.







Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Activate

Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	  
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	  

The policy above shows a device will be assigned a non-compliant role if it has been tagged as AV-Off or non-compliant. The order of the rules is important, as they are evaluated in descending order.

Configuring ACLs for WMI access

When a device has full access or enforcement is disabled, WMI remote queries should always work. However, when a device is quarantined, it would be necessary for the endpoint device to be able to communicate with the AD server to validate the WMI query.

Below is a sample ACL that should be assigned when a device is out of compliance to allow the WMI query to work. In this example, the AD server has IP address 192.169.253.100.

```
ALLOW WHEN PROTO=='UDP' AND PORT==53
ALLOW WHEN PROTO=='TCP' AND PORT==53
ALLOW WHEN PROTO=='UDP' AND PORT==67
ALLOW WHEN PROTO=='TCP' AND PORT==67
ALLOW WHEN ADDR=="192.168.253.100"
HTTPREDIRECT(RemediatePortal)
DENY WHEN TRUE
```

The ACL example below should be used if DNS Redirection is also required. In this example the AD server has FQDN host name: WIN-EH9KPK2TKSH.iex.demo with IP address 192.168.253.100

```
ALLOW WHEN PROTO=='TCP' AND PORT==67
ALLOW WHEN ADDR=="192.168.253.100"
DNSALLOW WHEN DNSTYPE==33
DNSALLOW WHEN HOSTNAME=="WIN-EH9KPK2TKSH.iex.demo"
DNSREDIRECT(RemediatePortal)
DENY WHEN TRUE
```

Moscii StarCat Integration

In CGX Access GUI go to Configuration → Integration

- Select “Moscii StarCat”

The screenshot shows the 'Edit Action' window for Moscii StarCat integration. The window title is 'Edit Action'. Below the title bar, the text 'Moscii StarCat' is displayed, followed by a checked checkbox for 'Enable integration'. A red rectangular box highlights the 'SQL Server' configuration section, which includes the following fields: 'Host or IP' (192.168.253.140), 'Port' (1433), 'Database' (StarCat), 'Username' (SA), 'Password' (masked with asterisks), and 'Query interval (seconds)' (150). A 'Test connection' button is located to the right of the Password field. Below the SQL Server section is the 'Policies' section, which is divided into 'CONDITIONS' and 'FLAG'. Under 'CONDITIONS', there are two checked checkboxes: 'Flag devices enrolled in Moscii StarCat' and 'Flag devices that have not connected in the past' (with a value of 7 days). Under 'FLAG', there are two dropdown menus: 'managed-device' and 'stale-device'. At the bottom right of the window are three buttons: 'Save', 'Cancel', and 'Help'.

- Check “Enable Integration”
- Enter Hostname or IP / database port / database name
- Enter Username / Password to connect to database
- Use "Test connection" button to validate settings
- Save changes

StarCat SQL Prerequisites:

- Verify the MS SQL Server on the StarCat server was enabled for TCP/IP and specify a port such as 1433.
- Use MS SQL Server management studio to create an account with permission to read the StarCat database. StarCat 2013 doesn't use a default database name, so check the SQL server for the correct name.
- Configure the firewall on the StarCat server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your StarCat server.

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and StarCat server have been successfully tested, policies can be set to enforce all Windows devices have been installed with the StarCat agent and connecting to the server regularly.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policies

CONDITIONS

Flag devices enrolled in Moscil StarCat

Flag devices that have not connected in the past days

FLAG

managed-device

stale-device

When selected CGX Access will set tags and automatically grant access to devices being managed by StarCat. While devices that have not connected in the past x days can be tagged as a stale-device.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The policy above shows a device will be assigned full-access if tagged as managed-device. However, it would be given a non-compliant role if it has been tagged as a stale-device. The order of the rules is important, as they are evaluated in descending order.

Tip: The managed-device tag is helpful in expediting deployments. Any device that is being managed by the StarCat server can automatically be granted access to the network.

Okta Integration

- In CGX Access GUI go to Configuration → Integration
- Click on "Okta"
- Check "Enable Integration"
- Enter Access URL and API Key

Edit Action

Okta Integration

Enable integration

Server Configuration

Access URL:

Api Token: Show query result data

Query Interval (Seconds):

Policy

CONDITION

Tag devices running Okta Verify

Tag devices with Encryption disabled

TAG

The Access URL is the same as Okta organization URL

The API key can be created by logging into Okta with Admin privileges: Okta → Security → API → Token

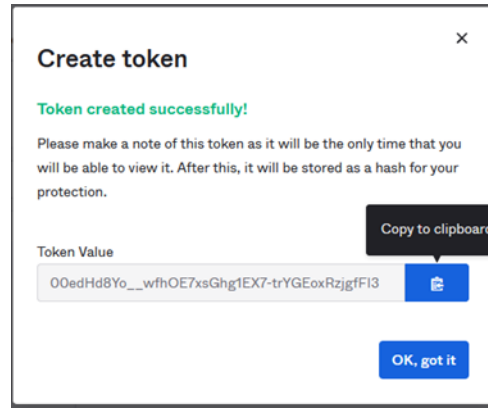
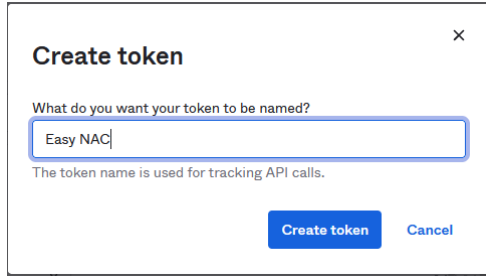
1. Click Create Token

API [Help](#)

Authorization Servers **Tokens** Trusted Origins

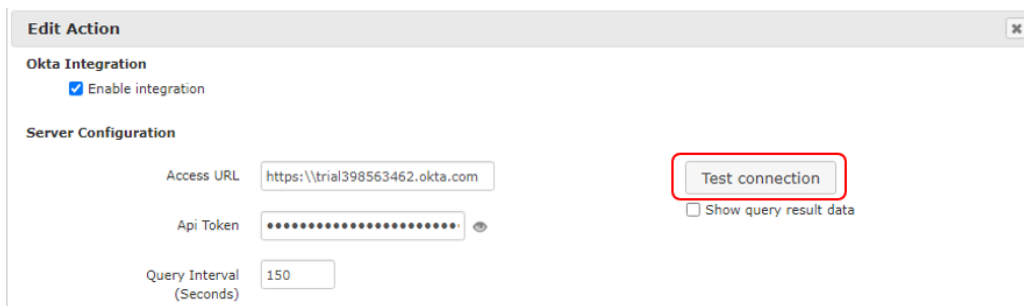
Token value Search by

Token types	Token name	Created	Expires	Last used	Actions
All	0				



2. Copy token to clipboard and paste to CGX Access

- Use "Test connection" button to validate settings



- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Note: The API token has a 30 days expiry time. This value cannot be changed. However, if the token is used, the expiration timer is reset each time so the token will remain available.

Setting and Enforcing Patch Compliance Policies

Once the communications between the CGX Access appliance and Okta have been successfully tested, policies can be set to auto detect devices running Okta Verify. Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION

- Flag devices running Okta Verify
- Flag devices with Encryption disabled

FLAG

managed-device

drive-encryption-off

When enabled, tags will automatically be set on specific devices that meet or fail the conditions. Auto Trust Policy will reference these tags to set the appropriate access for the devices.

Palo Alto Cortex XDR Integration

- In Cortex XDR management console go Settings → Configurations → Integrations → API Keys
- Click “+ New Key” button

Generate API Key

General

Security Level

Advanced
API key must be hashed with nonce and timestamp (suitable for proprietary scripts and intended to prevent replay attacks).

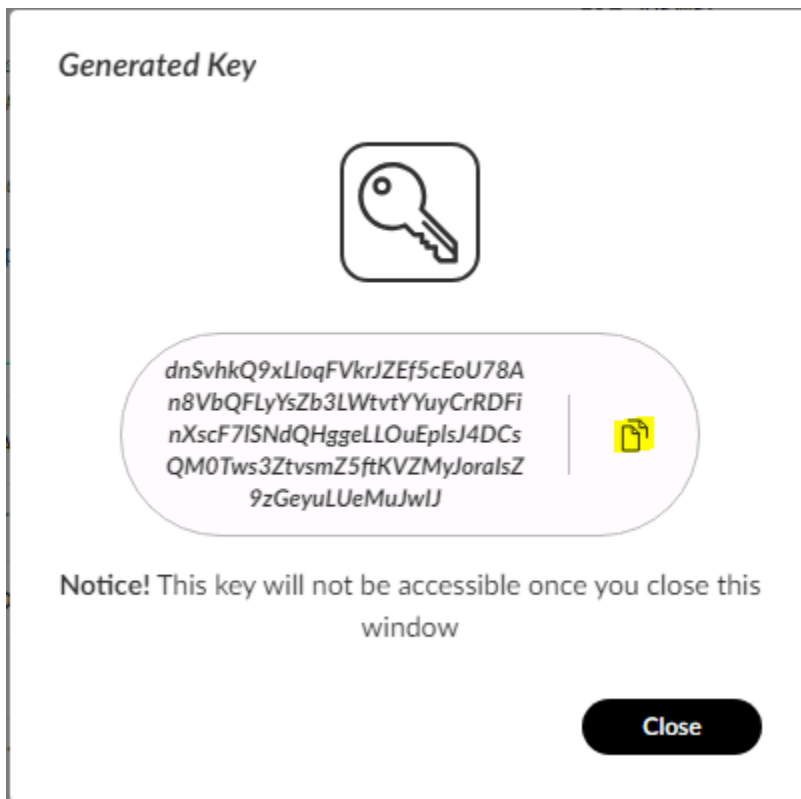
Standard
API key can be used as-is (suitable for curl).

Enable Expiration Date

Role
Viewer

Comment
Easy NAC integration

- Select a Standard Security Level and select Viewer Role
- Click Save to generate API key
- Copy API Key



- In CGX Access GUI go to Configuration → Integration
- Click on "Cortex XDR" Integration"
- Check "Enable Integration" and paste the API Key

Edit Action

EARLY RELEASE

Cortex XDR Integration

Enable integration

Server Configuration

Access URL

API Key ID

API Key

Query Interval (Seconds)

Test connection

Show query result data

Use the hostname for finding and flagging devices

- Return the Cortex XDR Management screen and copy the API URL, and take note of the API ID

API Keys Found 5 results

+ New Key Copy API URL

<input type="checkbox"/>	CREATION TIME	ID	CREATED BY	COMMENT	SECURITY LEVEL	ROLE	EXPIRATION
<input type="checkbox"/>	Oct 29th 2023 15:41:24	15	Jonathan Mabie	Easy NAC integration	Standard	Viewer	Never

- Return to CGX Access GUI and paste the API URL and type to API ID value

Edit Action

EARLY RELEASE

Cortex XDR Integration

Enable integration

Server Configuration

Access URL

API Key ID

API Key

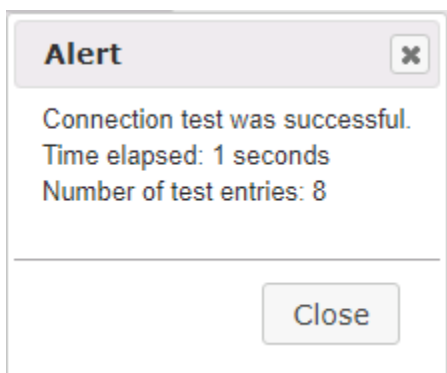
Query Interval (Seconds)

Test connection

Show query result data

Use the hostname for finding and flagging devices

- Use "Test connection" button to validate settings



- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and Cortex XR have been successfully tested, policies can be set to enforce compliance with policies.

Select the Tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION	TAG
<input checked="" type="checkbox"/> Tag devices running Cortex XDR Agent	XDR-managed
<input checked="" type="checkbox"/> Tag devices that are offline	Sensor-offline
<input checked="" type="checkbox"/> Tag devices with Cortex XDR protection disabled	Sensor-off
<input checked="" type="checkbox"/> Tag Cortex XDR isolated device	infected
<input checked="" type="checkbox"/> Tag devices that have not been reported in <input type="text" value="7"/> days	Sensor-stale
<input checked="" type="checkbox"/> Tag devices that have not updated in <input type="text" value="90"/> days	Sensor-out-of-date







There are multiple conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust policies, devices with specific tags can be assigned different roles.

Auto Trust Policy

Activate

Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	 
XDR Sensor offline Has any of these tags: Sensor-offline Device's last DHCP broadcast request more than 5 minutes ago	Set role to non-compliant - XDR Sensor is not connected	 
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	 

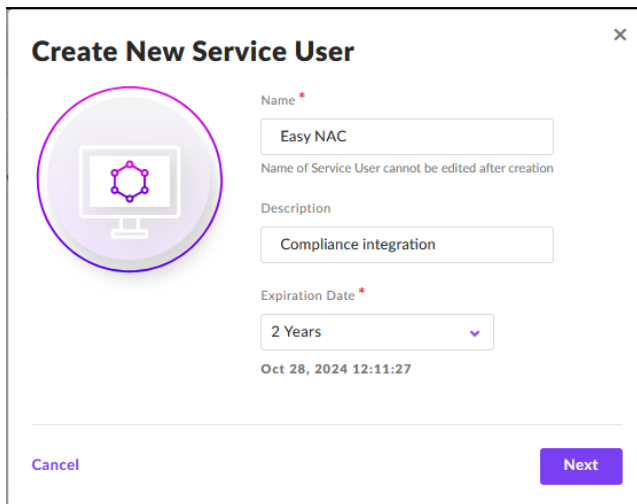
The example above shows a device will be assigned a non-compliant role if it has been tagged as sensor-stale, Sensor-out-of-date, or Sensor-offline, or Sensor-off. The order of the rules is important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The Sensor-offline tag may not be set when a device 1st joins the network, as the device may be just starting up, and not connected to the server. To avoid an initial restriction, a recent DHCP request condition can be used to provide the endpoint a 5-minute grace period. The grace period should be at least 1 minute longer than the configured query interval.

Tip: The XDR-managed tag is helpful in expediting deployments. Any device that is being managed by the organization's Cortex XDR deployment can automatically be trusted on the network.

SentinelOne Integration

- In SentinelOne management console go Settings → Users → Service Users
- Create a New Service User

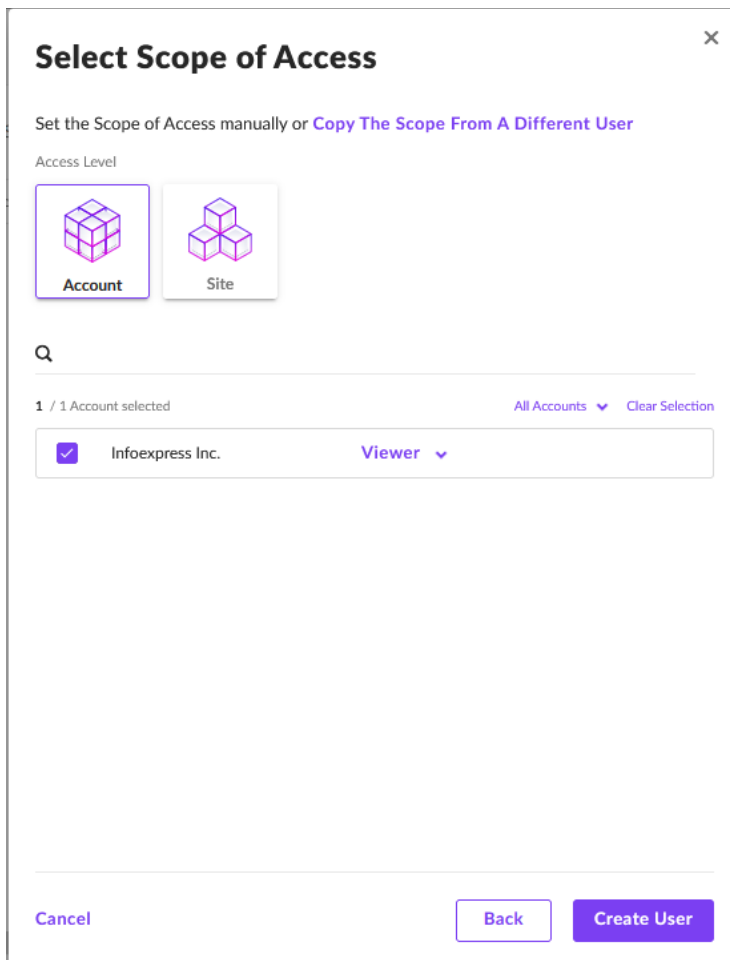


The screenshot shows a modal window titled "Create New Service User". On the left is a circular icon with a computer monitor and a network diagram. The form fields are as follows:

- Name:** "Easy NAC" (with a red asterisk indicating a required field). Below the input is the text: "Name of Service User cannot be edited after creation".
- Description:** "Compliance integration".
- Expiration Date:** "2 Years" (selected from a dropdown menu). Below it is the date: "Oct 28, 2024 12:11:27".

At the bottom, there are two buttons: "Cancel" on the left and "Next" on the right.

- Select Appropriate Access Level



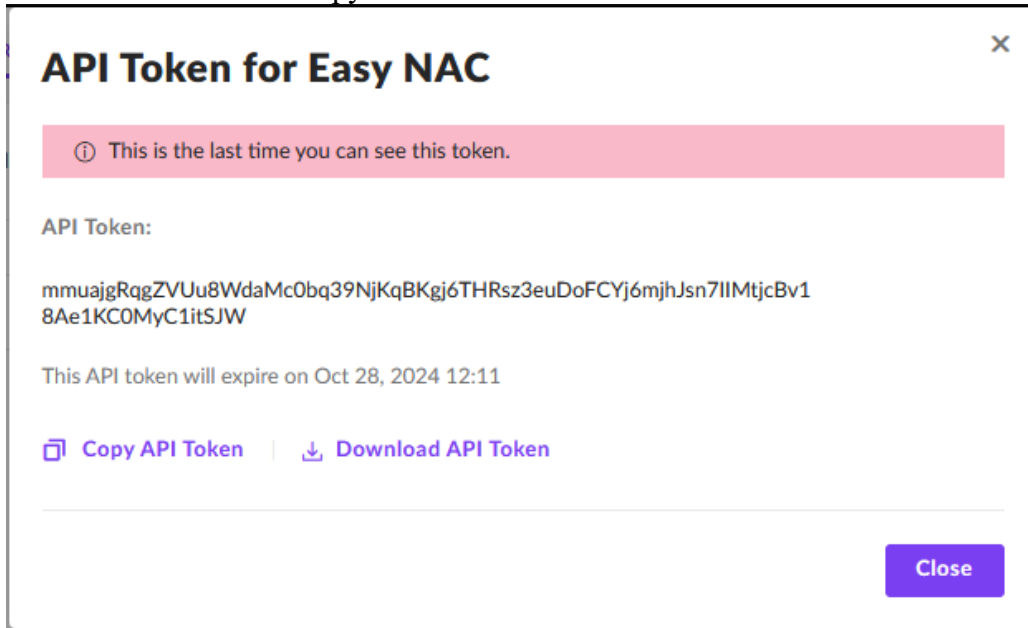
The screenshot shows a modal window titled "Select Scope of Access". It contains the following elements:

- Text: "Set the Scope of Access manually or [Copy The Scope From A Different User](#)".
- Access Level:** Two options are shown: "Account" (with a 3D cube icon) and "Site" (with a 3D cube icon).
- Search:** A search bar with a magnifying glass icon and the text "1 / 1 Account selected". To the right are links for "All Accounts" and "Clear Selection".
- Selection List:** A table with one row:

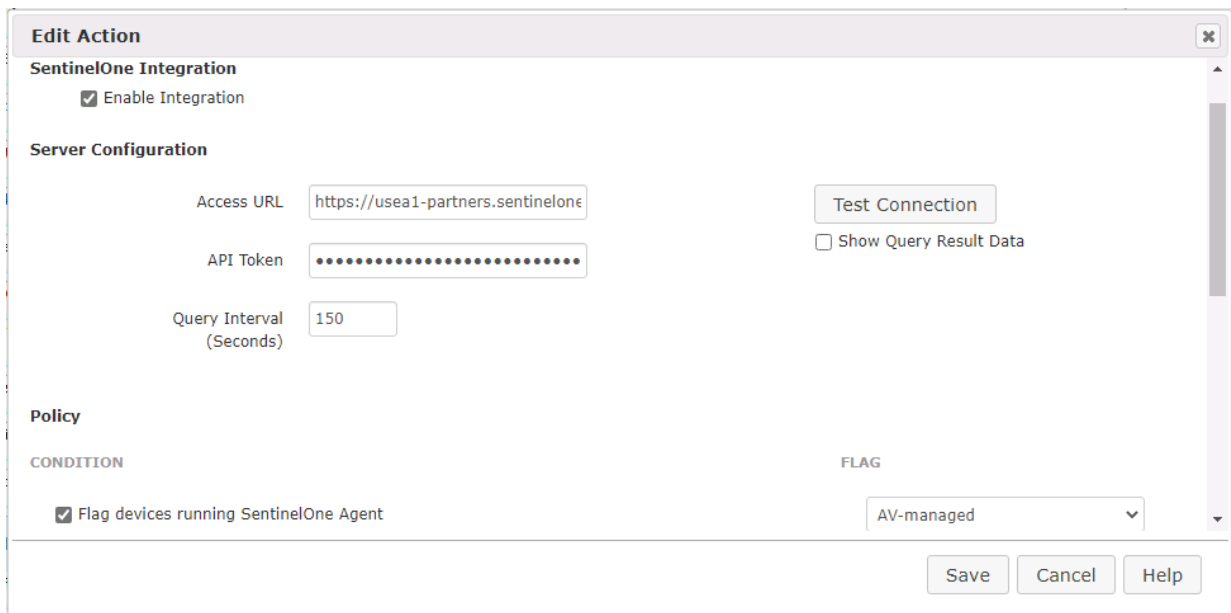
<input checked="" type="checkbox"/>	Infoexpress Inc.	Viewer
-------------------------------------	------------------	--------

At the bottom, there are three buttons: "Cancel" on the left, "Back" in the middle, and "Create User" on the right.

- Once API is created – Copy API Token



- In CGX Access GUI go to Configuration → Integration
- Click on "SentinelOne Integration"
- Check “Enable Integration” and paste the API Token
- Input the Access URL. It’s the same URL used by the SentinelOne management console



- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Compliance Policies

Once the communications between the CGX Access appliance and Sentinel One have been successfully tested, policies can be set to enforce compliance with policies. Select the tags that should be assigned to devices that meet or fail the specific conditions.

CONDITION	FLAG
<input checked="" type="checkbox"/> Flag devices running SentinelOne Agent	AV-managed
<input checked="" type="checkbox"/> Flag devices that are offline	AV-offline
<input checked="" type="checkbox"/> Flag devices that have not reported in <input type="text" value="7"/> days	AV-stale
<input checked="" type="checkbox"/> Flag devices with SentinelOne Agent out of date	AV-out-of-date
<input checked="" type="checkbox"/> Flag devices that are infected by malware	infected
<input checked="" type="checkbox"/> Flag devices with Apps Vulnerability not up to date	patch-pending
<input checked="" type="checkbox"/> Flag devices with Network Quarantine disabled	AV-Config
<input checked="" type="checkbox"/> Flag devices with Firewall disabled	FW-off
<input checked="" type="checkbox"/> Flag devices with Encryption disabled	drive-encryption-off

There are multiple conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

[Add Rule](#)

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
AV offline Has any of these tags: AV-offline Device's last DHCP broadcast request more than 5 minutes ago	Set role to non-compliant - AV is off-line	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-offline or AV-out-of-date. Rules are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the organization's SentinelOne deployment can automatically be trusted on the network.

Sophos Integration

Easy NAC supports integration with the on-premise Enterprise Console or the Sophos Central cloud version. Either option can be enabled individually or together to support a migration to the cloud.

Configuring Enterprise Console:

- In CGX Access GUI go to Configuration → Integration
- Select Sophos
- Check “Enable integration” and select the “Enterprise Console (SQL Server)”

The screenshot shows the 'Edit Action' dialog box for Sophos integration. It has a title bar with 'Edit Action' and a close button. Under the 'Sophos' section, there is a checked checkbox for 'Enable integration'. Below that is the 'Configuration' section, which contains a checked checkbox for 'Enterprise Console (SQL Server)'. This section is highlighted with a red rounded rectangle. It includes four input fields: 'Host or IP' with the value '192.168.253.100', 'Username' with the value 'sa', 'Port' with the value '1433', and 'Database' with the value 'Sophos540'. There is also a 'Password' field with masked characters. A 'Test connection' button is located to the right of the 'Database' field. Below the 'Enterprise Console' section is an unchecked checkbox for 'Sophos Central'. At the bottom, there is a 'Query interval (seconds)' field with the value '20'.

CGX Access communicates with the Sophos Enterprise Console by querying the SQL database.

- Setup the SQL Server used by Sophos to support SQL queries over TCP 1433. See below.
- Enter Hostname or IP / database port / database name
- Enter Username / Password to connect to database
- Use "Test connection" button to validate settings → Save changes

Sophos SQL Prerequisites:

- Configure the MS SQL Server on the Sophos server to enable TCP/IP and specify a port such as 1433
- Install and use MS SQL Server management studio to create an account with permission to read the Sophos DB
- Sophos uses different schemas. Check which schema/database name Sophos is using: Examples include: SOPHOS540 (Sophos EP 5.4), or SOPHOS521 (Sophos EP 5.2)
- Configure the firewall on the Sophos server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your Sophos Server.

Configuring Sophos Central:

- In Sophos Central go to System Settings → API Token Management
- Create an API Token for CGX Access

The screenshot shows the 'CGX Access' configuration page in Sophos Central. It includes a 'Renew' and 'Delete' button at the top right. Below is the 'API Token Summary' section with the following details:

Name	CGX Access
Expires	Dec 18, 2019
API Access URL	https://api3.central.sophos.com/gateway
Headers	x-api-key: jZAyz7gc9X7d3s3c30rCv91wNwa2HjWd6ZNxyKjs Authorization: Basic NmZlMzQxM2UtZTBhYy00ZGJkLTk0YjYtNzE4ZmY3N2Q2MDBlOkZDUTZPWUJFSUNDQ0JKVvFFN0tS1dJUDVQQU5SSFJUK2paQXI6N2djOVg3ZDNzM2MzT3JDdjkd053YTJlaldkNlp0eHlLanM=
API Access URL + Headers	url: https://api3.central.sophos.com/gateway, x-api-key: jZAyz7gc9X7d3s3c30rCv91wNwa2HjWd6ZNxyKjs, Authorization: Basic NmZlMzQxM2UtZTBhYy00ZGJkLTk0YjYtNzE4ZmY3N2Q2MDBlOkZDUTZPWUJFSUNDQ0JKVvFFN0tS1dJUDVQQU5SSFJUK2paQXI6N2djOVg3ZDNzM2MzT3JDdjkd053YTJlaldkNlp0eHlLanM=

Each of these fields has a 'Copy' button next to it. The 'Copy' button for the 'API Access URL + Headers' field is highlighted with a red box.

- Copy the API Access URL + Headers
- In CGX Access GUI go to Configuration → Integration
- Select Sophos
- Check “Enable integration” and Check the “Sophos Central”
- Place cursor in API field and right-click to paste the API Access URL + Headers

The screenshot shows the 'Edit Action' configuration page for Sophos Central. It includes the following sections:

- Sophos**: Enable integration
- Configuration**: Enterprise Console (SQL Server)
- Sophos Central**: Sophos Central

The 'API Access URL + Headers' field is highlighted with a blue box, and a context menu is open over it, showing options like 'Undo', 'Redo', 'Cut', 'Copy', 'Paste', and 'Paste as plain text'. The 'Paste' option is highlighted. A 'Test connection' button is visible to the right of the field.

- Test the Connection
- If test is successful, save changes
- If test is unsuccessful, check that the CGX Access appliance has access to the Sophos Cloud.

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and Sophos server have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

There are several conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↻ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

Symantec Endpoint Protection Manager - 14.x

- In CGX Access GUI go to Configuration → Integration
- Click on "Symantec Endpoint Protection Manager"
- Check "Enable Integration" and select 14.x
- Enter Hostname or IP / port
- Enter Username / Password to login to SEPM

The screenshot shows a dialog box titled "Edit Action" with a close button (X) in the top right corner. The main title is "Symantec Endpoint Protection Manager".

Integration Settings:

- Enable integration
- Version: 14.x (dropdown menu)

Configuration:

- Host or IP: 10.20.0.31 (text input)
- Port: 8446 (text input)
- Query interval (seconds): 150 (text input)
- Username: admin (text input)
- Password: [masked with dots] (password input)
- Domain: [empty] (text input)
- Test connection button

Policy:

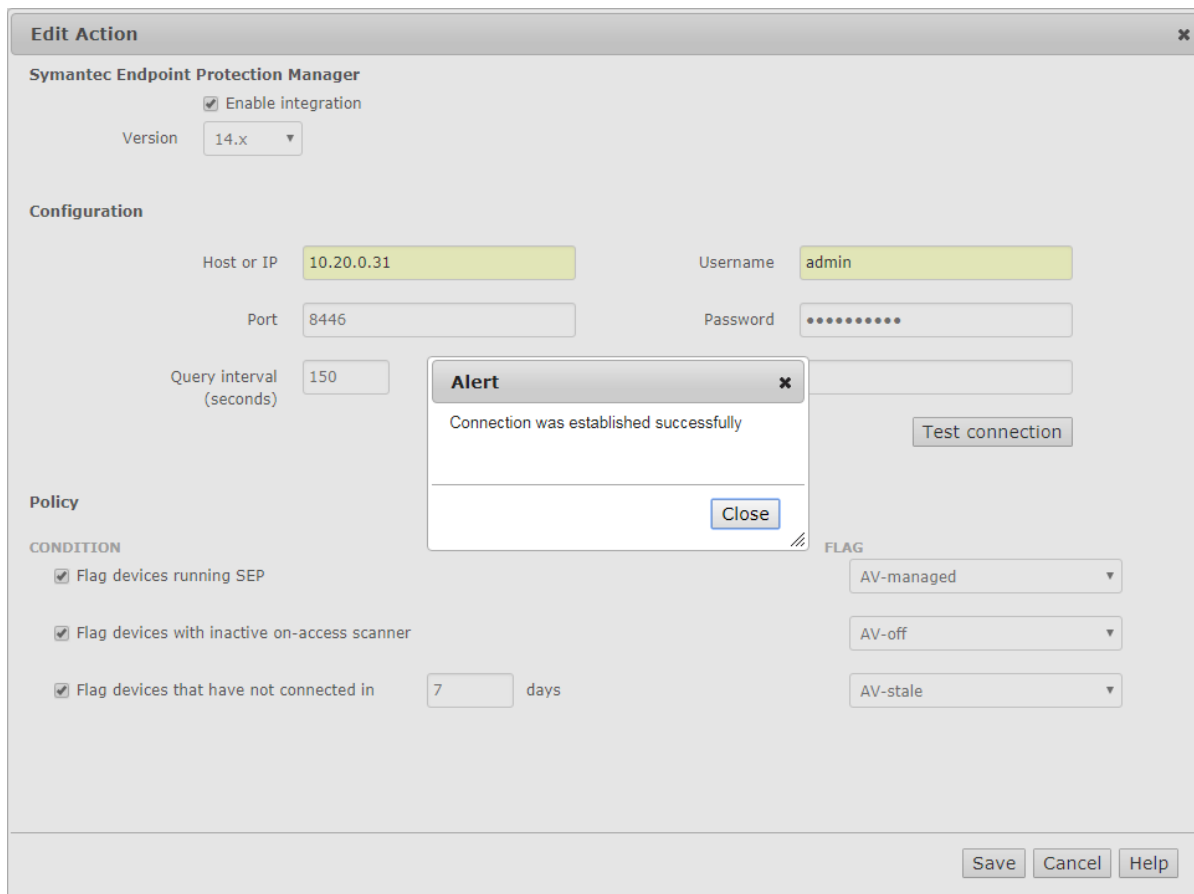
CONDITION

- Flag devices running SEP
- Flag devices with inactive on-access scanner
- Flag devices that have not connected in 7 days (text input)

FLAG

- AV-managed (dropdown menu)
- AV-off (dropdown menu)
- AV-stale (dropdown menu)

Buttons at the bottom: Save, Cancel, Help



- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and Symantec server have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION

- Flag devices running SEP
- Flag devices with inactive on-access scanner
- Flag devices with AV signature older than days
- Flag devices if Proactive Threat Protection is disabled
- Flag devices if Firewall is disabled
- Flag devices if Network Intrusion Prevention is disabled
- Flag devices if Browser Intrusion Prevention IE is disabled
- Flag devices if Browser Intrusion Prevention FF is disabled
- Flag devices if Memory Exploit Mitigation is disabled
- Flag devices if Tamper Protection is disabled

FLAG

-
-
-
-
-
-
-
-
-

There are several conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	<input type="button" value="🔍"/> <input type="button" value="📄"/> <input type="button" value="✖"/>
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	<input type="button" value="🔍"/> <input type="button" value="📄"/> <input type="button" value="✖"/>

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

Trend Micro Integration

Easy NAC supports integration with the on-premise enterprise console or the Apex Central cloud version. Either option can be enabled individually.

Configuring Enterprise Console:

- In CGX Access GUI go to Configuration → Integration
- Select the “Trend Micro”
- Check “Enable integration” and select the “On-premise” server type

The screenshot shows the 'Edit Action' dialog box for Trend Micro Integration. The 'Enable Integration' checkbox is checked. Under 'Server Configuration', the 'Server Type' is set to 'On-premise'. A red box highlights the 'Host or IP', 'Port' (1433), 'Database', 'Username', 'Password' (masked with dots), and 'Test Connection' button. Below the red box is a 'Query Interval (Seconds)' field set to 120. At the bottom, there are 'Policy' and 'CONDITION' labels, a 'FLAG' label, and 'Save', 'Cancel', and 'Help' buttons.

CGX Access communicates with Trend Micro by querying its SQL database.

- Setup the SQL Server used by Trend Micro to support SQL queries over TCP 1433. See prerequisites below.
- Enter Hostname or IP / database port / database name
- Enter Username / Password to connect to database
- Use "Test connection" button to validate settings
- Save changes

Apex One SQL Prerequisites:

- For integration with CGX Access, it is required to use an SQL database. If SQL is not in use, Trend Micro provides a migration tool to make this easy: <https://success.trendmicro.com/solution/1059973-migrating-officescan-osce-server-database-to-an-sql-server>
- Verify the MS SQL Server on the OCSE server was enabled for TCP/IP and specify a port such as 1433.

- Configure the firewall on the APEX One server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your Apex One Server.

Configuring APEX Central:

- In Apex Central, use Automation API Access Settings to generate an Application ID and API Key
- In CGX Access GUI go to Configuration → Integration
- Select Trend Micro
- Check “Enable integration” and select the “APEX Central”
- Add Host or IP address
- Copy the Application ID and API Key to CGX Access

The screenshot shows a window titled "Edit Action" for "Trend Micro Integration". The "Enable Integration" checkbox is checked. Under "Server Configuration", the "Server Type" dropdown is set to "Apex Central". Below this, there are input fields for "Host or IP", "Port" (with the value "443"), "Application ID", and "API key". A "Test Connection" button is located below the "API key" field, and a "Show Query Result Data" checkbox is below it. The "Query Interval (Seconds)" is set to "120". At the bottom, there are "Save", "Cancel", and "Help" buttons. The "Policy" section is partially visible at the bottom, showing "CONDITION" and "FLAG" headers.

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and Trend Micro server have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION

- Flag devices running Apex One Security Agent
- Flag devices that Apex One Security Agent is offline
- Flag devices with inactive on-access scanner
- Flag devices with AV signature more than days old
- Flag devices that have not connected in days

FLAG

-
-
-
-
-

There are multiple conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Note: when using APEX central, they may be less options, due to Trend Micro's API limitations.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

⌂ Activate ⌂ Cancel Changes

[Add Rule](#)

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
AV offline Has any of these tags: AV-offline Device's last DHCP broadcast request more than 5 minutes ago	Set role to non-compliant - AV is off-line	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off, AV-out-of-date or AV-offline. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

Trellix ePolicy Orchestrator Integration

- In CGX Access GUI go to Configuration → Integration
- Select the “Trellix ePolicy Orchestrator”

Edit Action

Trellix ePolicy Orchestrator Integration

Enable Integration

Server Configuration

Host or IP: 10.20.0.95 Username: SA

Port: 1433 Password:

Database: ePO2k8R2SP1-IE10 Test Connection

Query Interval (Seconds): 150

Policy

CONDITION

Tag devices running ePO Agent

Tag devices with inactive on-access scanner

TAG

AV-managed

AV-off

Save Cancel Help

CGX Access communicates with the ePolicy Orchestrator by querying its SQL database.

- Setup the SQL Server used by ePO to support SQL queries over TCP 1433; See below.
- Check “Enable Integration”
- Enter Hostname or IP / database port / database name
- Enter Username / Password to connect to database
- Use "Test connection" button to validate settings → Save changes

ePO SQL Prerequisites:

- Configure the MS SQL Server on the ePO server to enable TCP/IP and specify a port such as 1433
- Configure the firewall on the ePO server to allow CGX Access to communicate with the MS SQL Server port: 1433

Tip: It may be helpful to search, “how to enable remote connections on SQL version...” referencing the specific version used by your ePO Server.

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and ePO SQL server have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITIONS	FLAG
<input checked="" type="checkbox"/> Flag devices running ePO Agent	AV-managed
<input checked="" type="checkbox"/> Flag devices with inactive on-access scanner	AV-off
<input type="checkbox"/> Flag devices that Endpoint Security Web Control is not installed	web-control-off
<input type="checkbox"/> Flag devices that Drive Encryption is not installed	drive-encryption-off
<input type="checkbox"/> Flag devices that Data Loss Prevention is not installed	DLP-off
<input checked="" type="checkbox"/> Flag devices with AV signature older than <input type="text" value="10"/> days	AV-out-of-date
<input checked="" type="checkbox"/> Flag devices that have not connected in <input type="text" value="7"/> days	AV-stale

There are seven conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions.

Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	⊙ ↻ ✕
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	⊙ ↻ ✕


The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

Webroot Integration

- In Webroot web management go to Settings → Unity API Access → New
- Create New Client Credential
 - The Event notification API will not be used

CREATE NEW CLIENT CREDENTIAL



Do you plan to use the event notification API?
Notification API allows you to subscribe to a set of events on different domain levels, and receive related notifications in near real-time (for example WebThreatShield.UrlAction or Endpoint.FileDetection).

Yes

No

[Cancel](#) [Previous](#) [Next](#)

CLIENT CREDENTIAL RECORD

Important! This is the client identifier and the client secret for the client credential record listed below. The client secret is not persisted and it is your responsibility to remember the client secret and treat it as sensitive information. If you lose the client secret you need to generate a new secret in order to continue using the affected client identifier in your application.

Name
Easy NAC

Description
Integration with Webroot and Easy NAC

Client ID
client_YAIIWKX@infoexpress.com

Client Secret
EN;ht11*Fa3#9?y

! Please make note of your client secret

[I Have Made Note Of The Client Secret](#)

- Once created – Copy Client ID and Client Secret key

- In CGX Access GUI go to Configuration → Integration
- Click on "Webroot"
- Check "Enable Integration"
- Paste Client ID and Client Secret key from above steps
- Enter details:
 - **Access URL:** <https://unityapi.webrootcloudav.com>
 - Username and password used to authenticate to the Webroot Management Console
 - **Key Code** – Use Webroot Key Code under Settings → Downloads

Note: Don't use Parent Keycode – Connection would be successful but no results will be retrieved

- Use "Test connection" button to validate settings
- You may leave Query interval and tagging conditions as default or modify as required
- Save this configuration

Setting and Enforcing Anti-Virus Compliance Policies

Once the communications between the CGX Access appliance and Webroot API have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the tags that should be assigned to devices that meet or fail the specific conditions.

Policy

CONDITION

- Flag devices running Webroot Agent
- Flag devices with Real-time Shield disabled
- Flag devices infected with malware
- Flag devices USB shield disabled
- Flag devices that have not connected in days
- Flag devices with Firewall disabled

FLAG







- AV-managed
- AV-off
- infected
- dev-control-off
- AV-stale
- FW-off

There are several conditions you can select to monitor. When selected CGX Access will set tags on specific devices that meet or fail the conditions. Using Auto Trust Policy, devices with specific tags can be assigned different roles.

Auto Trust Policy

[Activate](#) [Cancel Changes](#)

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	  
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	  

The example above shows a device will be assigned a non-compliant role if it has been tagged as AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

Tip: The AV-managed tag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

Orchestration with Syslog

Firewalls, APT solutions, and other security solutions that are designed to monitor devices and network traffic can send event-based alerts for administrative action. CGX Access can receive event-based syslog messages from all types for security devices and take immediate action when necessary. If CGX Access receives an alert that a device has malware or misbehaving, we can restrict it immediately.

Any solution that can send event-based syslog messages can be configured to work with CGX Access.

- In CGX Access GUI go to Configuration → Integration
- Click on "Syslog - Orchestration"

Edit Action [Close]

Syslog Integration

Enable syslog integration

Listen on port(s) UDP (514) TLS Over TCP (6514)

ORIGINATING SOURCES

Enable	Event Name	Event Source IPs
<input checked="" type="checkbox"/>	SonicWall IPS-PortScanning ▼	192.168.253.100
<input checked="" type="checkbox"/>	SonicWall IPS-TCPXmasTree ▼	192.168.253.100
<input checked="" type="checkbox"/>	SonicWall IPS-EICAR-Test ▼	192.168.253.100
<input checked="" type="checkbox"/>	SonicWall IPS-TCPNullFlag ▼	192.168.253.100
<input type="checkbox"/>	Select ▼	
<input type="checkbox"/>	Select ▼	
<input type="checkbox"/>	Select ▼	
<input type="checkbox"/>	Select ▼	

[Save] [Cancel] [Help]

From this screen, an Event can be enabled. The event source IP is the IP address of the security appliance that is sending the syslog message to CGX Access. Multiple IP addresses or IP ranges can be entered.

Syslog Event Creation

CGX Access can work with any solution (Firewall, APT, IPS, SIEM, etc.) that can send event-driven syslog messages. To create new Events

- In CGX Access GUI go to Policies → Orchestration Events
- Click on "New Event"
- Select "Device event from syslog"

The screenshot shows a dialog box titled "Create New Action" with a close button (X) in the top right corner. On the left, there are two radio buttons: "Device event from an email alert" (unselected) and "Device event from syslog" (selected). The main area is titled "Define a device event from syslog" and contains the following fields and options:

- Event Name:** A text box containing "SonicWall IPS-PortScanning".
- Search syslogs for:** A text box containing "Possible Port Scan Detected".
- Case sensitive while searching for pattern:** An unchecked checkbox.
- Skip syslogs containing:** A text box containing "Regular Expression describing the pattern".
- Case sensitive while searching for exclusion:** An unchecked checkbox.
- Type of information extracted:** Two radio buttons: "IP Address" (selected) and "Hostname" (unselected).
- Extract IP from:** A text box containing "SRC:(%IP)".
- Case sensitive while searching for IP:** An unchecked checkbox.
- Flag the device as:** A dropdown menu with "IPS-Event" selected.

At the bottom right, there are three buttons: "Save", "Cancel", and "Help".

This dialog box defines how a device event can be triggered from a syslog. If the search pattern is found, this event is triggered for the IP found in the syslog message. To set up an event four sections must be configured

Event Name

Give this event a name that explains which device is sending the syslog and what is looking for.

Search syslogs for

The system will search for Syslog messages that match the keywords specified here. For example: "ID=attack detected". Regular expressions can be used but don't include "/" at the beginning and the end.

Type of Information Extracted

Select whether the syslog message should be scanned for an IP address or Hostname.

If using IP: The system will extract the IP address of the offending endpoint using the predefined macro: (%IP) for the IP address's position. For example, we will specify: "SRC=(%IP)" if the IP value can be found after SRC:=..."

If using Hostname: The system will extract the hostname of the offending endpoint using after a keyword. For example, hostname:

Tag the Device as

Choose a tag that should be assigned to the offending device if the event is triggered. Using Device Classification policy, the device can then be automatically quarantined.

Custom tags names can be created under Configuration → General Settings → Names Used by Policies

Orchestration - Email Alerts

CGX Access can receive e-mail messages from all types for security devices and take immediate action when necessary. If CGX Access receives an email alert that a device has malware or is misbehaving, we can restrict it immediately.

Any solution that can send email messages can be configured to work with CGX Access.

- Verify an inbound e-mail server has been configured – See Page 19
- In CGX Access GUI go to Configuration → Integration
- Click on "Email - Orchestration"

The screenshot shows a dialog box titled "Edit Action" with a close button (X) in the top right corner. The main heading is "Email Alert Integration". Below this, there is a checked checkbox labeled "Enable email alert integration". Underneath, there is a text input field for "Sender's addresses" which is currently empty. Below that is a "Query interval (seconds)" input field containing the value "120".

The section "ORIGINATING SOURCES" contains a table with two columns: "Enable" and "Event Name".

Enable	Event Name
<input checked="" type="checkbox"/>	Sophos -Infection
<input type="checkbox"/>	Select
<input type="checkbox"/>	Select
<input type="checkbox"/>	Select

At the bottom of the dialog box, there are three buttons: "Save", "Cancel", and "Help".

- From this screen, an Event can be enabled.
- To limited which e-mail addresses are allowed to send an e-mail alert to the CGX Access appliance, specify the approved e-mails in the Sender's Address section. When blank all addresses are allowed.
- The Query interval specifies how often CGX Access checks the mail server for new e-mail alerts.

Email Event Creation

CGX Access can work with any solution (Firewall, APT, IPS, SIEM, etc.) that can send e-mail messages. To create new Events

- In CGX Access GUI go to Policies → Orchestration Events
- Click on "New Event"
- Select "Device event from an email alert"

The screenshot shows the 'Edit Action' dialog box with the title 'Define a device event from an email alert'. Below the title is a descriptive paragraph: 'Listens and handles email alerts except those containing the skip pattern. If the search pattern is found an event is triggered. When triggered, the IP or hostname noted in the email will be tagged as specified.' The form contains several sections:

- Event Name:** A text field containing 'Sophos -Infection'.
- Search email alerts for:** A text field containing 'Virus/spyware'.
- Case sensitive while searching for pattern:** An unchecked checkbox.
- Skip email alerts containing:** A text field containing 'Regular Expression describing the pattern'.
- Case sensitive while searching for exclusion:** An unchecked checkbox.
- Type of information extracted:** Radio buttons for 'IP Address' (unchecked) and 'Hostname' (checked).
- Extract Hostname from:** A text field containing 'Machine:'.
- Case sensitive while searching for keyword:** An unchecked checkbox.
- Tag the device:** Radio buttons for 'Add Tag' (checked) and 'Remove Tag' (unchecked).
- Tag:** A dropdown menu with 'infected' selected.

At the bottom right of the dialog are three buttons: 'Save', 'Cancel', and 'Help'.

This dialog box defines how a device event can be triggered from an e-mail. If the search pattern is found, this event is triggered for the IP or hostname found in the e-mail message. To set up an event four sections must be configured:

Event Name

Give this event a name that explains which device is sending the e-mail and why.

Search email alerts for

The system will search the email messages for keywords specified here. For example: "Virus/Spyware". Regular expressions can be used but don't include "/" at the beginning and the end.

Type of Information Extracted

Select whether the email message should be read for an IP address or Hostname.

If using Hostname: The system will extract the hostname after reading a keyword. For example, if Machine: is specified as the keyword, any name following it will be assumed as the hostname.

If using IP: The system will extract the IP address of the offending endpoint using the predefined macro: (%IP) for the IP address's position. For example, we will specify: "SRC=(%IP)" if the IP value follows after SRC:=.

Tag the Device as

Choose a tag that should be assigned to the offending device if the event is triggered. Using Device Classification policy, the device can then be automatically quarantined.

Custom tags names can be created under Configuration → General Settings → Names Used by Policies

Advance Security

Malware Lateral Spread Protection - Zero-Day

With its layer-2 visibility, CGX Access can detect devices making connection attempts to other devices within the same segment. If an end-user device suddenly attempts to connect to an excessive number of devices on the same subnet or tries to connect to Dark IPs that are not active on the network, this is suspicious behavior. This behavior is indicative of a network scan being performed or malware trying to probe the network in an attempt to spread. Easy NAC can detect this behavior and immediately quarantine this device so it can't spread malware laterally on the network.

- In CGX Access GUI go to Policies → Advance Security
- Click on "Malware Lateral Spread Protection – Zero-Day"

Edit Action

Malware Lateral Spread Protection – Zero Day

MALWARE LATERAL SPREAD PROTECTION PROTECTS AGAINST WORMS, MALWARE AND USERS WITH MALICIOUS INTENT BY DETECTING DEVICES MAKING UNUSUAL CONNECTIONS ATTEMPTS TO OTHER DEVICES ON THE SAME LOCAL SUBNET. LAYER-2 ARP TRAFFIC IS INVISIBLE TO MOST SECURITY SOLUTIONS BUT IS AN EARLY WARNING SIGN OF TROUBLE. WITH FAST DETECTION, MALWARE CAN BE PREVENTED FROM SPREADING OVER THE NETWORK.

Enable Integration

Query Interval (Seconds)

CONDITION

Tag devices trying to connect to excessive # of used IPs
 different IPs within one minute is considered excessive

Tag devices trying to connect to excessive # of unused IPs
 different IPs within one minute is excessive

TAG

Scan-detected

Dark-IP-scan

Save Cancel Help

When enabled, devices making connection attempts to an excessive number of hosts will be tagged as “Scan-detected”. While devices attempting connection attempts to unused IP addresses will be tagged as “Dark-IP-Scan”

Policy-Based Response

When the “Scan-detected” tag and “Dark-IP-Scan” tag is assigned to a device, the CGX Access can take quarantine actions based on Auto Trust Policy.

- In CGX Access GUI go to Policies → Auto Trust
- Add Rule to take action when a device is tagged “Scan-detected” and “Dark-IP-Scan”

Auto Trust Policy

↻ Activate
↶ Cancel Changes

[Add Rule](#)

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Deception Event - Honey Pot hit detected Has all of these tags: Deception-Event, Honeypot-hit	Set role to High-Risk-Event - Suspicious behavior detected Send message to: Admin via Email	⊙ ↻ ✕
Malware Lateral Spread Risk - Scan Detected Has all of these tags: Dark-IP-scan, Scan-detected	Set role to High-Risk-Event - Excessive network scanning activity was detected	⊙ ↻ ✕

- The new rule should be dragged near the top of the list, so it has higher priority over other sets of conditions

Tip: By specifying “All tags” both the “Scan-detected” tag and “Dark-IP-scan” tag needs to be present. Requiring both tags to be present can reduce false positives.

Clearing Zero-day Events

Once a device has been restricted, it will be necessary to clear the event so the device can have network access again.

- In CGX Access GUI go to Visibility → Alerts and Notifications
- Click “Devices with Events”
- Select the device(s) that should be cleared, Select the “Clear event” option and Apply

Alerts and Notifications

Devices with events [Back](#) [Refresh](#) [Export](#) [Help](#)

updated at Thu Jun 04 2020 18:33:46

Show Report Filter

Clear events ▼
Apply to selected devices

Total # of devices: 1

Make it a custom report
Add a schedule report
Devices Per Page 100 Page 1 of 1. First << [1] >> Last

☐	MAC	Hostname	Events	Access Group	Roles	Location	IP Address	OS	Flags / Lists	Last Seen	Access Status	Grant Access	⊙
<input checked="" type="checkbox"/>	00:0C:29:4B:70:2E	managed01	2020-06-04 18:33:40 arpSCAN (Scan-detected) 2020-06-04 18:33:40 darkip (Dark-IP-scan)	restricted	High-Risk	VM demo	192.168.253.54	Windows 7 Professional 6.1 Build 7601 Service Pack 1	virtual AD-managed AV-managed Scan-detected Dark-IP-scan	2020-06-04 18:32:48	●	ON OFF Auto	⊙

Handling Exceptions

For network monitoring, it may be necessary to configure exceptions on some devices. To ignore Zero-day behavioral detection, you can tag the allowed devices as “arp-scan-ignoring” and “darkip-scan-ignoring”. These tags can be set using the Device Manager or Device with Events report.

- In CGX Access GUI go to Visibility → Alerts and Notifications
- Click “Devices with Events”
- Select the device(s) that should be exempted, Select the “Ignore Zero-Day Behavioral Detection” option and Apply

Alerts and Notifications

Devices with events [Back](#) [Refresh](#) [Export](#) [Help](#)

updated at Thu Jun 04 2020 18:42:56

Show Report Filter

Ignore Zero-Day Behavioral Dete [Apply to selected devices](#)

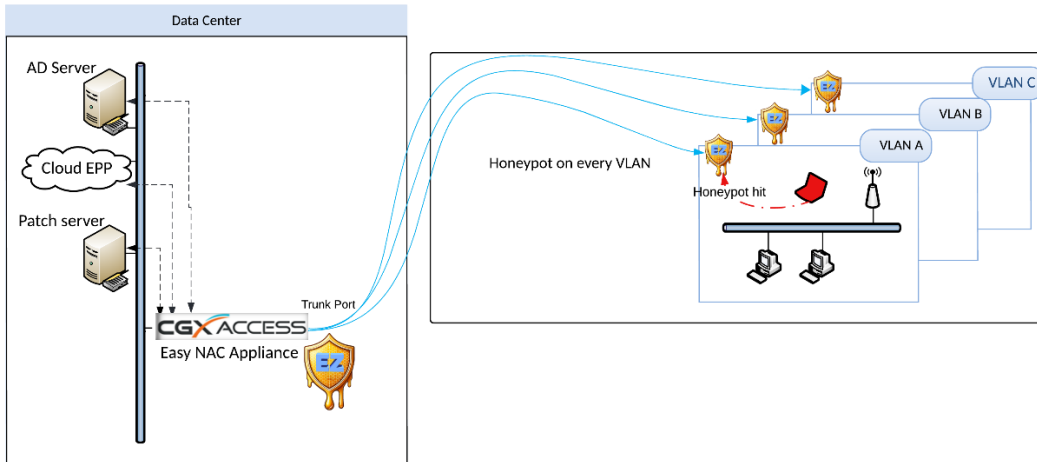
Total # of devices: 1 [Make it a custom report](#) [Add a schedule report](#) Devices Per Page Page 1 of 1. First << [1] >> Last

<input type="checkbox"/>	MAC	Hostname	Events	Access Group	Roles	Location	IP Address	OS	Flags / Lists	Last Seen	Access Status	Grant Access		
<input checked="" type="checkbox"/>	00:0C:29:4B:70:2E	managed01	2020-06-04 18:34:59 arpscan (Scan-detected) 2020-06-04 18:34:59 darkip (Dark-IP-scan)	restricted	High-Risk	VM demo	192.168.253.54	Windows 7 Professional 6.1 Build 7601 Service Pack 1	virtual AD-managed AV-managed Scan-detected Dark-IP-scan	2020-06-04 18:42:45	●	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Auto		

Note: by default, devices tagged as Network Infrastructure are exempt from scanning checks.

Deception – Hacking Detection

With its layer-2 protection, the Easy NAC solution will host fake services such as SSH, Telnet, FTP, etc. on every VLAN or subnet it's protecting, creating a distributed honeypot. These fake services serve no real business purpose, so if any person or bot tries to login to these fake services, it's a strong indicator of hacking activity. With virtual honeypots on every VLAN, it provides early detection of hacking activity before hackers reach the core of the network.



- In CGX Access GUI go to Policies → Advance Security
- Click on "Deception – Hacking Detection"

Edit Action

Deception - Hacking Detection

THE DECEPTION - HACKING DETECTION FEATURE WAS DESIGNED TO QUICKLY DETECT HACKING ACTIVITY AT THE EDGE OF THE NETWORK, BEFORE A HACKER REACHES THE NETWORK CORE. EASY NAC HAS AN IP ON EVERY PROTECTED VLAN THAT IT USES FOR REAL-TIME VISIBILITY AND CONTROL. LEVERAGING THESE SAME IP ADDRESSES, EASY NAC WILL HOST HONEY-POT SERVICES ON EVERY VLAN. IF ANY DEVICE ATTEMPTS TO ACCESS THESE FAKE SERVICES, IT WOULD BE A STRONG INDICATOR OF HACKING ACTIVITY.

Enable Integration

Protocols

- SSH
- Telnet
- FTP
- Windows File Sharing

IP Ranges to Exclude

e.g. 10.0.0.1-10.0.0.255
20.0.0.0/255.255.255.0
30.0.0.1

CONDITION

- Tag devices that have attempted connections to fake services
- Tag devices that have attempted to login to fake services

TAG

Honeypot-hit

Deception-Event

Save Cancel Help

The “Honey-pot-hit” tag will be assigned to any device that attempts to connect to any of the fake services. To avoid false positives, exclude IPs that are allowed to scan the network.

The “Deception-Event” tag would be assigned after the user attempts to login into the fake services. For near-zero false positives, it’s best practice to quarantine a device only when both flags are present.

Policy-Based Response

When the “Honey-pot-hit” tag and “Deception-Event” tags are assigned to a device, the CGX Access can take quarantine actions based on Auto Trust Policy.

- In CGX Access GUI go to Policies → Auto Trust
- Add Rule to take action when a device is tagged “Honey-pot-hit” and “Deception-Event”

Auto Trust Policy

↻ Activate
↶ Cancel Changes

[Add Rule](#)

Conditions	Actions taken when conditions are met
Device is on routerlist	Set role to full-access - Device is on routerlist
Device is on allowlist	Set role to full-access - Device is on allowlist
Device is on blocklist	Set role to restricted - Device is on blocklist
Deception Event Has all of these tags: Honey-pot-hit, Deception-Event	Set role to High-Risk-Event - Suspicious behavior detected Send message to: EasyNAC Admin via Email

Credentials used

The Deception feature will record the credentials used in the detected hacking attempt. To view:

- Click the MAC address of the restricted device
- Click the Honey-pot Tab

MAC	Hostname	Roles	Location	OS	Last Seen	Comment	First Seen	Vendor	Tags / Lists	IP Address / IPv6	Access Status	Grant Access
00:50:56:AF:A3:D8	desktop-6fjp5su	High-Risk-Event	Cloud demo	Windows 10 Enterprise 6.3 Build 19045 Service Pack None	2023-12-18 16:45:17	AD Joined Client	2022-04-23 12:28:55	VMware, Inc.	virtual AD-managed AV-managed honey-pot-hit Deception-Event	10.160.0.222	●	ON OFF Auto

Device Detail Data

General
NMAP
DHCP
FingerBank
Honey-pot
Web
Sophos
AD
ARP

Agent Audit
Access Changes

```

{
  "mac": "00:50:56:AF:A3:D8",
  "ip": "10.160.0.222",
  "ssh": {
    "session": "07dfc0c6061f",
    "ts": "2023-12-18 16:44:45",
    "clientVersion": "SSH-2.0-PuTTY_Release_0.79",
    "credentials": [
      {
        "password": "password",
        "username": "admin"
      }
    ]
  }
}

```

Edge Protection – Layer-2 Security

With its layer-2 visibility, the Easy NAC solution can help detect configuration issues (IP conflicts and ARP storms) or security risks (ARP spoofing) occurring at the edge of the network.

Edit Action ✕

Edge Protection - Layer 2 Security

CONDITION

Tag devices with IP-conflicts

Devices to exclude

Tag devices detected as ARP Poisoning

Sensitivity Level: Low Medium High Custom ✎

Tag devices sending excessive Gratuitous ARP

Sensitivity Level: Low Medium High Custom ✎

TAG EVENT

ip-conflict

arp-poisoner

arp-storm

Save
Cancel
Help

Policy-Based Notifications

When an “ip-conflict”, “arp-poisoner” or “arp-storm” tag is assigned to a device, the Easy NAC solution can send notifications based on Device Monitoring Policy.

- In CGX Access GUI go to Policies → Monitoring → Device-Monitoring-Policy
- Add Rule to send alert when a device is tagged “ip-conflict”, “arp-poisoner” or “arp-storm”

Monitoring Policies >> Device-Monitoring-Policy

[Back](#)

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Excessive Access Changes Above 10 Access Changes/Hour	Send message to: Admin via Email	⊙ ✎ ✕
Edge Monitoring Has any of these tags: ip-conflict, arp-storm, arp-poisoner	Send message to: Admin via Email, Microsoft Teams	⊙ ✎ ✕
New Device on the Network Device 1st seen less than 2 minutes ago	Send message to: Admin via Email	⊙ ✎ ✕

Agent Support

Easy NAC was designed to be an agentless solution. However, agent licenses are optional and can be used for more in-depth compliance checks, automatic remediation, and other capabilities. Agents are only required for VPN protection. When using agents, you can also consider a hybrid deployment model, where laptops needing stronger security checks use the agents, while desktops use the agentless approach. The table below summarizes the differences in these approaches.

	CGX Access - Agent	CGX Access – Agentless
Detection	Agent would detect changes within 10 seconds	Compliance check with integration module depends on the re-check interval
Supported OS	<ul style="list-style-type: none"> • Microsoft Windows • Apple MacOS • Linux 	The Operating Systems supported by Integration solution(s)
Compliance checks	<p>Compliance check can be customized to include but not limited to the followings:</p> <ul style="list-style-type: none"> • Running Process • Registry values • Files and locations • Ini files and contents • Machine names and OS check • Authentication 	Agentless solution – Integrations with AD, 3 rd -party AV, Patch, and WMI
End-user compliance communication	Pop-up Message	HTTP Redirection
Real-time Wi-Fi adapters control	<p>When connected to any wired network that has connectivity to CGX-Access (ie. Corporate Network). The wireless network adapter can be disabled automatically.</p> <p>It would be re-enabled once wired NIC is disconnected</p>	<p>N/A</p> <p>Can use Windows Connection Manager as a substitute</p>
Automatic Remediation	When a compliance check fails, a remediation action can be kicked in. It includes running scripts or binary in the host that has the agent installed. With or without administrative rights.	N/A

Working with Agents

Easy NAC virtual appliances come with default agents and default policies that can be used for testing or as a baseline to start building your custom compliance policies.

By default, Auto Trust Policy will assign a device passing an agent audit with full access. While a device failing audit would be assigned a failed-agent-audit role. The order of the policies is important, so in some environments, it may be necessary to drag these policies up for higher priority.

- In CGX Access GUI go to Policies → Auto Trust

Auto Trust Policy

↻ Activate
↶ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Deception Event - Honey Pot hit detected Has all of these tags: Deception-Event, Honeypot-hit	Set role to High-Risk-Event - Suspicious behavior detected Send message to: Admin via Email	⊙ ✎ ✕
Malware Lateral Spread Risk - Scan Detected Has all of these tags: Dark-IP-scan, Scan-detected	Set role to High-Risk-Event - Excessive network scanning activity was detected	⊙ ✎ ✕
Fingerprint Mismatch Has any of these tags: FP-mismatched	Set role to High-Risk-Event - Device failed fingerprint check	⊙ ✎ ✕
Orchestration Event Has any of these tags: SIEM-Event, IPS-Event, infected, FW-Event, APT-Event	Set role to High-Risk-Event - Malware or suspicious behavior has been detected	⊙ ✎ ✕
Passed Agent Audit Passed Agent Audit	Set role to full-access - Passed agent audit	⊙ ✎ ✕
Failed Agent Audit Failed Agent Audit	Set role to failed-agent-audit - Failed agent audit	⊙ ✎ ✕

When assigned a “failed-agent-audit” role the device will be assigned “restrict-agent” ACL. By default, restrict-agent ACL blocks all traffic except DNS, DHCP, and the agent traffic over port TCP 11698.

Edit Action ✕

Configure NAC rules for access group

Access group

Condition ▾

ACL rules

```

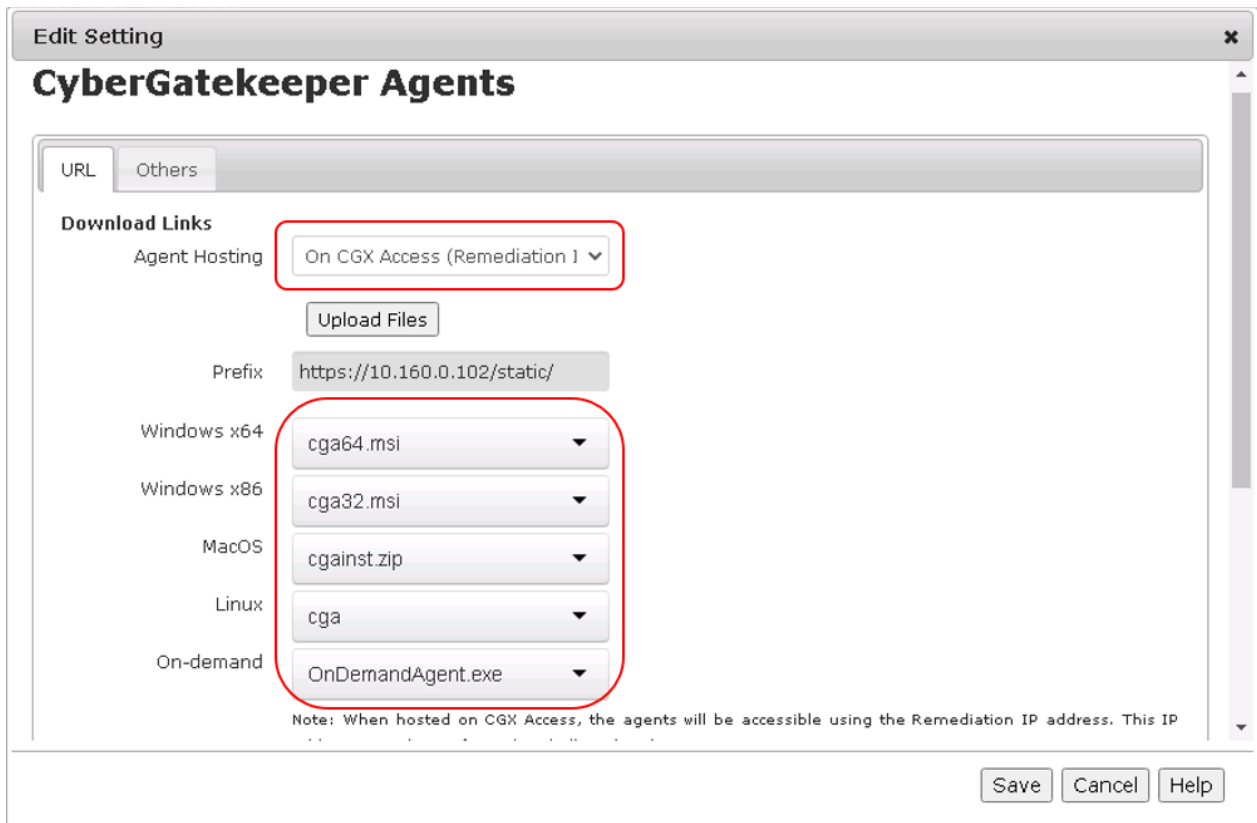
ALLOW WHEN PROTO=='UDP' AND PORT==53
ALLOW WHEN PROTO=='TCP' AND PORT==53
ALLOW WHEN PROTO=='UDP' AND PORT==67
ALLOW WHEN PROTO=='TCP' AND PORT==67
ALLOW WHEN PROTO=='TCP' AND PORT==11698
DENY WHEN TRUE
                
```

It is recommended the default “restrict-agent” ACL be edited to allow access to approved remediation resources such as the AV server, patch server, etc.

Hosting Agents

Easy NAC virtual appliances come with default agents that will meet most customer requirements. To make these agents available for use:

- In CGX Access GUI go to Configuration → Global Settings → CyberGatekeeper Agents
- Adjust your Captive portal settings to allow the download of the agents



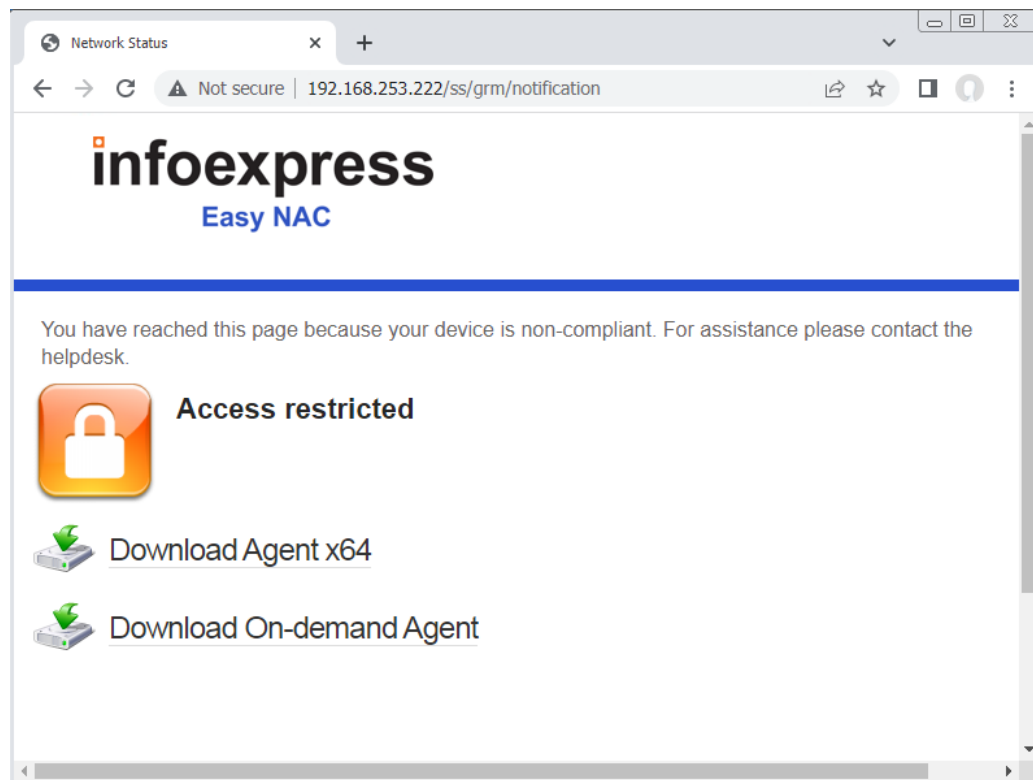
To host agents on the appliance, it will be necessary to use the Remediation IP address. Once the above settings are configured; you can decide when to show the agent installers to your end-users.

Show Links

- After successful guest registration / authentication.
- After employee registers device.
- On the main landing page.
- On Remediation page.
- Show all configured agent links.

Based on requirements, you can choose when to display the agent installers. This would be helpful for special situations where you require guest, consultant or BYOD devices to install agents for network access.

The appliance will only show the agent type appropriate for the Operating System, so a guest with a MAC computer will only be shown the OSX agent. If you want to display all the available agent options, you can check “Show all configured agent links”.



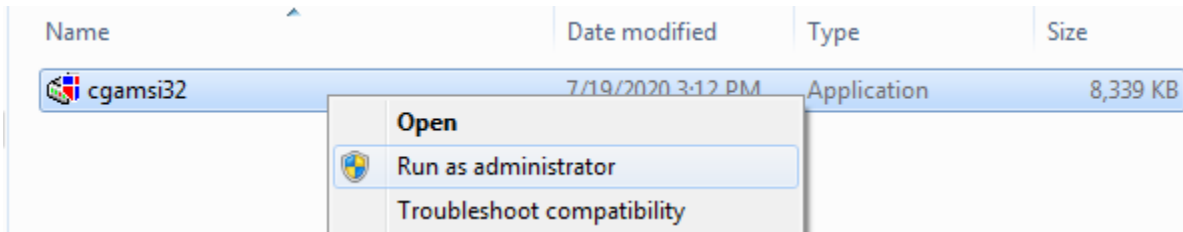
Installing Agents

The CyberGatekeeper Agents are designed to install silently. Once the installer is run the agent will install silently with no configuration options or reboots required. The Windows installers are approximately 8-10 MB in size. The MAC OSX agent installer is approximately 4 MB. These sizes make it quick to download and install. When installed and running the agents will use 4-6 MB of RAM and utilize ~1% CPU every 30 seconds.

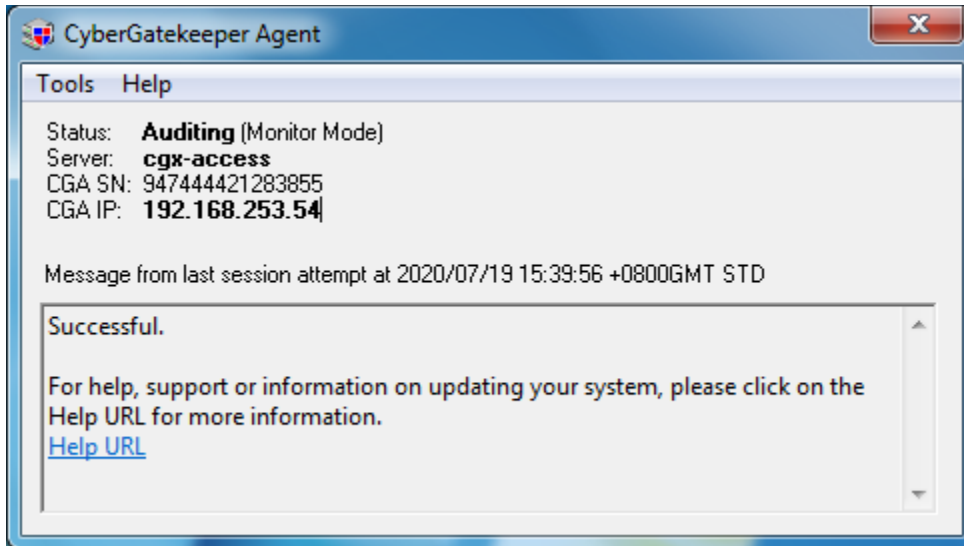
Most organizations choose to use a software deployment tool or AD Group policy with a computer startup script to install the agent automatically for their managed devices. Contact InfoExpress support for a sample script.

In the case of manual deployment, local administrative rights are required.

- Right-click the installer file and choose to “Run as administrator”



- There will be no prompts or confirmations. Allow 30-60 seconds for the install to be completed in the background
- When finished an icon in the system tray will be visible. When double clicked the agent viewer will show the current status



On-demand Agents (Recommended for Consultants)

The normal CyberGatekeeper agents are designed to be installed on managed devices, and requires administrative rights to be installed. Once installed, this agent will be started in the background to provide transparent and continuous checks. However, it may be desirable to perform similar compliance checks on unmanaged computers used by consultants. For this requirement, you can use the on-demand agents.

A key difference with the on-demand agent, is that it doesn't require admin rights to install, because it doesn't get installed. The on-demand agent is 2-3 MB executable that runs in memory until the agent viewer is closed. Once the agent viewer is closed, the agent checks are stopped, and the consultant will need to run the executable again if she needs to reconnect to the network. By default, a device passing audit will continue to be passing audit for 5 minutes, after this agent has been closed.

Requirements \ Limitations:

- Supported on Windows 64-bit Operating Systems only (Windows 7 and Windows 10)
- Supports Windows Security Center and Windows Update plug-ins
- Nic Manager Plug-in or any plug-in requiring admin rights is not supported
- Automatic Remediation is not supported

Agent Compliance Policies

Easy NAC virtual appliances come with default agent compliance policies that have been pushed to the appliance. These default policies will provide checks for common AV solutions:

- Anti-Virus Installed
- Anti-Virus Running
- AV Up-to-date
- Real-time scanning enabled
- Windows Updated Enabled
- Recent Microsoft updates

These policies are a good starting point, but it would be recommended every customer adjust these policies to meet their specific requirements. For example, if your organization's endpoint security is TrendMicro, then it may only be necessary to check for this brand.

To adjust the policies, it will be necessary to install a CyberGatekeeper Policy Manager. Contact InfoExpress support or your partner for a copy of the CGPM installer and a copy of the of the Easy NAC Default Settings installer.

1. Install Policy Manager
2. Keep Policy Manager closed
3. Run Easy NAC Default settings

Note: If you plan to use the default agents, it will be necessary to run the Easy NAC Default settings installer to ensure the agents and Policy Manager have the correct shared settings.

Policy Manager

Policy Manager, also called CGPM (CyberGatekeeper Policy Manager) is a Windows-based application that can be installed on any 64bit Microsoft Windows Operating System.

The Policy Manager application is used for:

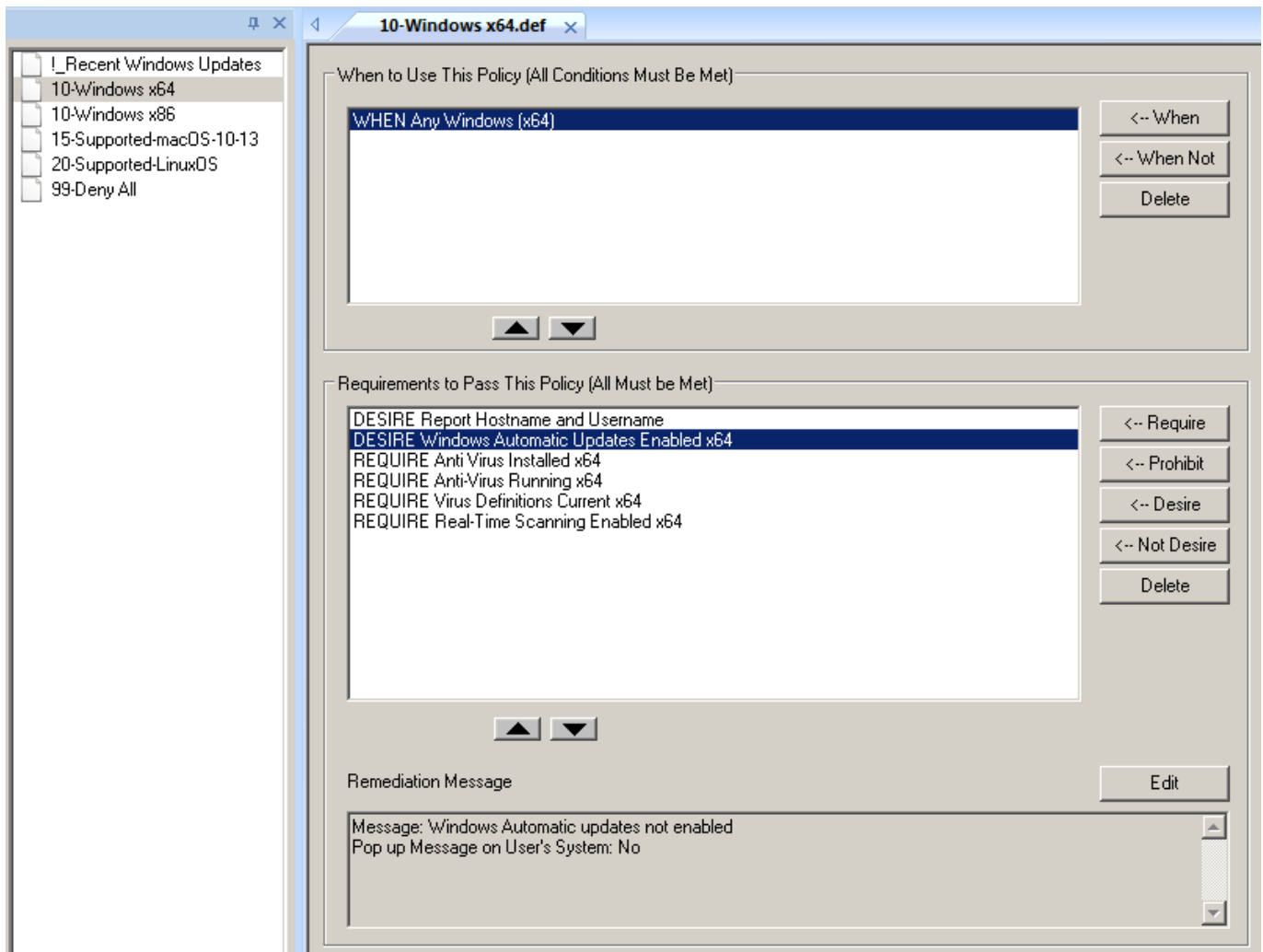
- Creating compliance tests
- Creating compliance policies
- Uploading compliance policies to CGX Access appliances
- Building agents for different operating systems

The sections below will serve as a QuickStart guide and Best Practices Guide on how to make use of policy manager to create the desire agent checks.

Tip: For complete details of the CyberGatekeeper Policy Manager, please refer to the Policy Manager Reference Manual.

Policies

The **Policies** creates and edits audit policies. Audit policies let administrators specify what applications, configurations, and systems should be allowed or denied into the corporate network.



A policy consists of a When Section and a Requirements section. Each requirement section can have their own remediation section. The When Section indicates which remote systems should be governed by this policy.

If this policy's When Section does not match the audit information from the remote system, the next policy will be checked. If the When Section matches the audit information from the remote system, the Requirements Section is checked to see whether the remote system should be given access to the corporate network.

When to Use This Policy...

The When Section contains conditions consisting of **WHEN** or **WHENNOT** commands followed by test conditions. The **WHEN** command passes if the test condition is true. The **WHENNOT** command passes if the test condition is not true. All of the When Conditions in the policy must match the audit information for the policy to be valid (All conditions are ANDed).

Ordered policies are policies starts with a number in their names. They are arranged in alphanumerical order. The order in which policies will be evaluated can be seen in the list of policies on CGPM. An agent can take only 1 ordered policy at a time. Once a match is found in the When Section, the policy would be taken by this agent and no other policies would be checked.

Policies Best Practices

- It is a best practice to name the polices with a numbered prefix. This way, you would be able to change the priority of when a policy gets evaluated by changing its prefix number easily.

For example, an ordered policy named **80-Windows.def** would be evaluated before another policy named **90-Windows.def** because the system would evaluate the policies in alphanumeric order.

- The more conditions that you have defined in the When Section, the policy should be evaluated first. You can do so by changing the name of the policy as suggested above.

For example, if your **90-Windows.def** has two When conditions defined (When Any Windows and When in IP range 192.168.0.0/24) and your **80-Windows.def** has 1 When condition defined (When Any Windows).

In this case, all your agents would be getting the **80-Windows.def** because it has a more generic When condition (only 1).

The correct way to do it, is to rename the **90-Windows.def** to, for example, **70-Windows.def**. This would make the policy list higher alphanumerically and hence be evaluated first.

- If you have a mixed 32bit and 64bit of Windows OSes that still need to be supported. It would be best to separate them into two sets of policies. Ie. One for 32bit and another one for 64bit.
- Policies created are stored in the Policy Manager installation folder, it is recommended to have a backup of the whole policy manager folder which is in C:\Program Files\InfoExpress\CyberGatekeeper Policy Manager.

Requirements to Pass a Policy

The Requirements Section contains requirements consisting of **REQUIRE**, **PROHIBIT**, **DESIRE** or **NOTDESIRE** commands followed by test conditions.

The **REQUIRE** command is used to ensure certain conditions are present and passes if the test condition(s) are true. If any **REQUIRE** command is not met, the agent would FAIL to pass this policy and hence the audit.

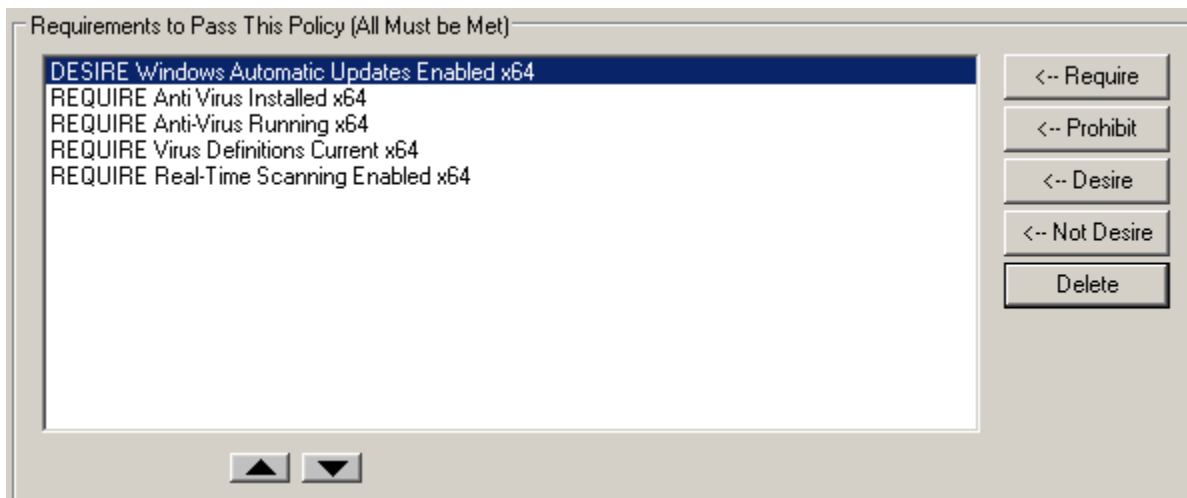
The **PROHIBIT** command is used to prevent certain conditions and passes if the test condition is not true. If any **PROHIBIT** command is not met, the agent would FAIL to pass this policy and hence the audit.

The **DESIRE** command is used to check if certain conditions are present. If the test condition(s) are true, it would pass the policy. However, even in the case the **DESIRE** command is not met, it would still pass. This is helpful if compliance information is desired, but no quarantine action should be performed.

The **NOTDESIRE** command is used to check if certain conditions are not present and passes if the test condition is not true. However, even in the case the **NOTDESIRE** command fails, it would still pass. This is helpful if compliance information is desired, but no quarantine action should be performed.

Requirements Priority

All the tests, when added to the policy, would be the requirements. These requirements would all be evaluated from top down.



For example, as per the screenshot above, **DESIRE** “Windows Automatic Updates Enabled” would be checked first, then followed by **REQUIRE** Anti-Virus Installed, then **REQUIRE** Anti-Virus Running, etc.

When a **REQUIRE** or **PROHIBIT** test fails, the audit would be marked as **FAIL** and any tests that sit below would not be checked.

However, because of the nature of the **DESIRE** or **NOTDESIRE** command, it would still be pass audit, even if it fails this test, so the next requirement would still be checked.

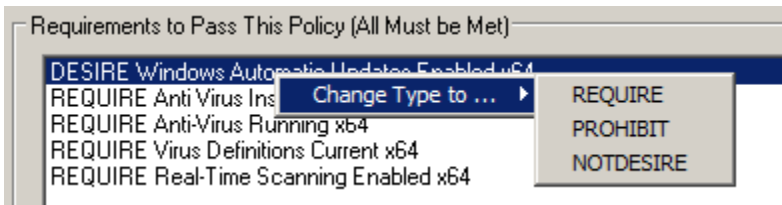
For example, if **REQUIRE** Antivirus Running failed, it would be marked as failing this test. The agent would not check for any test below, in this case the **REQUIRE** Virus Definitions Current and the **REQUIRE** Real-Time Scrolling Enabled would not be checked.

Requirement Best Practices

- It is recommended to put the DESIRE and NOTDESIRE commands in the requirements to the top by using the arrow button. This way, we ensured all these tests are checked properly before REQUIRE and PROHIBIT commands.



- You can change the command type by right-clicking on a command. For example, change from DESIRE to REQUIRE.



- Please check if there are prerequisites for tests and arrange the order of these tests accordingly.

For example, a test check for Antivirus running should be checked first before the Antivirus signature is not older than 7 days. It is because the antivirus program might not be able to update the signature if it is not even running.

Remediation

If an agent fails a policy requirement, the administrator has the option of running a remediation action, displaying a remediation message to the user or both.

- The remediation action can be configured to bring the device back into compliance so that it can successfully audit against the policy.
- The remediation message pops up a dialog box with informational or instructional information to users.
- A unique remediation action and/or pop-up message can be configured for each of the requirements set in a policy.

To configure the remediation, please highlighted the corresponding test in the requirement section and then click the Edit button. This would bring the **Edit Remediation Option** dialog box.

Edit Remediation Option

Remediation Message

Pop up Message on User's System

Remediation Link (e.g. http://xxxx... , \\server\path\file)

Remediation Link Name Shown on Agent Viewer

Command Arguments

Run Remediation for Desktop Agent

- Run Remediation with Admin Rights
- Run Remediation for Web Agent (for Windows only)
- Run only once a user has logged in (for Windows only)
- Show Download Progress Bar

Advanced Options (for Windows only)

OK
 Cancel

Pop-up Messages

The Remediation Message box can be edited to include any remediation message that the administrator deems appropriate. For example, "No authorized antivirus software is found".

Messages do not pop up by default. In order to have the message displayed on the agent upon a failed requirement, the "Pop up Message on User's System" check box should be selected.

An URL can be embedded in the remediation message to direct the user to further resources to help provide further information or this URL can be put in the Remediation Link box.

Remediation Actions

The remediation action must be entered under the **Remediation Link** input box. It can contain either a URL tag or UNC tag (Universal Naming Convention). The tag points to a file that will be run on the end user system if that endpoint fails the requirement.

The file that the tag points to can be any file type that can be run on the hosts system: common file types include executables (.exe), Windows scripts (.vbs, .bat, .cmd). If the remediation scripts or executables require parameters (arguments) they can be entered under "Command Arguments". Multiple parameters should be separated by spaces.

For example:

URL Tag: `http://192.168.253.128/fix/ResShieldOn.bat`

UNC Tag: `\\server\path\ResShieldOn.vbs`

Even if you defined a remediation script URL in the Remediation Link, it may still require the user to click on the link to download and run the script manually.

Auto-remediation

To provide a better end user experience, the remediation action can be configured to run automatically without any user intervention.

Also, the user privilege that the remediation script runs would also be configurable.

To allow the remediation script to run automatically with the current logged on user privilege, select the **Run remediation for Desktop Agent**.

To allow the remediation script to run automatically but with local administrative rights, select both the **Run remediation for Desktop Agent** and **Run Remediation with Admin Rights**.

Note: Only standard Windows Agent and Mac OS Agent support remediation actions.

Remediation Best Practices

- It is recommended to configure the remediation action via an URL instead of a UNC path. Because the agent runs with the local system account on the endpoint. If a network resource is accessed, it might not have the sufficient privilege. You can host the remediation scripts on the CGX Access appliance or Central Visibility Manager
- The remediation action is best to configure to run without any user intervention.

For example, running a batch file (.bat) as a remediation script is supported but it might trigger a command prompt to be shown on the user's endpoint. It would look malicious to users. However, when running it with a VB Script, it can do the same remediation action but can be configured in the script to hide any user feedback (more transparent user experience).

- Depending on the nature of the remediation script, the necessary privilege would need to be configured properly for the script to run properly. For example, if the script requires administrative privilege (restarting a service), running the script automatically with the user privilege alone might not work for everyone.

Using Active Directory User Group in Auto Trust Policy

It is possible to use Active Directory User Group of a current logged on user in an agent installed device as a condition for the Auto Trust Policy.

Prerequisites

- DNS server and Domain Settings for CGX Access
- Configure Active Directory User Group
- CGX Access to be joined as a Domain Member
- Additional “Authentication Plugin” in CyberGatekeeper Agent

DNS server and Domain Settings for CGX Access

The DNS server, hostname and domain name of CGX Access should be properly configured as the Active Directory Server. It is necessary for the CGX Access to be joined as a Domain Member.

Configure Networking:

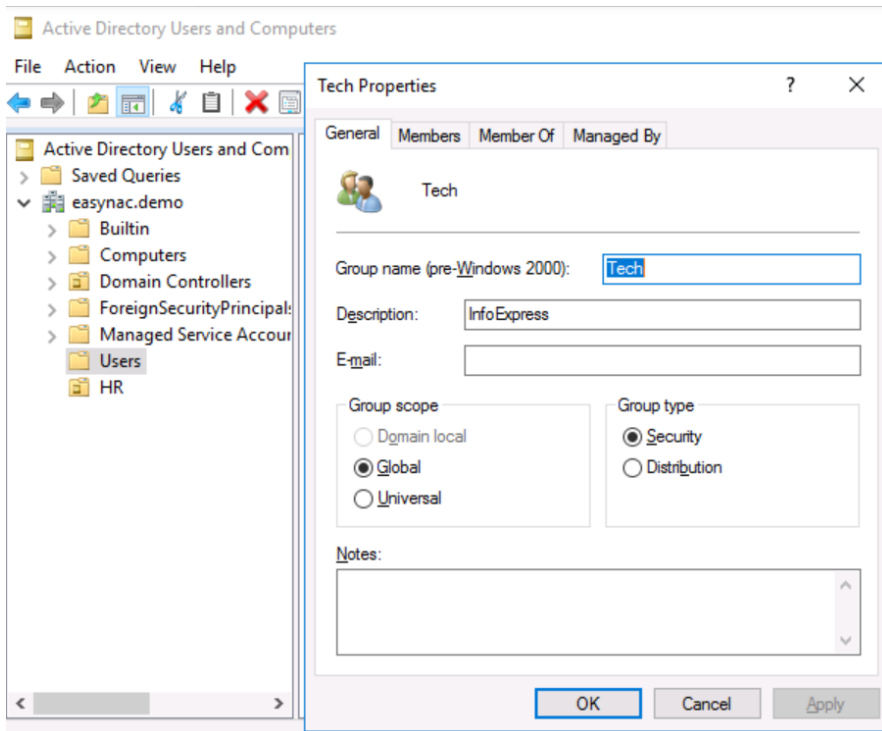
Adapters	IP / Netmask	Gateway
Adapter #1 MAC: 00:50:56:a4:e4:12 Speed: 10 Gb/s	10.160.0.100/255.255.255.0	10.160.0.1
Adapter #2 MAC: 00:50:56:a4:89:0c Speed: 0 Gb/s	/	
DNS Servers	10.160.0.200	
Hostname	cgx-access	
Domain Name	easynac.demo	

In the example above, the CGX Access’s hostname is configured as cgx-access and the Domain Name of the Active Directory is configured as “easynac.demo”. The DNS server is pointing to the Active Directory Server’s IP address.

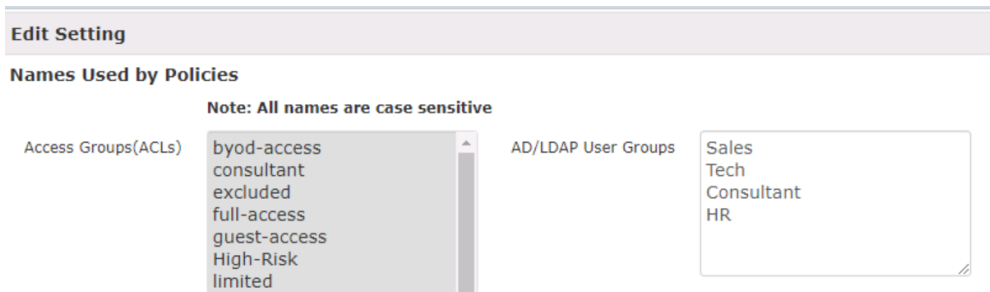
Configure Active Directory User Group

To configure the Active Directory User Group, the following steps are required

- 1) Below is an example of a User Group called “Tech” to be used in CGX Access. Add Active Directory Users to the corresponding Active Directory Group.



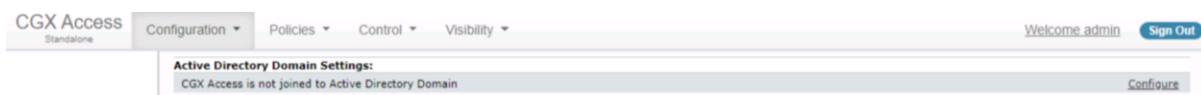
- 2) Add the Group Name of AD to be used in the CGX Access.
 - a. In CGX Access GUI go to Configuration → General Settings
 - b. Click the “Name used by Policy” of Configuration Settings
 - c. Add the Active Directory User Group to be used as follow



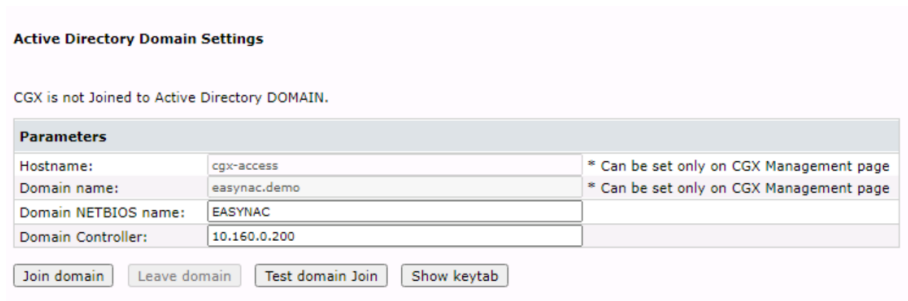
- d. Click Save to confirm

Joining CGX Access to Active Directory

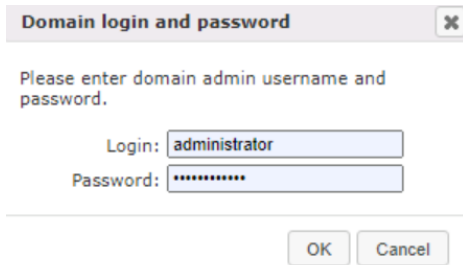
- In CGX Access GUI, goto Configuration → Appliance Settings



- Click Configure under the “Active Directory Domain Settings” and configure the Domain NETBIOS name and Doman Controller.



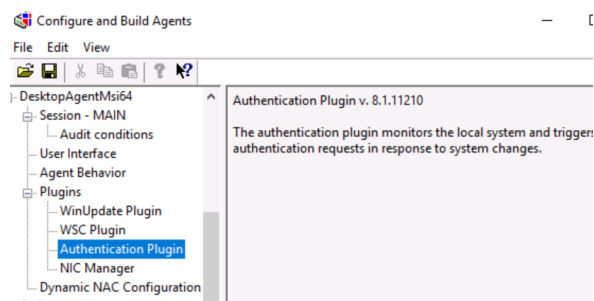
- Click Join Domain and type the Domain Administrator credential into the dialog box.



- Click OK to confirm.

CyberGatekeeper Agent Authentication Plugin

When building the CyberGatekeeper Agent installer in Policy Manager, please kindly add the “Authentication Plugin” as shown below before building the agent installer.



To confirm the Authentication Plugin has been added to the agent installer, goto CyberGatekeeper Agent GUI, click Help → About to ensure the AuthPlugin has been added.



Add the User Group as a condition in Auto Trust Policy

To create a rule under the Auto Trust Policy with the “User Group” added as a condition. Select the User Group that you would like to check and assign it to the corresponding device role.

Create New Condition

Device Authentication	Criteria Match any of the groups checked <input type="checkbox"/> Check All Applicable <input type="checkbox"/> User Groups <input type="checkbox"/> Sales <input type="checkbox"/> Tech <input type="checkbox"/> Consultant <input type="checkbox"/> HGM <input type="checkbox"/> HR
Device Access	
Device Flag	
Device IP Address	
Device List	
Device MAC Address	
Device OS	
Check Device's Online Status	
User Group	
Device Status	

The Auto Trust Policy rules are examples of how the User Group can be used to assign to different roles based on the user logged on.

Auto Trust Policy

↻ Activate
✕ Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Sales VPN access Device location matches any of VPN IP Range User is a member of any of these groups: Sales Passed Agent Audit	Set role to Sales	⊙ ↻ ✕
Tech VPN Access Device location matches any of VPN IP Range User is a member of any of these groups: Tech Passed Agent Audit	Set role to Tech	⊙ ↻ ✕

Troubleshooting Agents

Installation Issues

Sometimes users can face problems with installing the agent on a windows PC for various reasons which may be specific to user environment. You can use the following command line options to troubleshoot installation issue.

From the admin command prompt type:

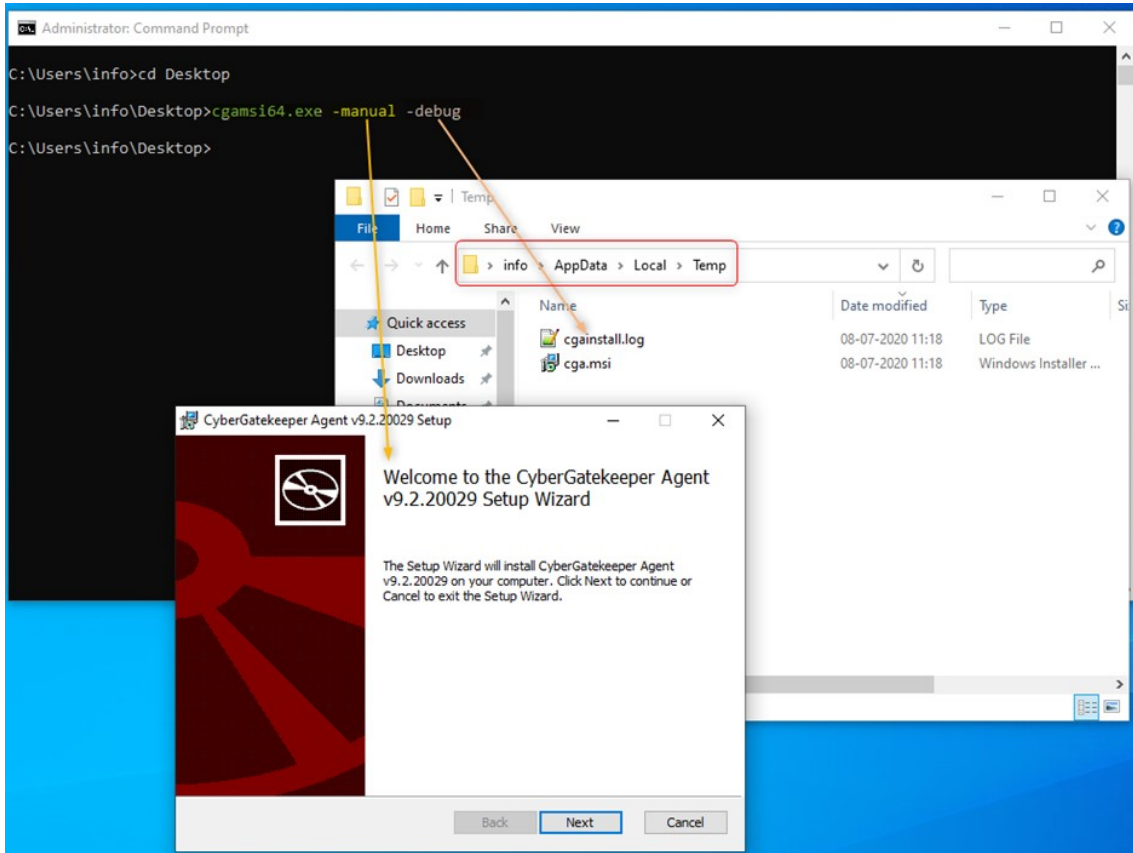
cgamsi32.exe or cgamsi64.exe and use any of the options below:

-debug	Generates installation log at %tmp%\cgainstall.log. <i>You can send this log to support when requiring assistance for installation issues</i>
-log	Enables agent debug logging in agent install dir [filenames=IEXCGAxxxxx.log]
-manual	Interactive install. Shows install window and progress.

For Example:

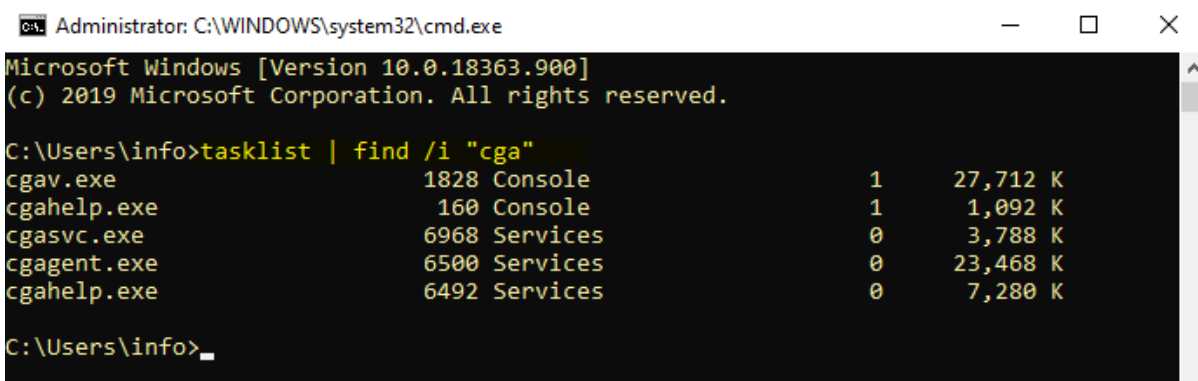
```
> cgamsi64.exe -manual -debug
```

This will start a manual installation with install progress & enable installation debug logging file at %tmp%\cgainstall.log



Once agent is installed, you can check if agent service is running.

```
> tasklist | find /i "cga"
```



Note: For problems installing Linux agents, please contact support for the **Linux agent install guide**.

Connection Issues

Outbound Ports use by CyberGatekeeper Agent:

TCP 11698: Agent Connections to CGX Access appliance

TCP 11697: Agent (NIC Manager) to CGX Access appliance

Once agent is installed correctly, there may be problems with agent connecting to the CGX Access appliance. The easiest way to check error messages is to open the agent window and note the message/warning. By default, the CyberGatekeeper agents are configured to talk with hostnames `cgx-access` and `cgx-access.local`. These values can be changed when building agents. Take note of the CGX-Access IP-address and/or Hostname configured in the agent. (Henceforth referred to as CGXA)

Error/warning seen on CGAgent window	Command to execute on end point CLI/Shell	Objective	Resolution
Failed. Cannot resolve hostname <CGXA>	> nslookup <CGXA>	To check if DNS is correctly resolving CGXA hostname. <i>[if hostname is used while agent building]</i>	Check is your DNS is configured to resolve CGXA hostname
Failed. Unable to connect to CyberGatekeeper <CGXA>	> Ping <CGXA>	to check CGXA reachability <i>(if your firewall allows ICMP)</i>	Check if agent or that network segment can reach CGXA appliance
Failed. Unable to connect to CyberGatekeeper <CGXA>	> telnet CGXA 11698	To check if agent can connect to audit port TCP 11698 on CGXA	Check if Anti-Virus or firewall is blocking TCP port 11698
Cannot establish session with a server from a different administrative domain or server is disabled.			See "different administrative domain error" below.
Failed. CyberGatekeeper indicated failure in audit session.			Agent has failed compliance. Check rules that agent should pass. Checking Device Manager - Reports would help identify why this agent failed compliance.

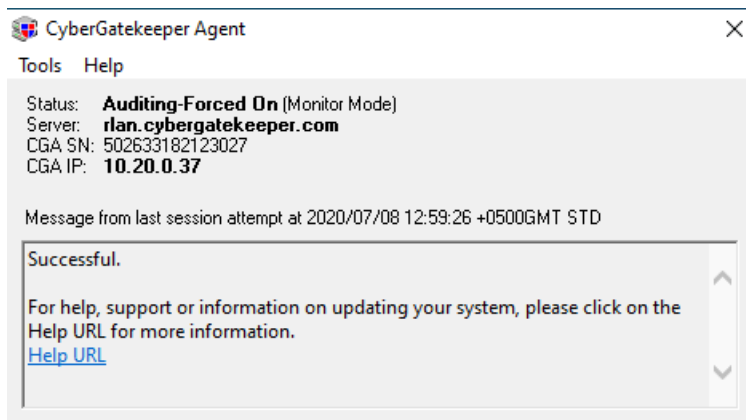
Different Administrative Domain error: This error occurs when the agent and the policy on the CGX Access were built from a different Policy Manager. It can also occur if no policy has been pushed to the CGX Access appliance. The agent and the appliance share a secret key, and this key is generated and provided by the Policy Manager. It is included when the agent is built, and when the policy is uploaded to the appliance. If the keys do not match, the client cannot connect to the appliance.

This can be fixed by any of the following:

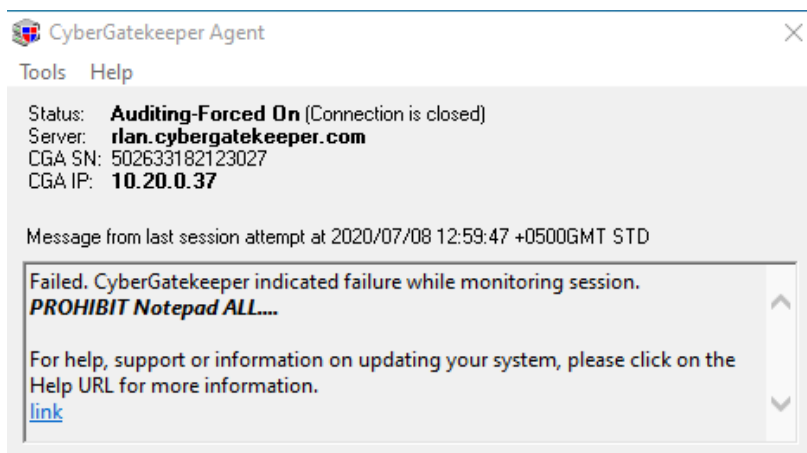
- Uploading the policy to the appliance, from the same Policy Manager that built the agent.
- Import the correct Shared Settings into the Policy Manager and re-upload the policies to CGX Access. (If using default agents, contact support for the default Easy NAC shared settings).
- Re-building and re-distributing the agent from the same system that uploaded the current policy.

Once agent connects to CGX Access appliance successfully, you should see “successful” message in agent window.

- When passing audit (compliant)



- When failing audit (non-compliant)



Advanced Configuration Options

Administration Permissions

CGX Access can query the Active Directory server to validate permissions for administrators to access the management GUI. CGX Access uses management accounts stored in Active Directory. Different levels of access are given to admin users based on their AD group membership.

Administrator roles

Initially there are three roles for administrators configured on a CGX Access: CGX-Admin, CGX-AdminRO and GRM-Sponsor. "CGX-Admin" is a default role that cannot be modified. It has full privileges. "CGX-AdminRO" is the one shown below and can be used for limited administrative privileges. GRM-Sponsor is a group allowed to sponsor guest access. Each permission role can be configured with different access rights. Permission roles may be deleted or added. These roles correspond to groups in Active Directory.

Roles correspond to groups defined in Active Directory, i.e. the administrative user uses their Active Directory credentials to authenticate and is given access based on the group they are a member of in Active Directory. In order for an Active Directory user to be placed into the CGX-Admin role on the CGX Access, the user must be member of an AD group of the same name.

- Go to Configuration → Permission Manager

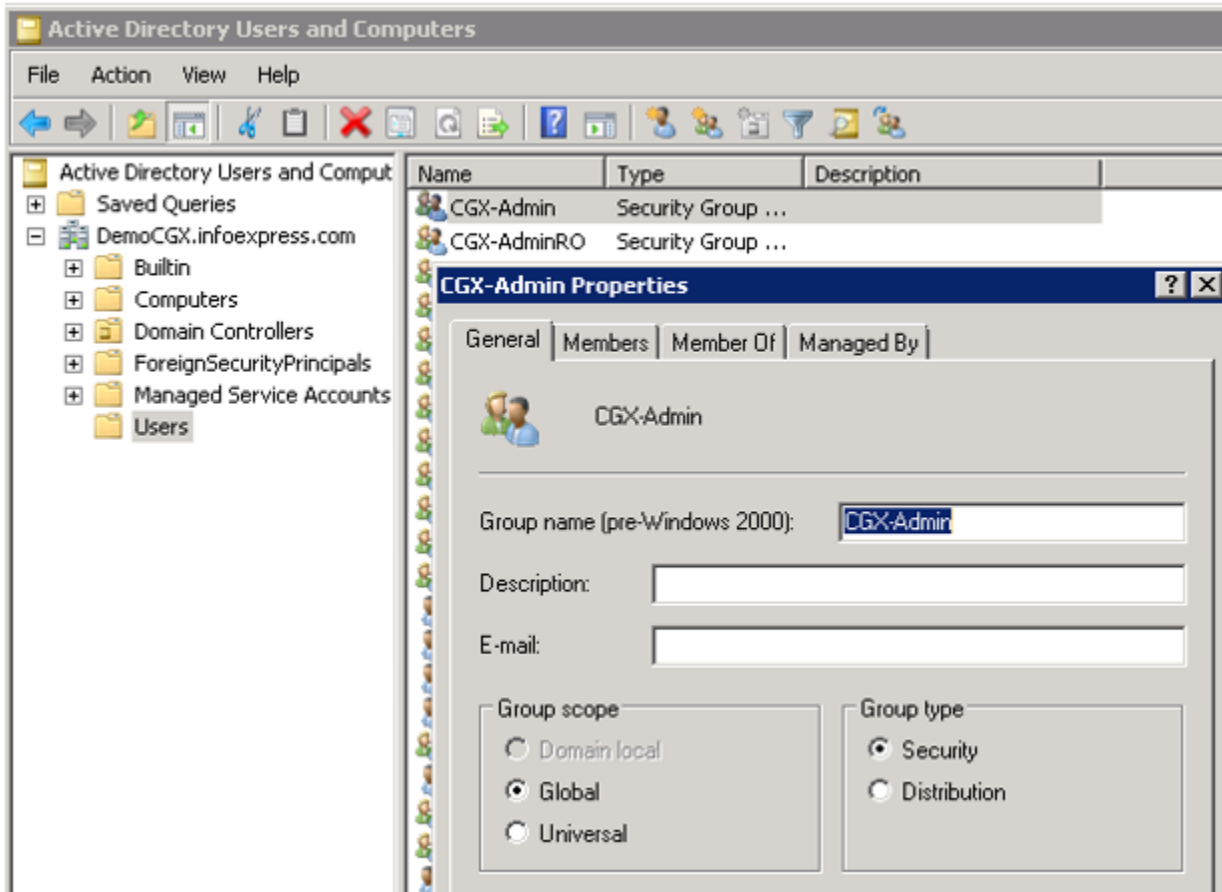
The screenshot shows the 'Permission Manager' interface. At the top, there is a dropdown menu for 'Role' set to 'CGX-AdminRO', with 'Add' and 'Delete' buttons next to it, and a 'Help' link on the right. Below this is a table of permissions categorized into several sections: Accounts, System/Operations, Guests/BYOD devices, Profiler, and Reports. Each permission has three radio button options: 'No access', 'Readonly', and 'R/W'. The 'Readonly' option is selected for most permissions.

Permission	No access	Readonly	R/W
Accounts			
Can create Account, set Permission	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Can force other users out on conflict	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
System/Operations			
Configuration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policies	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Guests/BYOD devices			
Access to Device Registration Templates	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Allow to Sponsor			
<input type="checkbox"/> All guest types			
<input type="checkbox"/> Consultant Register Themselves			
<input type="checkbox"/> 1 day guest			
Access to Device Registration Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Profiler			
Access to Policies	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Reports			
Device Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Create CGX Access admin groups in Active directory

Using the "Active Directory Users and Computers" MMC:

- Add the groups CGX-Admin, CGX-AdminRO and GRM-Sponsor. Please note that upper/lower case is significant when creating these groups.



- As a minimum add one account (your own) to the CGX-Admin group

If you create a new account, make sure it's not set with "User must change password at next logon" as that will prevent the account from being used on the CGX Access until the user changes the password.

Test AD connection

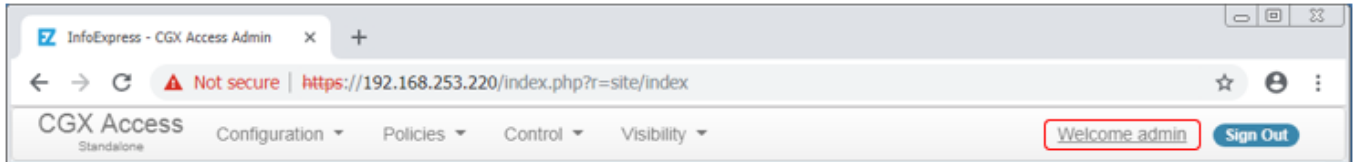
- Log out of the CGX Access admin GUI
- Log in with your AD domain account

If you can authenticate using your AD credentials, then the CGX Access is successfully communicating with the AD domain. If your AD credentials do not work double check that the address of the LDAP server and the account suffix was entered correctly. Also, double check that the changes/additions you made to AD groups have been synchronized to the DC that the CGX Access is connecting to (i.e. the host or IP entered).

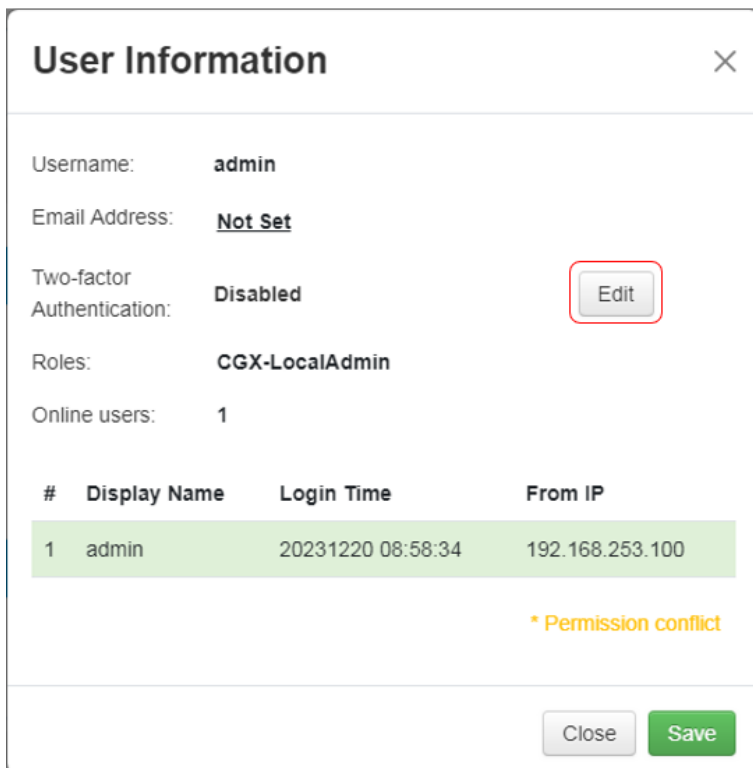
Configuring 2FA for CGX Admin Login

Two-factor authentication can be enabled on CGX-Access accounts, using Time-based One-Time Password (TOTP) apps. **To Enable:**

- After logging in to the CGX Access GUI, click on your user name.



- Click Edit button



- Reconfirm your password




- Select preferred Authentication App and complete the process

Authentication App (TOTP) Setup

Scan this QR code with your app

Scan the QR code below with the two-factor authentication app on your phone.



Provide the used 2FA app's name to remind yourself.

Google Authenticator

- Google Authenticator
- Duo Mobile (Cisco)
- Microsoft Authenticator
- Other

If you can't use QR code, [enter manually](#)

Enter the six-digit code

After scanning the QR code, the app will display a six-digit code that you can enter below.

Please enter your password to continue

- When complete – you will be shown a list of backup codes. Keep these codes in a secure place in case your TOTP application is no longer available.

Configuring Radius for CGX Admin Login or BYOD Authentication

Radius Server Configuration

Note: Free RADIUS server was used in this guide. For specific instructions for Microsoft NPS Radius server please see [Appendix F](#)

- On Radius, Configure CGX Access as a client to allow query
- Add VSA id 2939 in dictionary with following attributes

```
VENDOR InfoExpress 2939
BEGIN-VENDOR InfoExpress
ATTRIBUTE iexgroup 11 string
END-VENDOR InfoExpress
```

- Add user, and assign a group. See more on groups in CGX settings later in this guide.

```
zeeshan Cleartext-Password := "zeeshan"
Service-Type = Framed,
Framed-Protocol = PPP,
iexgroup = CGX-AdminRO
```

CGX-Access Configuration

- Go to Configuration → General → Servers → Radius Server
- Configure your Radius Server details (PAP or MSCHAPv2)

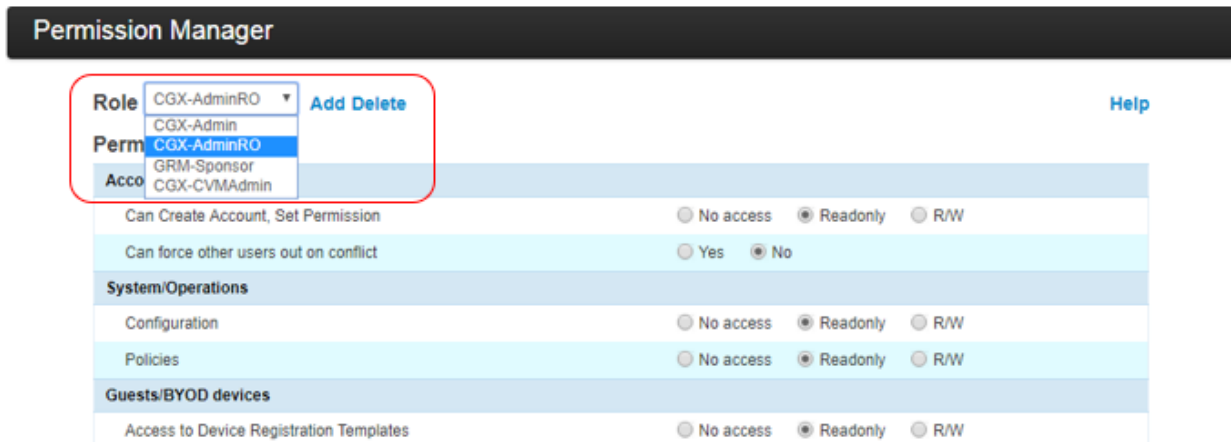
The screenshot shows a window titled "Edit Setting" with a close button (X) in the top right corner. Below the title bar is a tabbed interface with six tabs: "Active Directory Servers", "RADIUS Server", "DHCP Servers", "Mail Server", "Web Proxy Server", and "SMS Gateway". The "RADIUS Server" tab is selected. The main content area is titled "RADIUS Server" and contains the following fields and options:

- Host or IP:** A text input field containing "radius.s1.com".
- Secret:** A text input field filled with 12 asterisks.
- Authentication type:** A dropdown menu with "MSCHAPv2" selected.
- Use for BYOD Authentication:** An unchecked checkbox.
- Use for CGX Access-ADMIN Authentication:** A checked checkbox.

At the bottom right of the dialog, there are three buttons: "Save", "Cancel", and "Help".

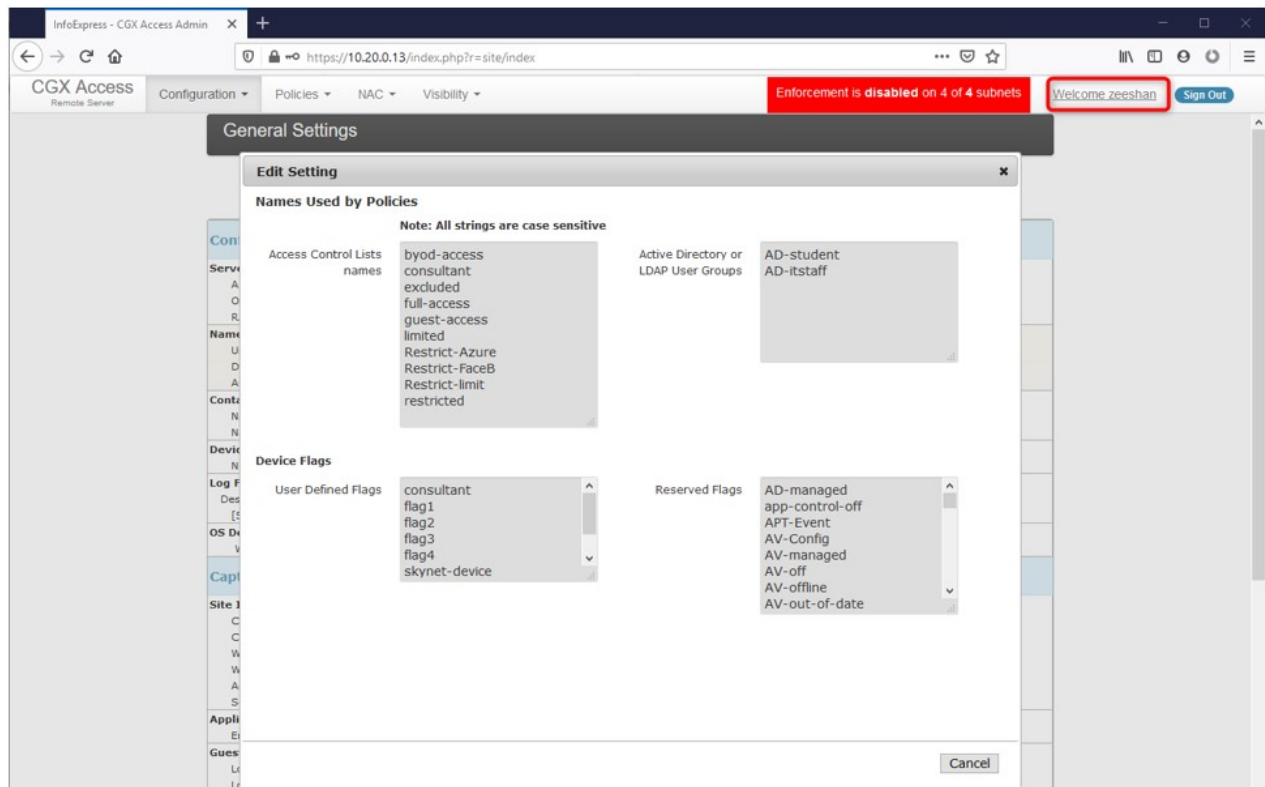
For assigning group level permissions, you can either use predefined groups or create your own group with custom permissions.

- Go to Configuration → Permission Manager



Note: The same group should be assigned and returned with radius VSA 2939 discussed above

- Save changes and log out
- Login in with user defined on Radius server
- Verify the permissions granted to the user



In the above example, user “zeeshan” is a read-only user and cannot make any changes to the above settings.

Customizing Landing Pages

CGX Access provides customization in two ways. Text fields can be edited through the main configuration interface (see Configuration → General Settings). The styles of the landing pages by modifying the CSS (cascading style sheet). Steps to create such a CSS can be found below.

CSS files govern the look and feel of the landing pages only. The GRM theme (landing page theme) is generated from LESS source files (see: <http://lesscss.org> for additional info on LESS).

Obtain a LESS editing program

LESS files are text-based files and any text editor can be used. "Crunch" (www.cruchapp.net) is recommended, as it includes a CSS compiler for LESS files. Other options, such as "Sublime" (www.sublimetext.com) + less2css plugin and an accompanying compiler can be used as well.

Download LESS files

A basic set of LESS files can be obtained from Infoexpress support. It will contain a base set of LESS files which can be compiled into a main.css and accompanying image files (see below)

Edit .less files as desired

After downloading and decompressing the less files, open them in the editor and make changes as desired. Below are some locations of parameters that can be changed

File	Description
main.less	Main file that links to sub-files with additional settings
variables.less	This file contains many of the default colors and images used
header.less	Contains settings for the top part of the pages
footer.less	Settings for the bottom of pages
button.less	Settings for buttons
mobile.less	Settings for pages in a small browser

Settings for individual pages can be found in the /page directory.

"Crunch" (compile) main.css files

When satisfied with the changes made, the *main.less* file should be compiled (it will invoke all the other files specified). The output file should be called *main.css*

Note: The compiler may place the main.css file in the same directory as the .less files.

Upload CSS and images to CGX Access

When done, the *main.css* file, as well as the images directory should be uploaded to the CGX Access through FTP using the *cguser* account. Below is the directory structure that should be present on the CGX Access

Path			Contents
/updates	/grm-theme	/css	contains the <i>main.css</i> file
		/images	contains the images referenced by the <i>css</i> file

Only the *main.css* file and images are needed on the CGX Access, The *.less* files do not need to be uploaded

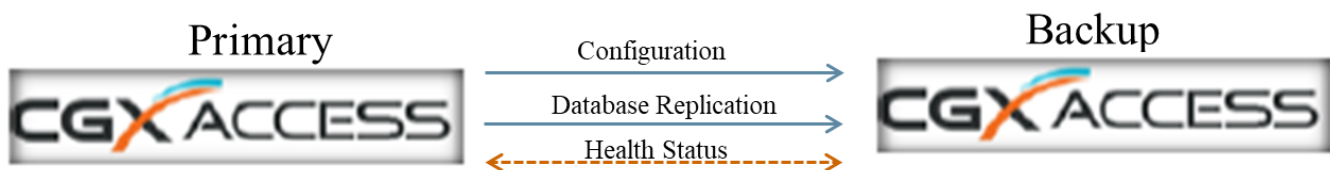
After uploading the files, the CGX Access will automatically pull these files and update the landing pages. No further commands are needed to update the pages. Please allow a few seconds for this action to complete.

High Availability

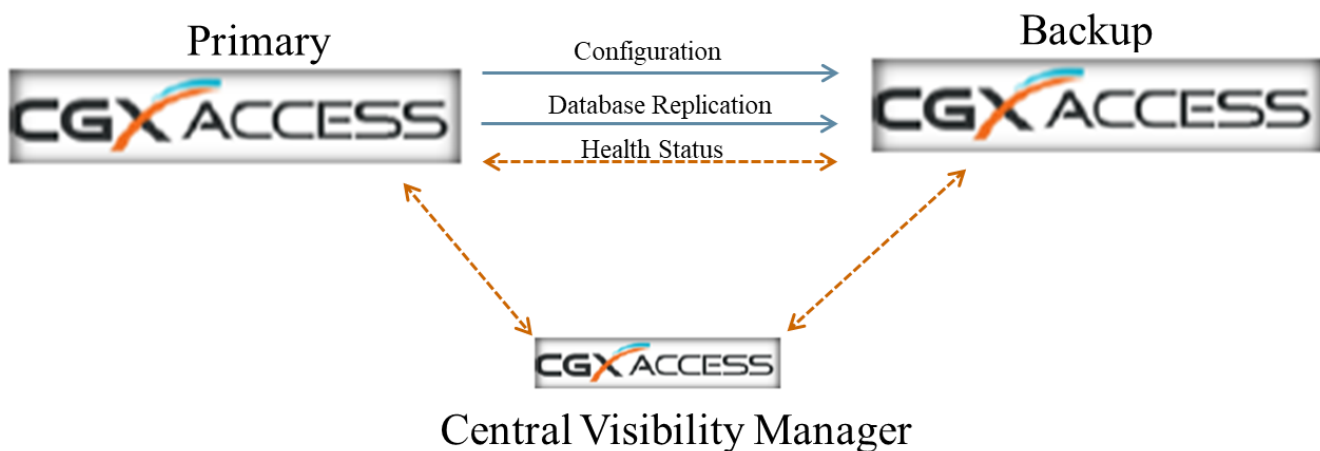
Overview

The High Availability option provides redundancy in the event an appliance or virtual appliance was to fail or be offline. HA is provided using a two-box design, where the Primary appliance syncs its database and configuration with a passive Backup appliance. If the Backup appliance determines the Primary appliance is offline, it will become active.

When the Primary appliance comes back online, the Backup will sync the configuration and database back to the Primary, and the Primary will become active again.



In environments that have Centrally Managed Appliances, the Central Visibility Manager can be configured to be an arbiter to participate in the decision of which appliance should be active.



Requirements

- An HA license is required
- The Backup appliance must use the same physical appliance type or same hypervisor. Mixing and matching of physical \ virtual appliances is not supported.
- The appliances trunk port configurations should be similar, but with unique IP addresses
- The Primary and Backup appliances should be deployed on the same VLAN
- Appliances must be able to ping its default gateway
- Appliances should not be configured for Inline Enforcement (a different HA design is recommended for Inline appliances)
- If configured with the CVM as the arbiter, each appliance pair will use a unique arbiter port

Configuration – Standalone Appliances

These configuration steps for setting-up HA with two appliances are simple, but must be done in the correct order.

1. Disable Enforcement (Use monitor mode on each VLAN)
2. Configure the Primary unit
3. Configure the Backup unit
4. Re-enable enforcement (as desired)

Tip: Before configuring HA, have a recent backup of the Primary Appliance.

Configure the Primary unit

The Primary unit is the main appliance where configurations are made.

Note: If the Primary unit is already in production, then Enforcement should be placed in Monitor mode until the HA setup is complete.

- In CGX Access GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" from Standalone Appliance to Standalone Appliance - HA mode

Site Settings:

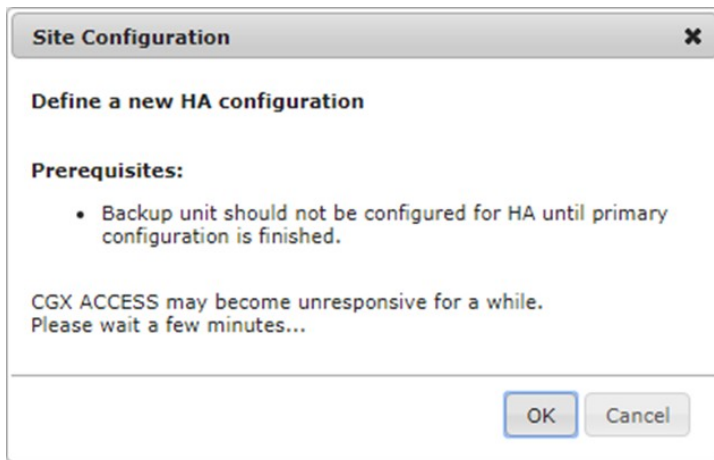
CGX Access Server Mode:	Standalone Appliance - HA mode ▼
HA Configuration:	Standalone Appliance
Primary CGX Access Server	Standalone Appliance - HA mode
Peer CGX Access Address	Centrally Managed Appliance
	Centrally Managed Appliance - HA mode
	Central Visibility Manager
	Central Visibility Manager - HA mode
	MSP Manager
	MSP Manager - HA mode

- Check box to make Primary CGX Access Server
- Configure the IP address of the backup appliance (Peer CGX Access Address)

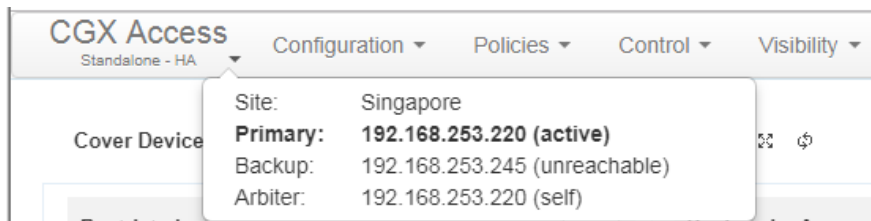
Site Settings:

CGX Access Server Mode:	Standalone Appliance - HA mode ▼
HA Configuration:	
Primary CGX Access Server	<input checked="" type="checkbox"/>
Replacement for existing primary	<input type="checkbox"/>
Peer CGX Access Address	192.168.253.245
External Arbiter:	<input checked="" type="radio"/> None <input type="radio"/> Other designated
Manual failover	None ▼
	<input type="button" value="Submit Server Mode"/>

- Click **Submit Server Mode**. You will be warned that the Backup should **not** already be configured. It's OK for the backup unit to be on the network, but it should not yet be configured for HA.



- You will be logged out of CGX-Access and the changes will take effect. Please wait 2-5 minutes before logging back in.
- Within 2-5 minutes the Primary appliance will be in HA mode.



Note: The Backup will not be reachable until it has also been configured for HA

Configure the Backup unit

The Backup unit will pull its configuration from the Primary unit, so only IP Addresses and network configurations need to be pre-configured. Except for the appliance's IP addresses, other network settings should be identical.

Note: Before configuring the Backup unit, the Primary unit must first be configured for HA, as instructed above.

- In CGX Access GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" from Standalone Appliance to Standalone Appliance - HA mode

Site Settings:

CGX Access Server Mode: Standalone Appliance - HA mode

HA Configuration:

Primary CGX Access Server

Peer CGX Access Address

- Standalone Appliance
- Standalone Appliance - HA mode
- Centrally Managed Appliance
- Centrally Managed Appliance - HA mode
- Central Visibility Manager
- Central Visibility Manager - HA mode
- MSP Manager
- MSP Manager - HA mode

- In the “Peer CGX Access Address” configure the IP address of the Primary appliance

Site Settings:

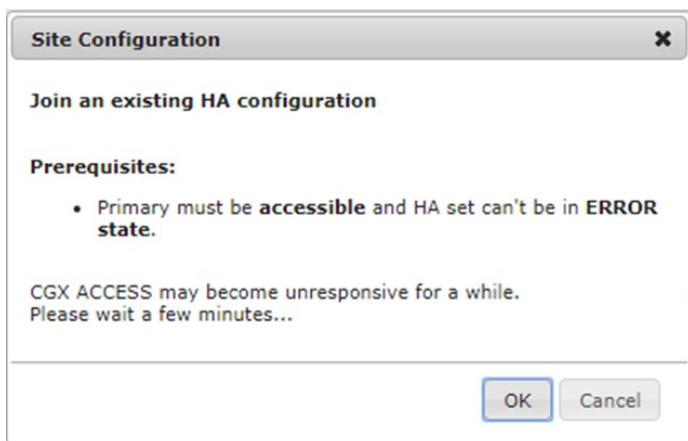
CGX Access Server Mode: Standalone Appliance - HA mode

HA Configuration:

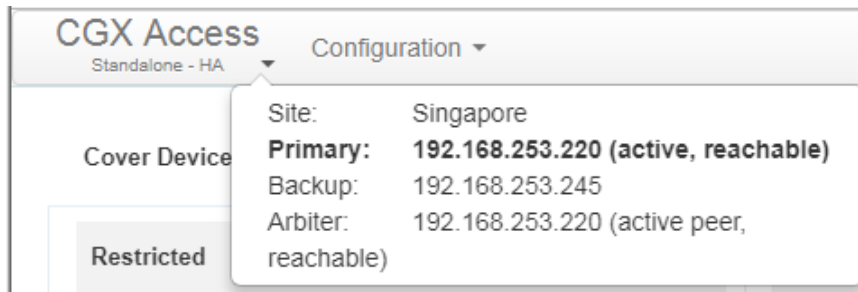
Primary CGX Access Server

Peer CGX Access Address

- Click **Submit**. You will be warned that the Primary unit should be in HA mode and in working state.



- You will be logged out of CGX-Access and the changes will take effect. The configuration and database will be sync'd from the Primary. This will take some time, so please wait 5-10 minutes before logging back in.
- Within 5-10 minutes the appliance will be in HA mode and show the Primary as Active.



Note: When in Backup mode, only the Configuration menu will be available.

Configuration – Centrally Managed Appliances

These configuration steps for setting-up HA with Centrally Managed appliances are simple, but must be done in the correct order.

1. Configure the CVM to be an Arbiter (optional)
2. Disable Enforcement (Use monitor mode on each VLAN)
3. Configure the Primary unit
4. Configure the Backup unit
5. Re-enable enforcement (as desired)

Tip: Before configuring HA, have a recent backup of the Primary Appliance.

Configure the CVM to be an Arbiter (optional)

In environments that have Centrally Managed Appliances, the Central Visibility Manager can be configured to be an arbiter to participate in the decision of which appliance should be active.

Note: In environments with reliable network connectivity to the CVM, having the CVM provide this independent arbiter functionality is recommended. However, if connectivity is inconsistent this could prevent the fail-over to the backup unit from occurring. Therefore, in environments with inconsistent connectivity, it's best not to use the CVM as an arbiter.

- In CVM go to Configuration → Appliance Settings
- Scroll down to Site Settings and click "Configure"

Site Settings:

CGX Access Server Mode:	Central Visibility Manager
Site Name	Central Visibility Manager
Inter-CGX Access Communication:	Configure (for old version CGX Access to connect to)
Arbiter Instances:	Configure
	<input type="button" value="Submit Server Mode"/>

- Select “New Arbiter Instance(s)”

Arbiter Instances:

Close
New Arbiter Instance(s)

Port	Bound to	Status	Action
Submit Server Mode			

- Configure a unique port for each appliance pair. If there will be 3 HA sets of appliances, then configure 3 unique ports, starting from port 27019.

Close
New Arbiter Instance(s)

Port	Bound to	Status	Action
27019		Listen	
27020		Listen	
27021		Listen	

Submit Server Mode

- Click “Submit Server Mode” to save changes

Site Settings:

CGX Access Server Mode: Central Visibility Manager ▼

Site Name: Central Visibility Manager

Inter-CGX Access Communication: [Configure](#)(for old version CGX Access to connect to)

Arbiter Instances: [Configure](#)27019,27020,27021

Submit Server Mode

Configure the Primary unit

The Primary unit is the main appliance where configurations are made.

Note: If the Primary unit is already in production, then enforcement should be placed in Monitor mode until HA setup is complete.

- In CGX Access GUI, go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" to Centrally Managed Appliance - HA mode

Site Settings:

CGX Access Server Mode:	Standalone Appliance Standalone Appliance Standalone Appliance - HA mode Centrally Managed Appliance Centrally Managed Appliance - HA mode Central Visibility Manager Central Visibility Manager - HA mode MSP Manager MSP Manager - HA mode
Services:	
SSH Service	
SNMP Server	

- Input a Site Name (often a location name)
- Input the correct CVM IP address
- Check box to make Primary CGX Access Server
- Configure the IP address of the Backup appliance (Peer CGX Access Address)
- If using CVM as an Arbiter than specify one unique port that had been configured on the CVM. (optional)

Site Settings:

CGX Access Server Mode:	Centrally Managed Appliance - HA mode
Site Name	Singapore
CVM or MSP Manager host or IP. (For HA, separate hosts or IPs with a comma)	10.10.10.100
HA Configuration:	
Primary CGX Access Server	<input checked="" type="checkbox"/>
Replacement for existing primary	<input type="checkbox"/>
Peer CGX Access Address	192.168.253.245
External Arbiter:	<input type="radio"/> None <input checked="" type="radio"/> CVM <input type="radio"/> Other designated
Arbiter Port	27019
	<input type="button" value="Submit Server Mode"/>

- Click **Submit Server Mode**. You will be warned that the Backup should not be configured. It's OK for the backup unit to be on the network, but it should not yet be configured for HA.

Site Configuration [X]

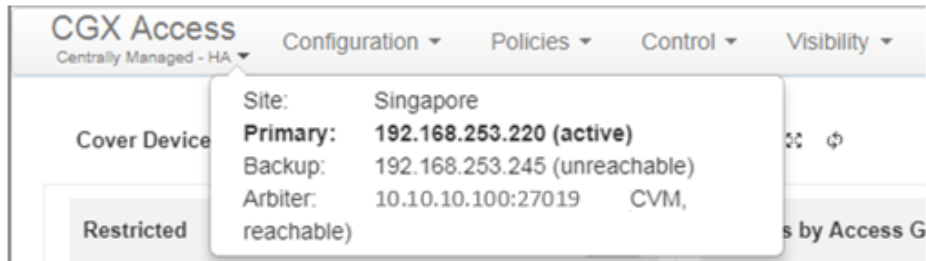
Define a new HA configuration

Prerequisites:

- Backup unit should not be configured for HA until primary configuration is finished.
- The arbiter instance on CVM(10.10.10.100:27019) must be running for this HA.

CGX ACCESS may become unresponsive for a while.
Please wait a few minutes...

- You will be logged out of CGX-Access and the changes will take effect. Please wait 2-3 minutes before logging back in.
- Within 2-3 minutes the Primary appliance will be in HA mode.



- Confirm the Arbiter is reachable.

Note: The Backup will not be reachable until it has also been configured for HA.

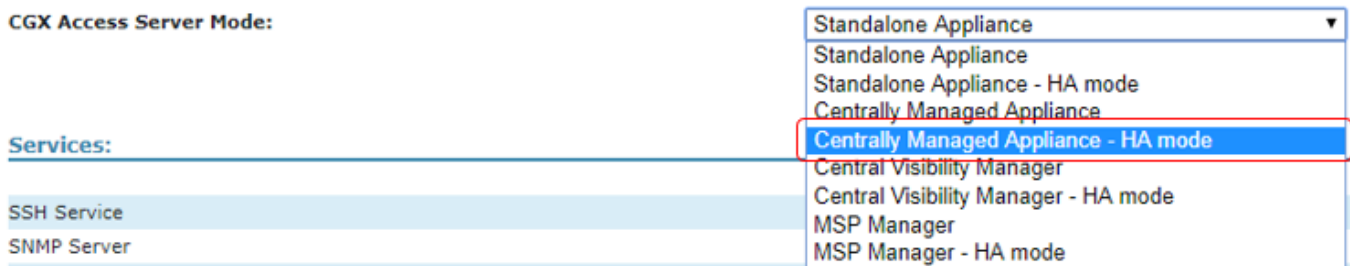
Configure the Backup unit

The Backup unit will pull its configuration from the Primary unit, so only IP Addresses and network configurations need to be pre-configured. Except for the appliance's IP addresses, other network settings should be identical.

Note: Before configuring the Backup unit, the Primary unit must first be configured for HA.

- In CGX Access GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" to Centrally Managed Appliance - HA mode

Site Settings:

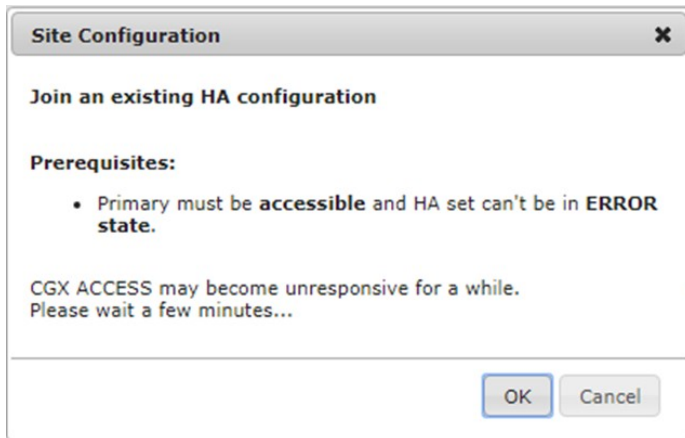


- In the "Peer CGX Access Address" configure the IP address of the Primary appliance

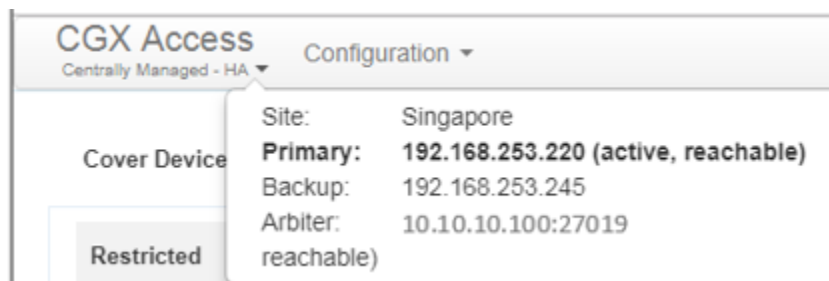
Site Settings:



- Click **Submit Server Mode**. You will be warned that the Primary unit should be in HA mode and in working state.



- You will be logged out of CGX-Access and the changes will take effect. The configuration and database will be sync'd from the Primary, so please wait 5-10 minutes before logging back in.
- Within 5-10 minutes the appliance will be in HA mode and show the Primary as Active.



Note: When in Backup mode, only the Configuration menu will be available.

- Login into the Central Visibility Manager, and select Appliance tab to verify HA status is shown correctly.

CGX Access Servers

Site	Management IP	Mode	Last Reported
Central Visibility Manager	10.10.10.100	CVM	● n/a
Singapore	192.168.253.220	HA Primary - Active	● 1 minute ago
Singapore	192.168.253.245	HA Backup	● 4 seconds ago

Making HA Configuration Changes

If it's necessary to make changes to a working HA setup, please be sure to follow the steps outlined below:

Replace a Primary

1. Make sure the original Primary is offline or off HA (i.e., standalone)
2. If new Primary has a different IP than the original one, change peer on Backup to the new IP
3. Configure the new Primary (check "Replacement for existing Primary")
4. No need to change arbiter configuration

Replace a Backup

1. Make sure the original Backup is offline or off HA (i.e., standalone)
2. If new Backup has a different IP than the original one, change peer on Primary to the new IP
3. Configure the new Backup
4. No need to change arbiter configuration

Restore from a Backup Image

1. Disable Enforcement
2. Change Backup to Standalone mode
3. Restore Primary
4. Rejoin Backup to HA
5. Re-enabled Enforcement

Upgrade to a New Version

1. Disable Enforcement
2. Change Backup to Standalone mode
3. Update Primary, Backup
4. Rejoin Backup to HA
5. Re-enabled Enforcement

Other Reconfiguration Changes

1. Convert both members of the HA to standalone
2. Remove the arbiter port if using CVM arbiter

Arbiter Instances:

The screenshot shows a configuration window titled "New Arbiter Instance(s)". It contains a table with the following data:

Port	Bound to	Status	Action
27019		Listen	

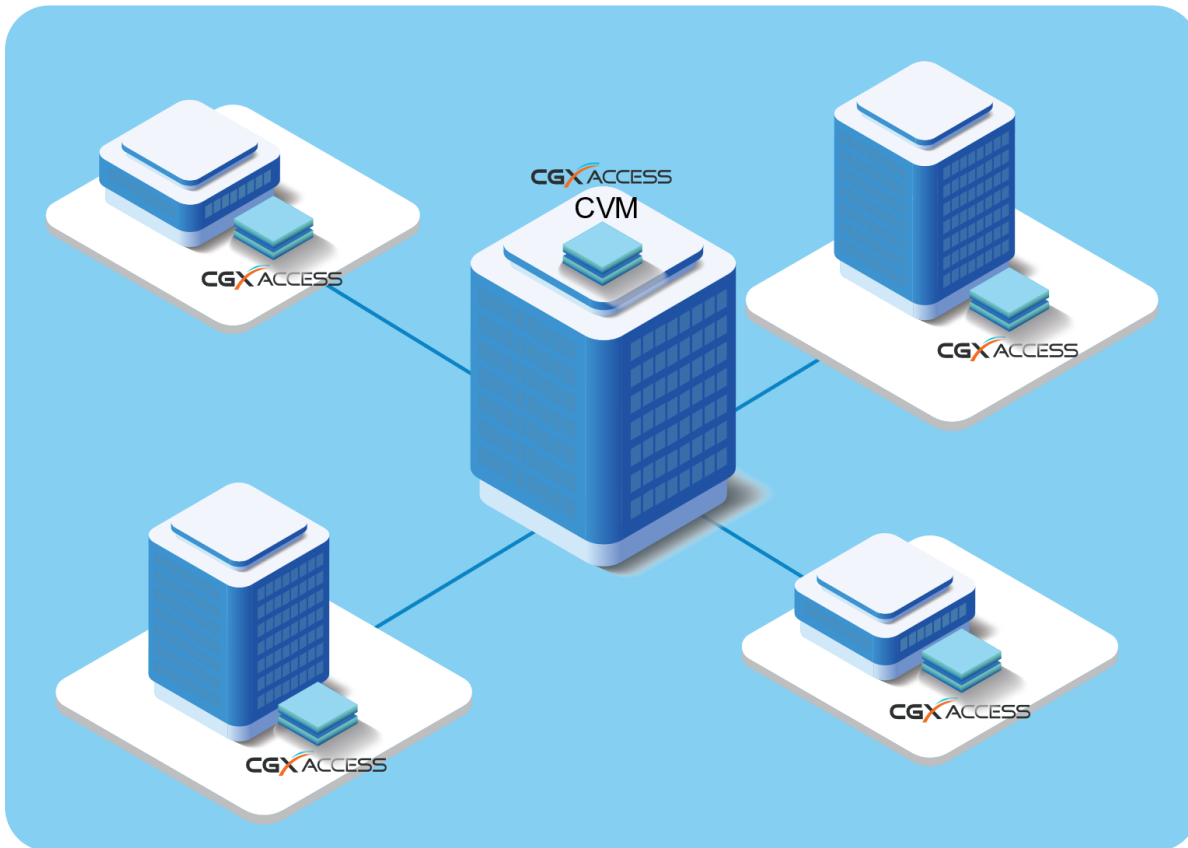
Below the table is a button labeled "Submit Server Mode".

3. Create HA from scratch

Central Visibility Manager

CVM Overview

It's common to deploy multiple CGX Access appliances in multiple offices. In these scenarios where more than one CGX Access appliance is deployed it is beneficial to use the Central Visibility Manager (CVM) for an organization-wide visibility and management of these appliances.



The Central Visibility Manager doesn't perform monitoring and enforcement actions itself. It's used for consolidated reporting and management of multiple appliances.

Required Ports

For normal operation the following ports should be allowed between the centrally managed appliances and CVM:

TCP 443 – Administrative GUI and Synchronization

TCP 10101 – for Synchronization

It may also be necessary to allow TCP 21 from a management subnet to the centrally managed appliances, so agent policies and software updates can be uploaded to the distributed appliances. See table below:

	Traffic Direction	Central Visibility Manager (CVM)	Centrally Managed Appliance (Primary)	Centrally Managed Appliance (Backup)
Central Visibility Manager (CVM)				
Centrally Managed Appliance (Primary)	→	TCP 10101 TCP 443 TCP xxxx (arbiter)*		TCP 10120
Centrally Managed Appliance (Backup)	→	TCP 10101 TCP 443 TCP xxxx (arbiter)*	TCP 10120	
Jump Server \ Policy Manager PC	→	TCP 443 TCP 21	TCP 443 TCP 21	TCP 443 TCP 21

*If CVM is configured as the arbiter in HA setups.

Configuring a Central Visibility Manager

The Central Visibility Manager uses the same appliance image as the normal CGX Access appliance, so the initial setup will be like setting up a CGX Access appliance.

Note: The CVM is licensed separately and has a unique CVM license required to operate.

Basic IP configuration

- For physical appliances, use a direct connect ethernet cable for SSH access to the default IP Address 10.0.0.250/24. Alternatively, plug-in a keyboard and HDMI monitor.
- For virtual appliances open a console window and power on the VM.

Once the boot cycle is complete you will be prompted for a login.

- Login as admin/admin.
- From the main menu choose 1 (Run setup wizard) and follow the prompts to set the Managed IP address and netmask, the default gateway, DNS servers, system name, time zone and date/time.

Note: Keep the admin password in a safe place. If it is lost, without having access to an alternate admin level account, there will be no way to recover the password.

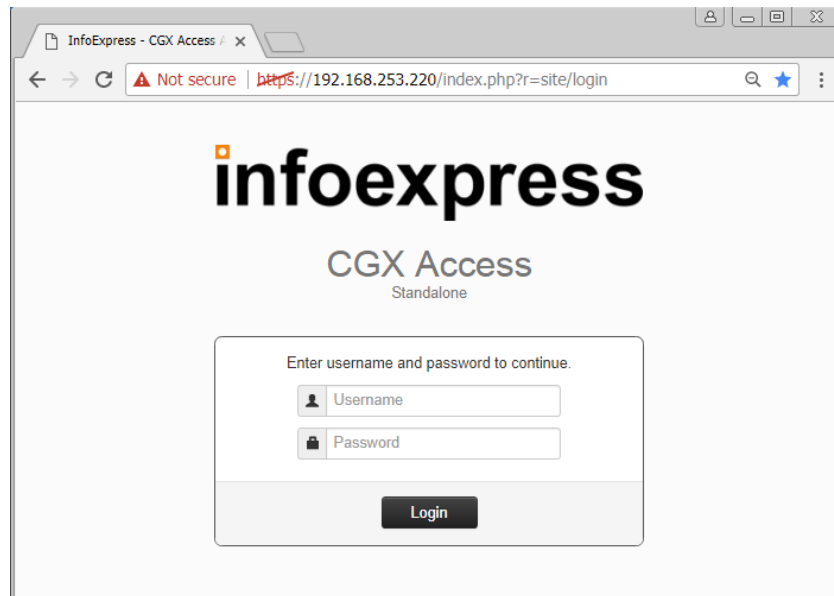
Default user accounts are:

- admin - used for initial setup and configuration as well as SSH access for maintenance tasks
- cguser - used for uploading files through ftp

The default passwords are the same as the username

When the setup wizard completes, the system should be accessible on the network.

- Confirm that you can ping the management IP from another system on the same subnet and also from a system on another subnet. If the pings fail double check the physical or virtual connections and the basic IP configuration
- Connect to the CGX Access web GUI by opening <https://<Managed ip>> (that was configured previously)



Login as user admin (default password admin). A modern browser such as Chrome is strongly recommended. Older versions of IE or Firefox may not display the pages correctly.

Using the web GUI additional setting can be configure:

- (Optional) Active Directory server settings (used for Permission Management)
- (Optional) E-mail & SMS server settings (used for alerting)
- **(Required)** Add license for Central Visibility Manager



1. In CGX Access GUI go to Configuration → License Manager
2. Click on "[New License](#)"
3. Paste the key into the space provided and apply

License Manager

License Type	Distributed deployment
Maximum Appliance Number	3
Device License	500
Licenses allocated	210
Licenses used	6
Licensed to	For Evaluation Purpose Only

The License Manager will show the maximum number of GX Access appliances that CVM can manage. If using a Distributed license, you will also see the number of devices that can be managed, and the current allocation of the license. With the distributed license, customers can allocate the license across different appliances, as shown below.

License Utilization

Site	IP Address	Licenses Allocated	Licenses Used	
Manila	192.168.253.220	200	3	
Singapore	192.168.253.230	10	3	

Once the initial configuration is done the new server can be switched to a Central Visibility Server.

- In CGX Access GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" from Standalone Appliance to Central Visibility Manager

Site Settings:

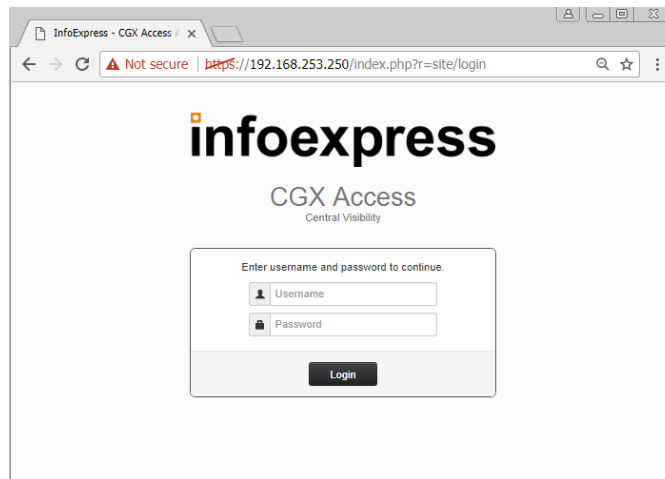
CGX Access Server Mode:	Central Visibility Manager ▼
Site Name	Standalone Appliance
Inter-CGX Access Communication:	Standalone Appliance - HA mode
Arbiter Instances:	Centrally Managed Appliance
	Centrally Managed Appliance - HA mode
	Central Visibility Manager
	Central Visibility Manager - HA mode
	MSP Manager
	MSP Manager - HA mode

- Set both the Site name.
 - If left blank the site name will be the default of Central Visibility Manager
 - Site Name should only consist of the characters A-Z, a-z, 0-9, and _

Site Settings:

CGX Access Server Mode:	Central Visibility Manager
Site Name	Central Visibility Manager
Inter-CGX Access Communication:	Configure (for old version CGX Access to connect to)
Arbiter Instances:	Configure
	<input type="button" value="Submit Server Mode"/>

- Click **Submit Server Mode**. You will be logged out of CGX-Access and the changes will take effect.



Configuring an Appliance to be Centrally Managed

Once a Central Visibility Manager has been configured, new or existing standalone CGX Access appliances can be configured to be manageable from CVM.

If the CGX-Access appliance will be a new deployment and not a conversion of an existing Standalone appliance, first perform an Initial Configuration as covered on Page 14. At a minimum, the appliance should have:

- Have a primary IP address assigned
- Have a Host name
- Have a DNS server

Once the server has a basic configuration it can be switched to a Centrally Managed Appliance:

- In CGX Access GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" from Standalone Appliance to Centrally Managed Appliance

Site Settings:

CGX Access Server Mode:	Central Visibility Manager
Site Name	Standalone Appliance
Inter-CGX Access Communication:	Standalone Appliance - HA mode
Arbiter Instances:	Centrally Managed Appliance
	Centrally Managed Appliance - HA mode
	Central Visibility Manager
	Central Visibility Manager - HA mode
	MSP Manager
	MSP Manager - HA mode

- Set the Site name and Central Visibility Manager IP Address.
 - Site Name should only consist of the characters A-Z, a-z, 0-9, and _

Site Settings:

CGX Access Server Mode:	Centrally Managed Appliance
Site Name	Singapore
CVM or MSP Manager host or IP. (For HA, separate hosts or IPs with a comma)	10.10.10.100
	<input type="button" value="Submit Server Mode"/>

- Click **Submit Server Mode**. You will be logged out of CGX-Access and the changes will take effect.
- Within two minutes device data should be replicated to the Central Visibility Manager.

Note: If the CVM is configured for High Availability, input both IP addresses separated with a comma, no space.

Site Settings:

CGX Access Server Mode:	Centrally Managed Appliance
Site Name	Singapore
CVM or MSP Manager host or IP. (For HA, separate hosts or IPs with a comma)	10.10.10.100,10.10.10.200
	<input type="button" value="Submit Server Mode"/>

Deployment Manager

The Central Visibility Manager includes a Deployment Manager that is used to accelerate deployments or configuration changes among different CGX Access appliances.

- In CVM GUI go to Configuration → Deployment Manager
- Create a Deployment Set

Deployment Manager

Use this to selectively synchronize configuration including settings and policies among remote CGX ACCESS

Deployment Set



Contents

Name: Singapore Settings

Source: Singapore (192.168.253.2)

Include [Select all](#) [Clear all](#)

<input checked="" type="checkbox"/> General Settings	<input checked="" type="checkbox"/> Device Registration Methods
<input checked="" type="checkbox"/> Integrations	<input checked="" type="checkbox"/> Device & Roles Classification
<input checked="" type="checkbox"/> Roles & Access	<input checked="" type="checkbox"/> Time/Location/List
<input checked="" type="checkbox"/> Device Events	<input checked="" type="checkbox"/> Monitoring
<input checked="" type="checkbox"/> Device Profiler	<input checked="" type="checkbox"/> ACL

1. Specify a name
2. Select the Source appliance to copy the settings from
3. Choose which settings to include in the Deployment set
4. Click Save

- Push a Deployment Set
1. Select a Deployment Set
 2. Select the location(s) to push to
 3. Click Push

Deployment Manager

Use this to selectively synchronize configuration including settings and policies among remote CGX ACCESS

Deployment Set

New...

Singapore Settings

Contents

Name Singapore Settings

Source 192.168.253.220

Include

<input checked="" type="checkbox"/> General Settings	<input checked="" type="checkbox"/> Device Registration Methods
<input checked="" type="checkbox"/> Integrations	<input checked="" type="checkbox"/> Device & Roles Classification
<input checked="" type="checkbox"/> Roles & Access	<input checked="" type="checkbox"/> Time/Location/List
<input checked="" type="checkbox"/> Device Events	<input checked="" type="checkbox"/> Monitoring
<input checked="" type="checkbox"/> Device Profiler	<input checked="" type="checkbox"/> ACL

Push selected to [Select all](#) [Clear all](#)

Singapore (192.168.253.220)

London (192.168.253.230)

4. Confirm the Push

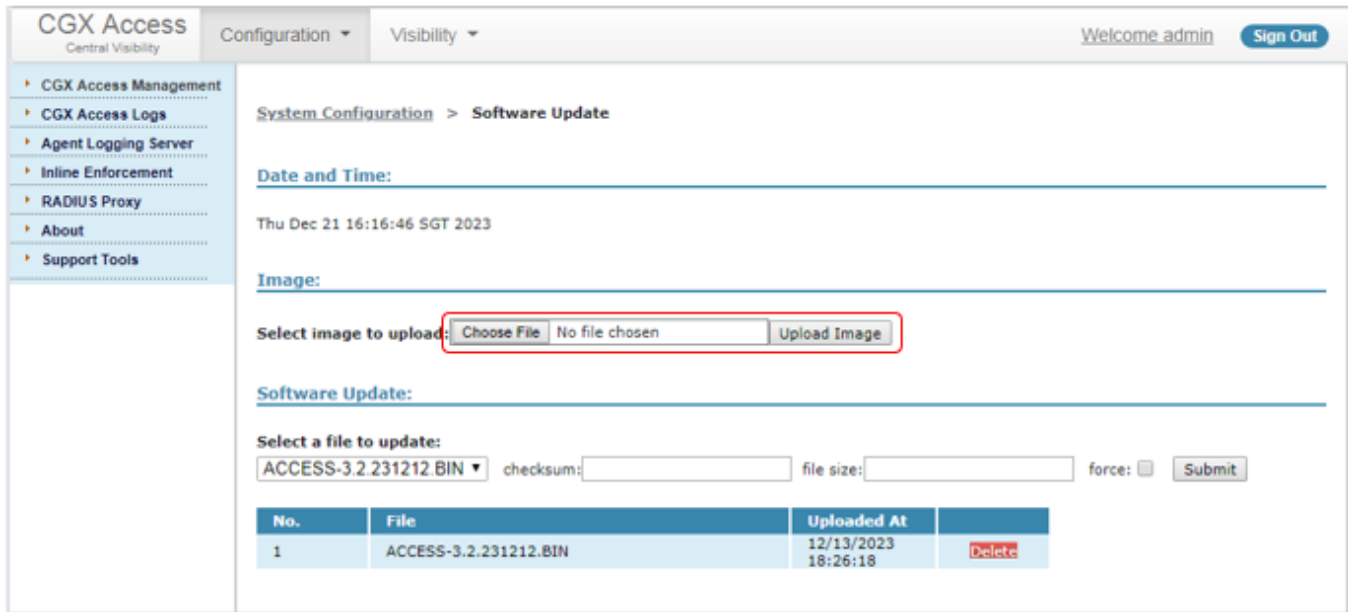
Confirmation

Do you want to push the deployment set?

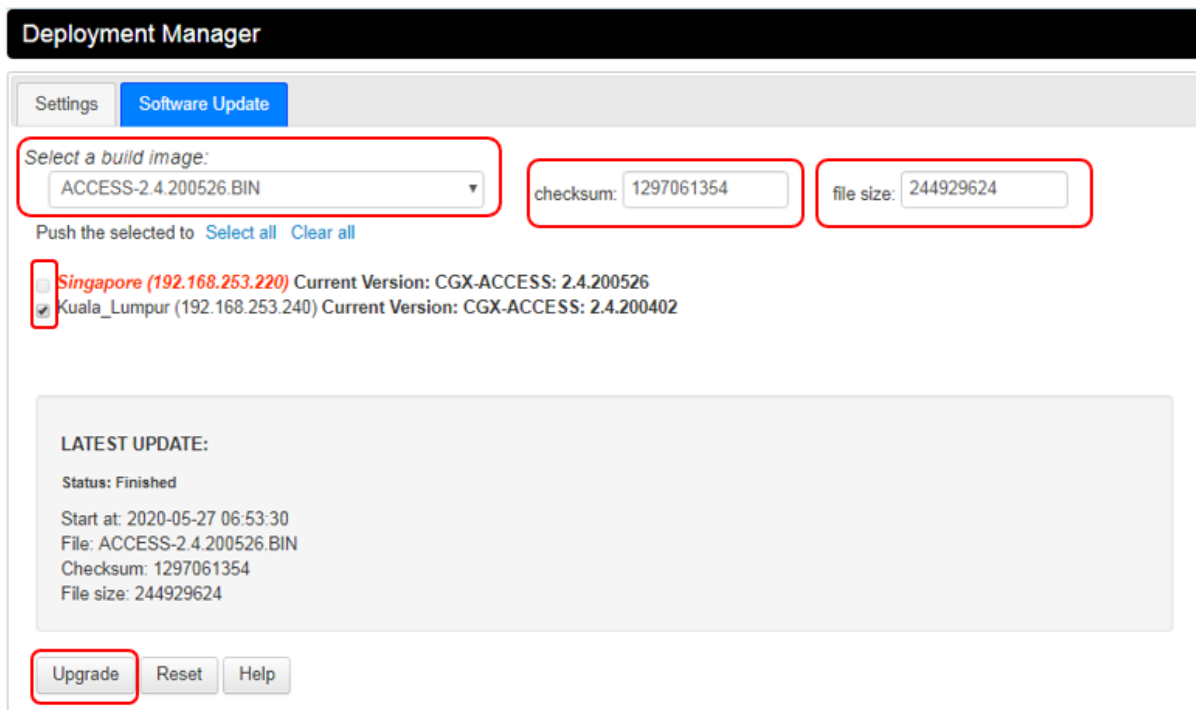
Software Updates

Deployment Manager can also be used to update software across multiple appliances at the same time.

- In CGX Access, go to Configuration → Appliance Settings
- Scroll down to Server Maintenance → Software Update
- Browse to location of file and upload the image



- Once uploaded, go to Configuration → Deployment Manager → Software Update tab
- Choose the correct image, complete checksum: and file size:
- Select the appliances to be upgraded and click **Upgrade**



The images will be downloaded to the appliances and if the Checksum and file size are accurate, each appliance will be upgraded. Allow 15-30 minutes for upgrades to occur. The appliances will be rebooted after the upgrade is complete.

Central Visibility Manager – Device Roaming

The Central Visibility Manager maintains a list of all devices that are connected to the extended enterprise. This list can be used to facilitate device roaming between locations. There is no setup required on the CVM itself. Each CGX Access Remote can be configured to control which type of devices and from what locations are allowed to connect.

- In CGX Access, go to Configuration → Integration → Central Visibility Manager – Roaming Integration
- Select Sites - devices can roam from these sites
- Select types of devices that can from the selected sites

Edit Action [X]

Central Visibility Manager - Roaming Integration

Enable roaming from the following locations:

- All sites
- Singapore Kuala_Lumpur

Query interval (seconds)

Policies

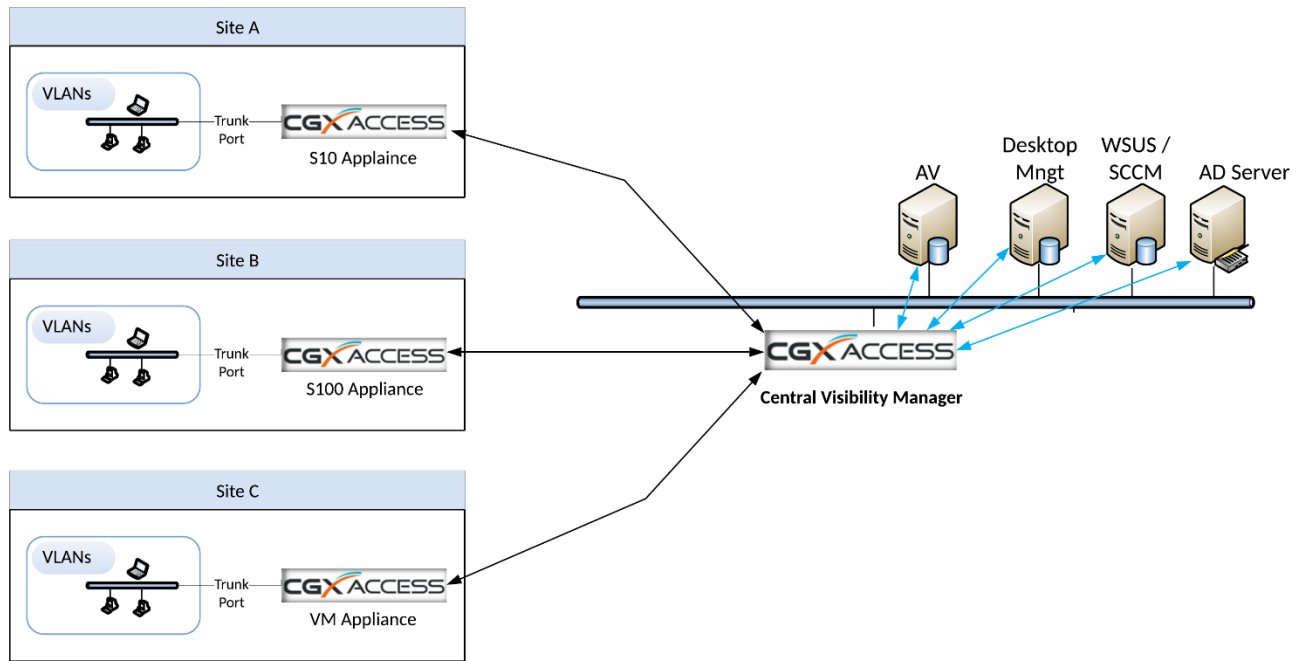
Flag roaming devices as

- Allow BYOD registered devices
- Allow Guest registered devices
- Allow devices flagged as

In the above example, only “BYOD” registered devices and devices tagged as “AD-Managed” will be allowed to roam from either of the sites. These roaming devices will be tagged “Roaming”, so using this “Roaming” tag, the devices can be assigned limited access to the network, as desired.

Central Visibility Manager – Integration Proxy

When integrating with 3rd party security solutions, it can be useful to use the CVM to act as an integration Proxy. Using this proxy feature, the Central Visibility Manager will integrate directly to the 3rd-party servers. The CVM would then share this integration data with the Centrally Managed Appliances. This architecture would aid deployments and minimize the load on the 3rd party servers.



Central Visibility Manager Configuration

- In CVM, go to Configuration → Integration Proxy
- Configure the desired integration (See Integration section for specific vendor info)

Edit Action

McAfee ePolicy Orchestrator Integration

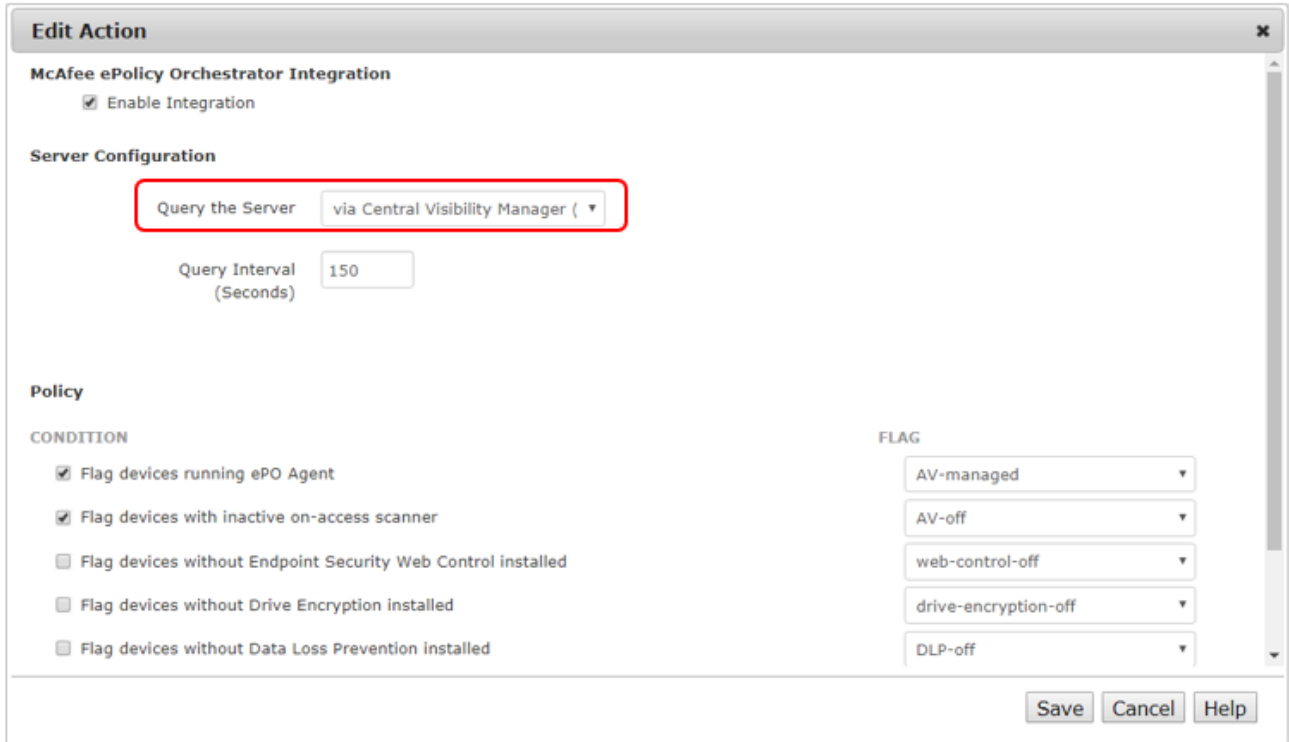
Enable Integration

Server Configuration

Host or IP	<input type="text"/>	Username	<input type="text"/>
Port	<input type="text" value="1433"/>	Password	<input type="password" value="....."/>
Database	<input type="text"/>	<input type="button" value="Test Connection"/>	
Query Interval (Seconds)	<input type="text" value="150"/>		

Centrally Managed Appliance Configuration

- In the managed appliances, go to Configuration → Integration
- Select the desired integration
- Select the “via Central Visibility Manager”



The screenshot shows the 'Edit Action' window for McAfee ePolicy Orchestrator Integration. The window is titled 'Edit Action' and has a close button (X) in the top right corner. The main content is organized into sections:

- McAfee ePolicy Orchestrator Integration**
 - Enable Integration
- Server Configuration**
 - Query the Server: via Central Visibility Manager (▼) [This dropdown menu is highlighted with a red rectangle in the original image.]
 - Query Interval (Seconds): 150
- Policy**
 - CONDITION**
 - Flag devices running ePO Agent
 - Flag devices with inactive on-access scanner
 - Flag devices without Endpoint Security Web Control installed
 - Flag devices without Drive Encryption installed
 - Flag devices without Data Loss Prevention installed
 - FLAG**
 - AV-managed (▼)
 - AV-off (▼)
 - web-control-off (▼)
 - drive-encryption-off (▼)
 - DLP-off (▼)

At the bottom right of the window, there are three buttons: 'Save', 'Cancel', and 'Help'.

Note: Each Centrally Managed Appliance would still be able to set their own policies.

Maintenance and Support

Upgrading firmware

Firmware updates may be provided by InfoExpress to upgrade the CGX Access with new functionalities or fix existing issues. A binary update file (BIN file) will be provided with a checksum and file size. An example of the BIN file may be CGX-Access-3.0.201208.BIN, with a checksum of 2977226413 and file size of 365779928.

Upgrading the firmware of the CGX Access can be done via the web interface

- In CGX Access GUI, go to Configuration → Appliance Settings
- Scroll down to Server Maintenance → Software Update
- Browse to location of file and upload the image

No.	File	Uploaded At	Delete
1	ACCESS-3.2.231212.BIN	12/13/2023 18:26:18	Delete

- Once uploaded, complete checksum: and file size: then **Submit**

Software Update:

Select a file to update:

ACCESS-3.2.231219.BIN ▼ checksum: 1114813831 file size: 616286118 force: Submit

No.	File	Uploaded At	Delete
1	ACCESS-3.2.231212.BIN	12/13/2023 18:26:18	Delete
2	ACCESS-3.2.231219.BIN	12/21/2023 16:32:51	Delete

The CGX Access may reboot. Allow 5-15 minutes for upgrade to occur.

Note: Select force, if it is necessary to downgrade a version.

Collecting Logs (Dump2)

For troubleshooting purposes, InfoExpress support may ask administrators to collect Dump2 Logs.

Note: Before collecting dump2 logs, please check with Support if you need to enable debug logging and the duration of logging required.

Enable Debug Logging

- In CGX Access SSH Console, use Option 91 - Server Maintenance
- Type “trace enable”

```
SERVER MAINTENANCE

These assist with the maintenance of the system. For updates, please
follow the instructions provided with the binary update.
NOTE: Commands are case sensitive.

Commands
-----
DUMP          - Show system configuration
UPDATE <args> - Update software, use args provided with instructions
STATS        - Display system statistics
MONITOR      - Monitor network traffic

Command (0=Back)? [default 0]: trace enable_
```

- Confirm TRACE ENABLED is shown at the top of the SSH Console

```
CGX Access Server

*****
*  o TRACE ENABLED          *
*****

=== General Setup ===
1  Run Setup Wizard

10 Configure Networking
11 Set Date and Time
12 Manage Passwords
13 Configure Logging
14 Configure Services

=== Information ===
Version: CGX-ACCESS: 2.4.200618
Hardware: 1000-SWA 3.10.0

Managed IP: 192.168.253.220/255.255.255.0
Def gateway: 192.168.253.254
Syslog Svr: None/None
DNS Servers: 192.168.253.100

=== Maintenance ===
91 Server Maintenance
99 Restart/Shutdown Server

Enter Option (0=Exit): _
```

- Wait for few minutes, as advised by Support, before collecting the logs.

Note: Collecting the logs will disable Trace Enable

Collecting Logs (Web GUI method)

- In CGX Access GUI, go to Configuration → Appliance Settings
- On left menu, Select → Support Tools → Click **Configure**

CGX Access Standalone Configuration Policies Control Visibility Welcome admin Sign Out

CGX Access Management
CGX Access Logs
Agent Logging Server
Inline Enforcement
RADIUS Proxy
About
Support Tools

Support tools

Wipe out database

Remove all data from CGX databases. This function should be run on the Central server(s) only. [Wipe out](#)

Reset CGX to the factory settings

Reset CGX's configurations and policies to the factory settings. [Reset now](#)

Ping Tool

Software utility used to test the reachability of a host on an Internet Protocol (IP) network. [Use](#)

Traceroute Tool

Network tool used to show the route taken by packets across an IP network. [Use](#)

Telnet Tool

Network tool used to establish a connection using the Telnet protocol. [Use](#)

Debug Logging

Enable/Disable/Dump logs. [Configure](#)

- Cleanup Logs
- Enable Logging and reproduce the problem

CGX Access Standalone Configuration Policies Control Visibility

CGX Access Management
CGX Access Logs
Agent Logging Server
Inline Enforcement
RADIUS Proxy
About
Support Tools

Support tools > Debug Logging

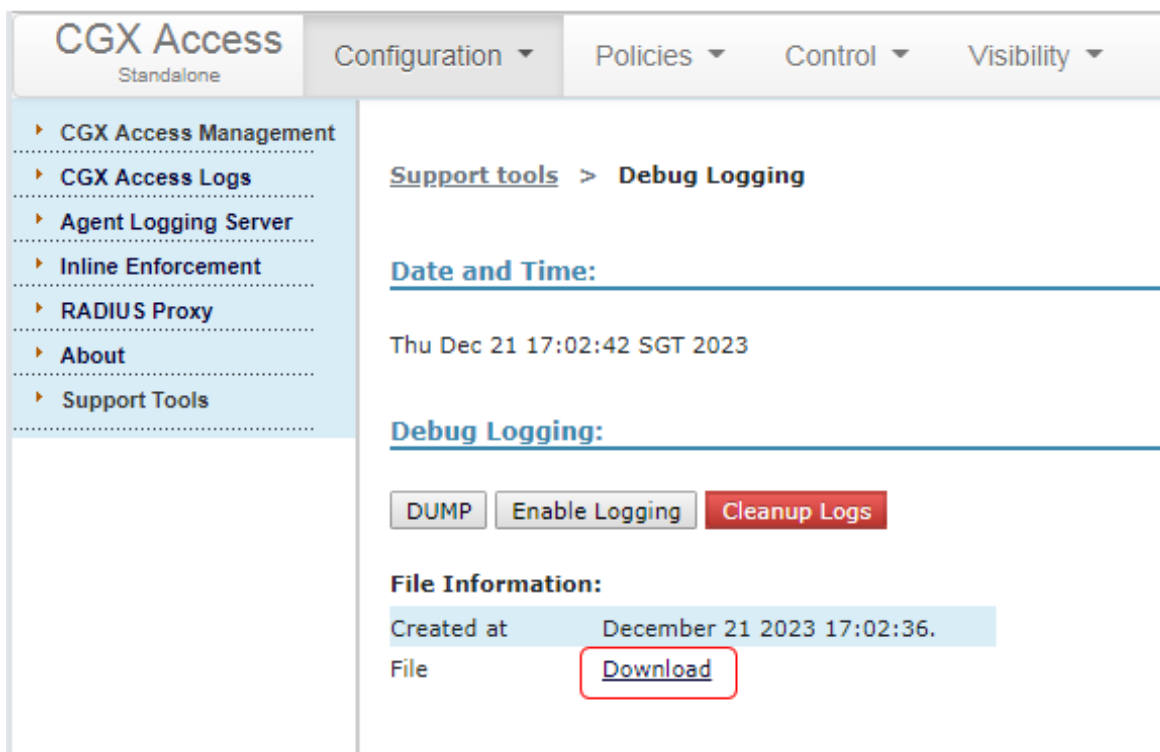
Date and Time:

Thu Dec 21 16:51:45 SGT 2023

Debug Logging:

[DUMP](#) [Enable Logging](#) [Cleanup Logs](#)

- Click the DUMP button
- Wait for Dump process to complete – It may take 5 to 15 minutes depending on number of endpoints. Longer if the system has had core dumps.
- Once complete, download the file and send to support.



Note: If the web interface is not available, the SSH CLI method can be used to collect the logs.

Collecting Logs (SSH CLI method)

- In CGX Access SSH Console, use Option 91 - Server Maintenance
- Type “dump2”
- Type “y” to confirm
- Wait for dump process to complete – It may take 5 to 15 minutes depending on number of endpoints. Longer if the system has had core dumps.

```
admin@cgx-240:/var/log
SERVER MAINTENANCE
These assist with the maintenance of the system. For updates, please
follow the instructions provided with the binary update.
NOTE: Commands are case sensitive.

Commands
-----
DUMP          - Show system configuration
UPDATE <args> - Update software, use args provided with instructions
STATS        - Display system statistics
MONITOR      - Monitor network traffic

Command (0=Back)? [default 0]: dump2
TRACE Mode is disabled!
Do you want to continue or quit (Y/N)? [default N]: y
Please wait while information is collected.....
Take the memory snapshot of running cgate2 processes : 2019-08-28T08:37:16.776+0530   connected to: localhost
2019-08-28T08:37:17.773+0530   [.....] core.ardb 0/1207 (0.0%)
2019-08-28T08:37:18.476+0530   [#####] core.ardb 1207/1207 (100.0%)
exported 1207 records
connected to: localhost
2019-08-28T08:37:19.502+0530   [.....] addb.ss_dpm 0/1206 (0.0%)
2019-08-28T08:37:20.209+0530   [#####] addb.ss_dpm 1206/1206 (100.0%)
exported 1206 records
:
compressing logs, please wait...

All logs have been collected. Please FTP to the appliance as an
administrator (E.G. user admin) to collect cgs_dump.tgz
and e-mail this file to support@infoexpress.com.

Dump complete. Hit Enter to continue...: _
```

- FTP to CGX Access appliance with Admin account to download the logs and send to support.

```
C:\WINDOWS\system32\cmd.exe
8:39:12.03 ftp 10.20.0.13
Connected to 10.20.0.13.
220 Welcome to CGX FTP service.
200 Always in UTF8 mode.
User (10.20.0.13:(none)): admin
331 Please specify the password.
Password:
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-rw-  1 0      0
-rw-rw-rw-  1 0      501
-rw-rw-rw-  1 0      501
-rw-rw-rw-  1 0      501
-rw-rw-rw-  1 0      501
-rw-rw-rw-  1 0      6190707 Aug 28 03:07 cgs_dump.tgz
-rw-rw-rw-  1 0      501
drwxrwxrwx  3 0      501
-rw-rw-rw-  1 0      501
-rw-rw-rw-  1 0      501
226 Directory send OK.
ftp: 778 bytes received in 0.02Seconds 48.63Kbytes/sec.
ftp> bin
200 Switching to Binary mode.
ftp> get cgs_dump.tgz
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cgs_dump.tgz (6190707 bytes).
226 Transfer complete.
ftp: 6190707 bytes received in 0.52Seconds 11928.14Kbytes/sec.
ftp> bye
221 Goodbye.

8:39:40.07>
```

Appendix A – Certificate Management

By default, CGX Access uses self-signed certificates which will not be trusted. To eliminate warnings on untrusted certificates, third-party certificates can be uploaded to the appliance.

Option 1 - Generate Certificate Signing Request (CSR) to obtain a certificate from your CA

Please note: CGX Access could be using 3 hostnames, one for management-IP, Captive portal, and Remediation portal. Therefore, it is advised that you create a wildcard certificate. (*.domain.com)

- Login to CGX Access using username **admin**, Go to Configuration → Appliance Settings.
- Configure DNS server, Hostname, Domain Name, Hostname for Captive portal & Remediation Portal, and IP Address for Captive portal & Remediation portal
- Click **Submit** to save the settings

The screenshot shows the CGX Access configuration interface. The top navigation bar includes 'Configuration', 'Policies', 'NAC', and 'Visibility'. A red notification banner states 'Enforcement is disabled on 1 of 3 subnets'. The main content area is titled 'System Configuration' and includes a 'Date and Time' section showing 'Mon Nov 12 9:26:38 IST 2018'. Below this is the 'Configure Networking' section, which contains a table for network adapters and a section for DNS and landing pages. The DNS Servers field is highlighted with a red box and contains the value '10.20.0.3'. Other fields include Hostname (mini), Domain Name (s1.com), and IP Address (A) (10.20.0.14/255.255.255.0). A 'Submit' button is located at the bottom of the configuration area.

Adapter #	IP / Netmask	Gateway	VLAN ID	Configuration	State
Adapter #1	10.20.0.13/255.255.255.0	10.20.0.2		(Management IP)	↑
Adapter #2	172.16.11.1/255.255.0.0	172.16.10.2		Using DHCP for IP address/gateway	↑
Adapter #3	192.168.10.10/255.255.255.0	192.168.10.2		Using DHCP for IP address/gateway	↑
Adapter #4	/			Off	↑

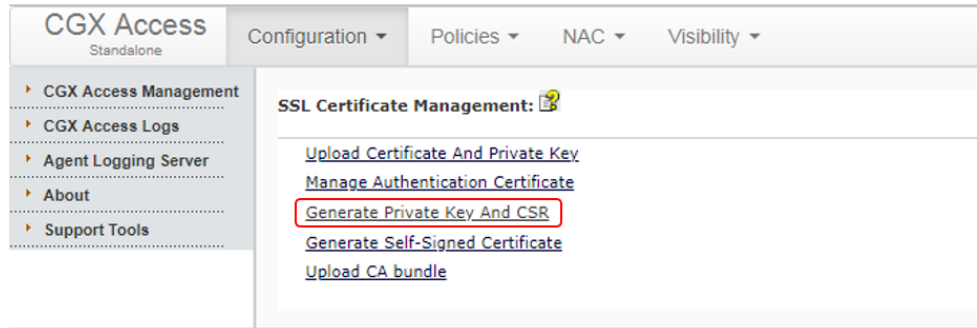
DNS Servers: 10.20.0.3
Hostname: mini
Domain Name: s1.com
Landing Pages
Host Name for Landing Pages: cgxa-landing
IP Address (A) (IP/Netmask): 10.20.0.14/255.255.255.0 Adapter #1

Note: Hostnames should match as to be entered in the certificate. Some settings may not be configurable until DNS server and Domain name is configured.

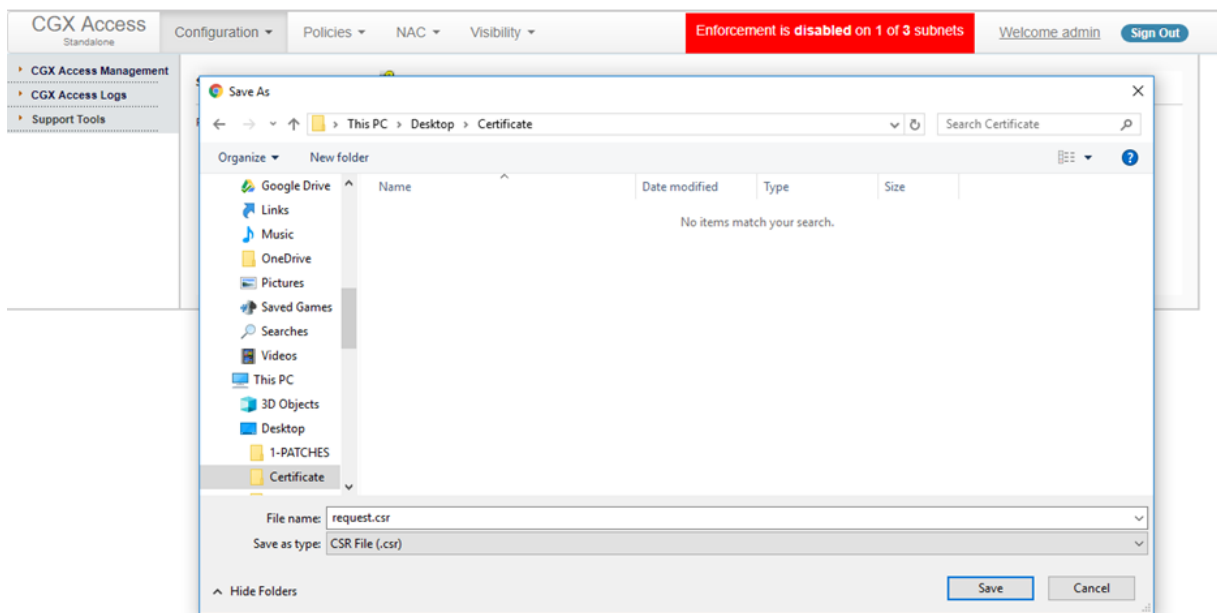
- Scroll down and Click **SSL Certificate Management**

The screenshot shows the 'Server Maintenance' menu. The 'SSL Certificate Management' option is highlighted with a red box. Other options in the menu include 'Manage Accounts', 'Radius Authentication', 'Software Update', and 'DUMP Logs'.

- Click on **Generate Private Key and CSR**



- Enter required details and click on **Generate**

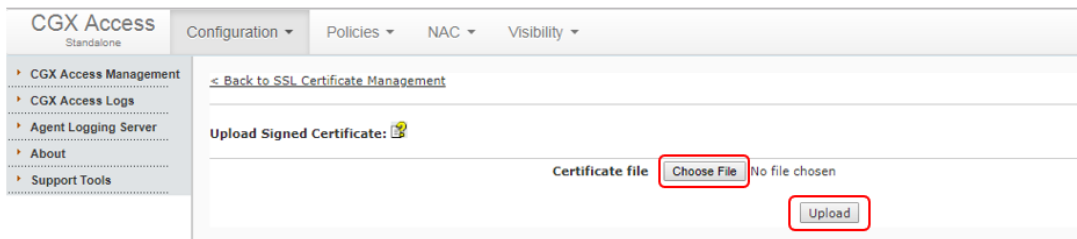


- Save the generated CSR
- Provide the CSR to certification authority (CA) to generate the certificate

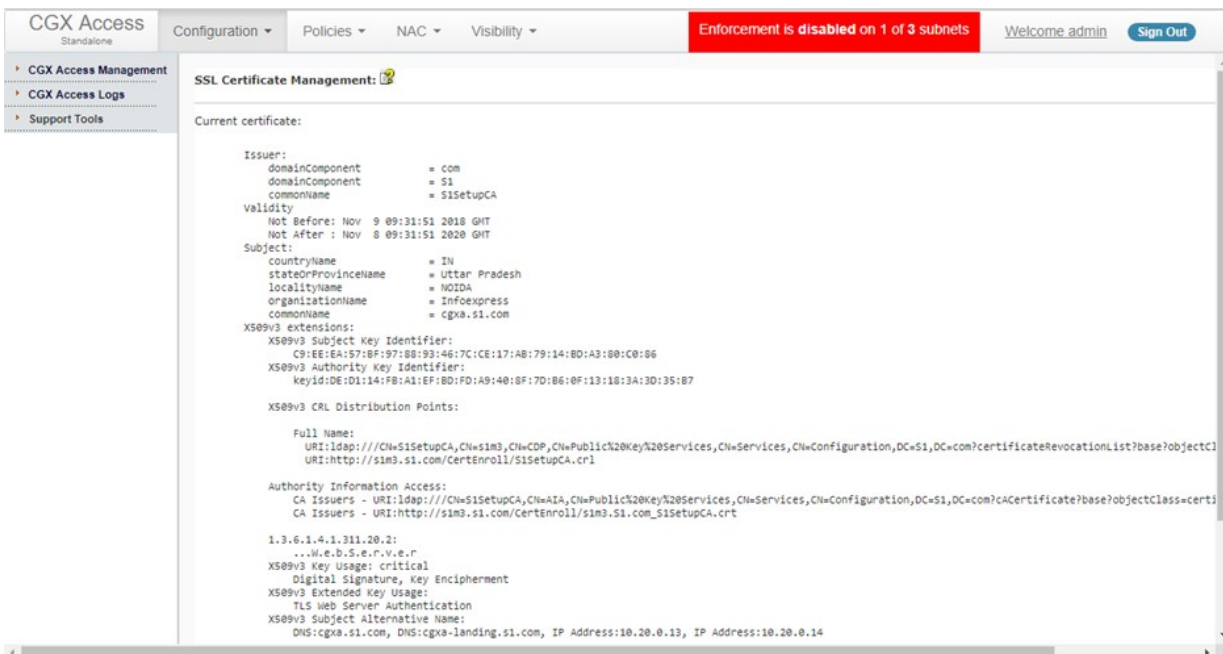
- Once you obtain the certificate from CA, Click on **Upload signed certificate**



- Choose certificate file to and upload

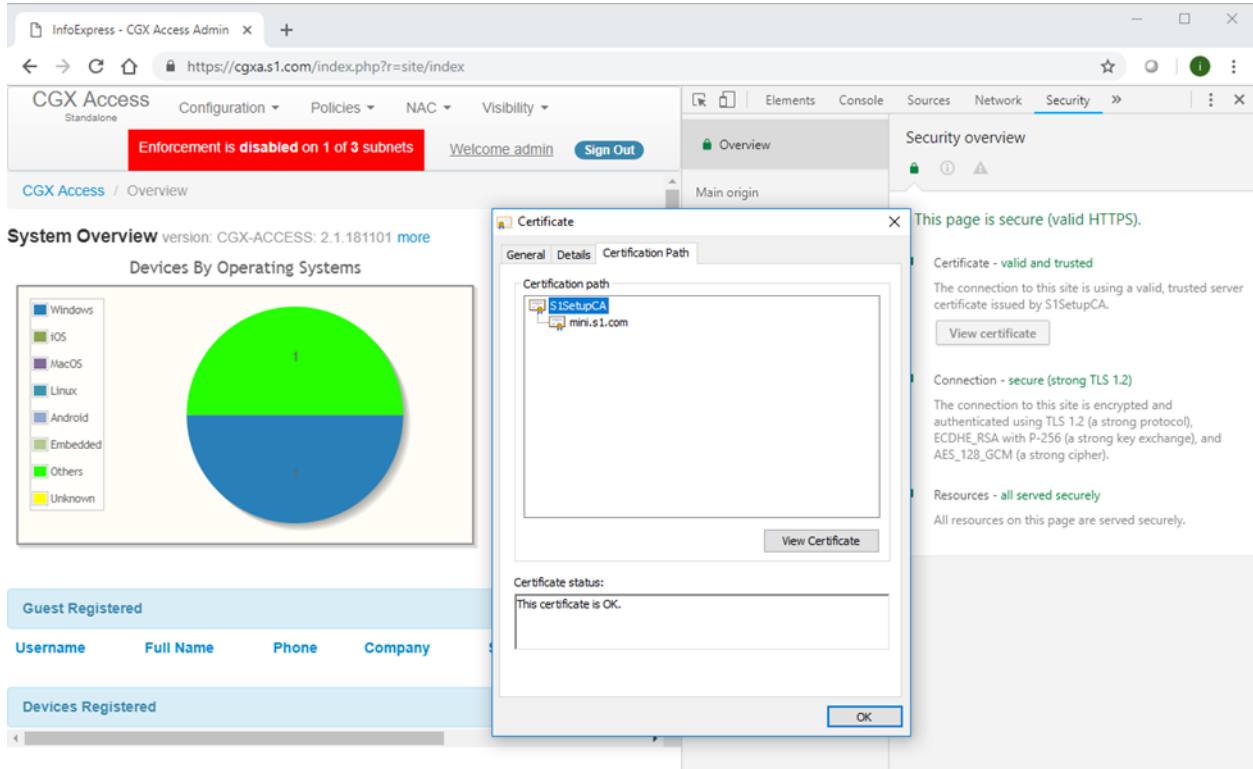


- New certificate will be uploaded and details will be shown

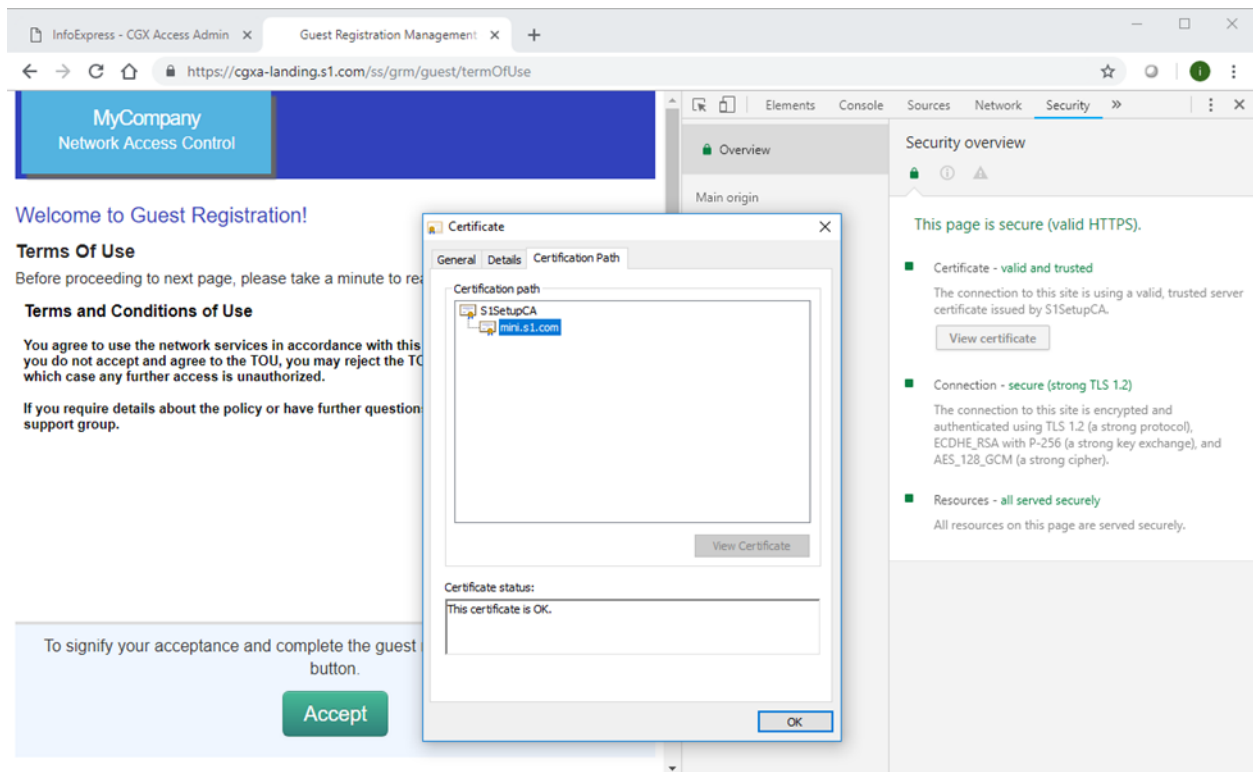


- Reboot CGX Access for new certificate to take effect

- To Check certificate, browse CGX Access using hostname



Note: You can also browse the Captive Portal page (This example used Subject alternative name and hence the same certificate was valid for both hostnames.)



Option 2 - Upload certificate and private key to CGX Access. (When CSR is not generated)

Please note: CGX Access could be using 3 hostnames, one for management-IP, Captive portal, and Remediation portal. Therefore, it is advised that you create a wildcard certificate. (*.domain.com)

- Login to CGX Access using username **admin**, Go to Configuration → Appliance Settings.
- Configure DNS server, Hostname, Domain Name, Hostname for Captive portal & Remediation Portal and IP Address for Captive portal & Remediation portal
- Click **Submit** to save the settings

The screenshot shows the CGX Access configuration interface. The top navigation bar includes 'Configuration', 'Policies', 'NAC', and 'Visibility'. A red notification banner states 'Enforcement is disabled on 1 of 3 subnets'. The main content area is titled 'System Configuration' and includes a 'Date and Time' section (Mon Nov 12 9:26:38 IST 2018) and a 'Configure Networking' section. The networking section contains a table with columns for Adapter, IP / Netmask, Gateway, VLAN ID, Configuration, and State. Below this table is a 'DNS Servers' section with fields for DNS Servers (10.20.0.3), Hostname (mini), and Domain Name (s1.com). There is also a 'Landing Pages' section with fields for Host Name for Landing Pages (cgxa-landing) and IP Address (A) (IP/Netmask) (10.20.0.14/255.255.255.0). A 'Submit' button is located at the bottom of the form.

Adapter	IP / Netmask	Gateway	VLAN ID	Configuration	State
Adapter #1 MAC: 00:e0:67:06:df:8b	10.20.0.13/255.255.255.0	10.20.0.2		(Management IP)	⬆
Adapter #2 MAC: 00:e0:67:06:df:8c	172.16.11.1/255.255.0.0	172.16.10.2		Using DHCP for IP address/gateway	⬆
Adapter #3 MAC: 00:e0:67:06:df:8d	192.168.10.10/255.255.255.0	192.168.10.2		Using DHCP for IP address/gateway	⬆
Adapter #4 MAC: 00:e0:67:06:df:8e	/			Off	⬆

DNS Servers	10.20.0.3
Hostname	mini
Domain Name	s1.com
Landing Pages	
Host Name for Landing Pages	cgxa-landing
IP Address (A) (IP/Netmask)	10.20.0.14/255.255.255.0

Note: Hostnames should match as to be entered in the certificate. Some settings may not be configurable until DNS server and Domain name is configured.

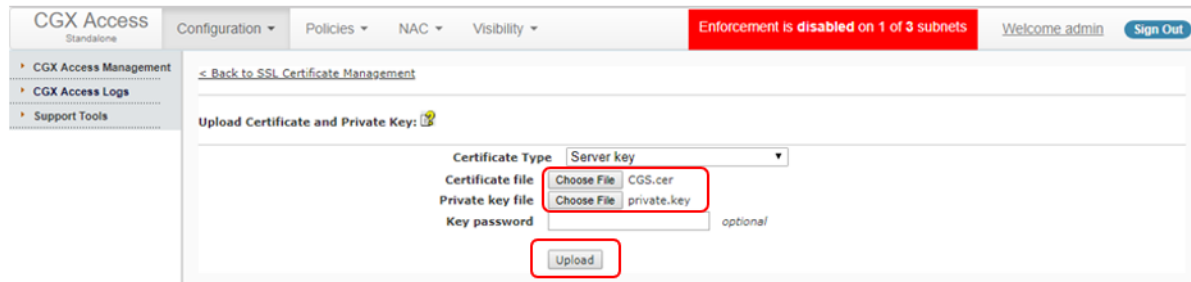
- **Scroll down and Click SSL Certificate Management**

The screenshot shows the 'Server Maintenance' section of the CGX Access interface. The menu items are: 'SSL Certificate Management' (highlighted with a red box), 'Manage Accounts', 'Radius Authentication', 'Software Update', and 'DUMP Logs'.

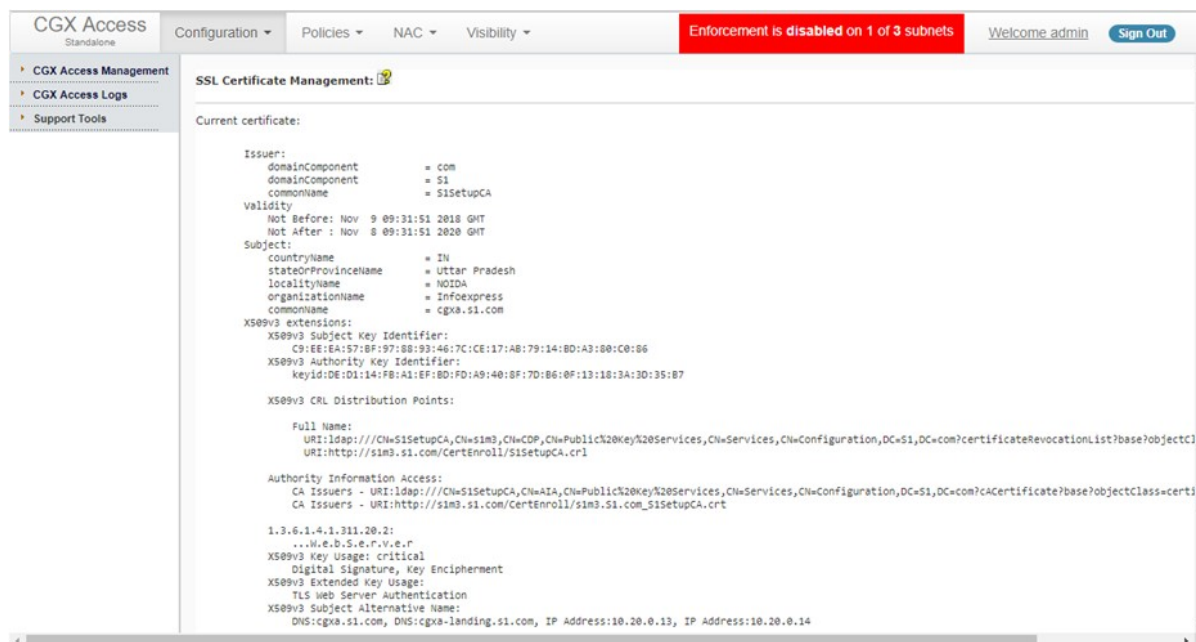
- Click on Upload Certificate and Private Key



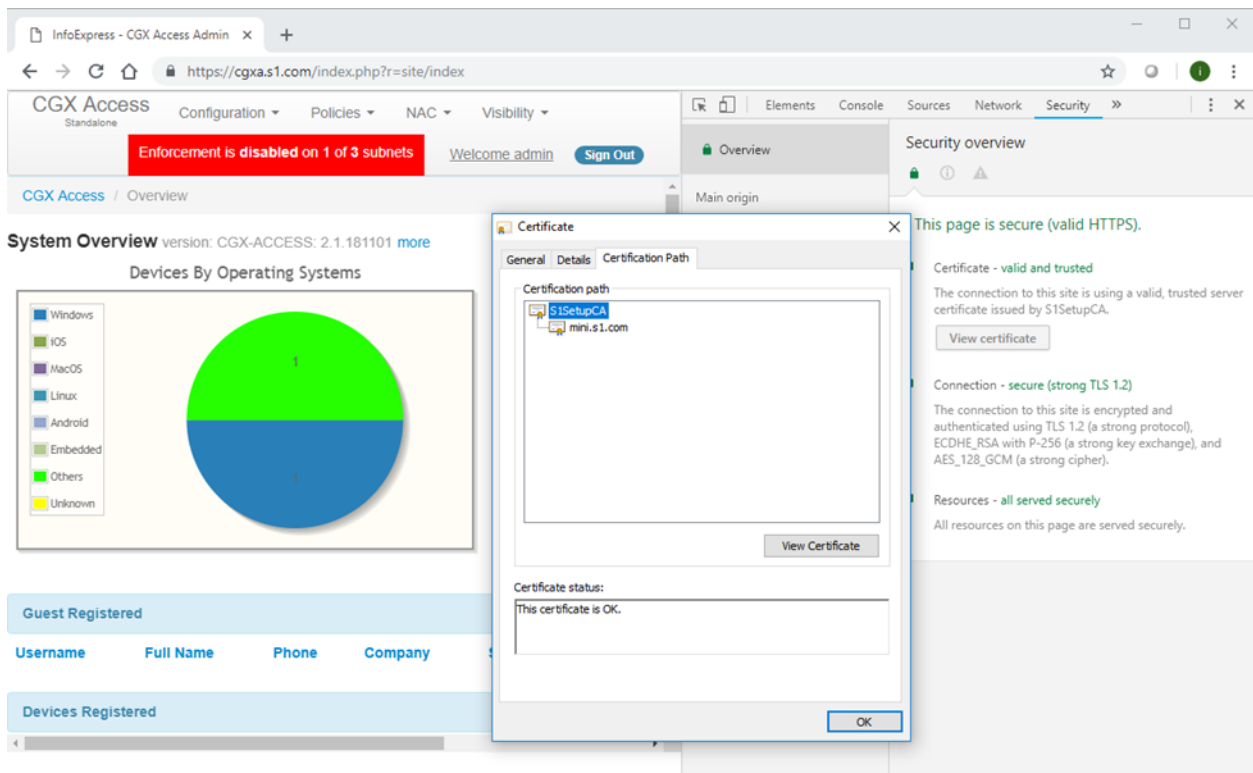
- Choose files to upload. (Enter password if required)
- Click Upload



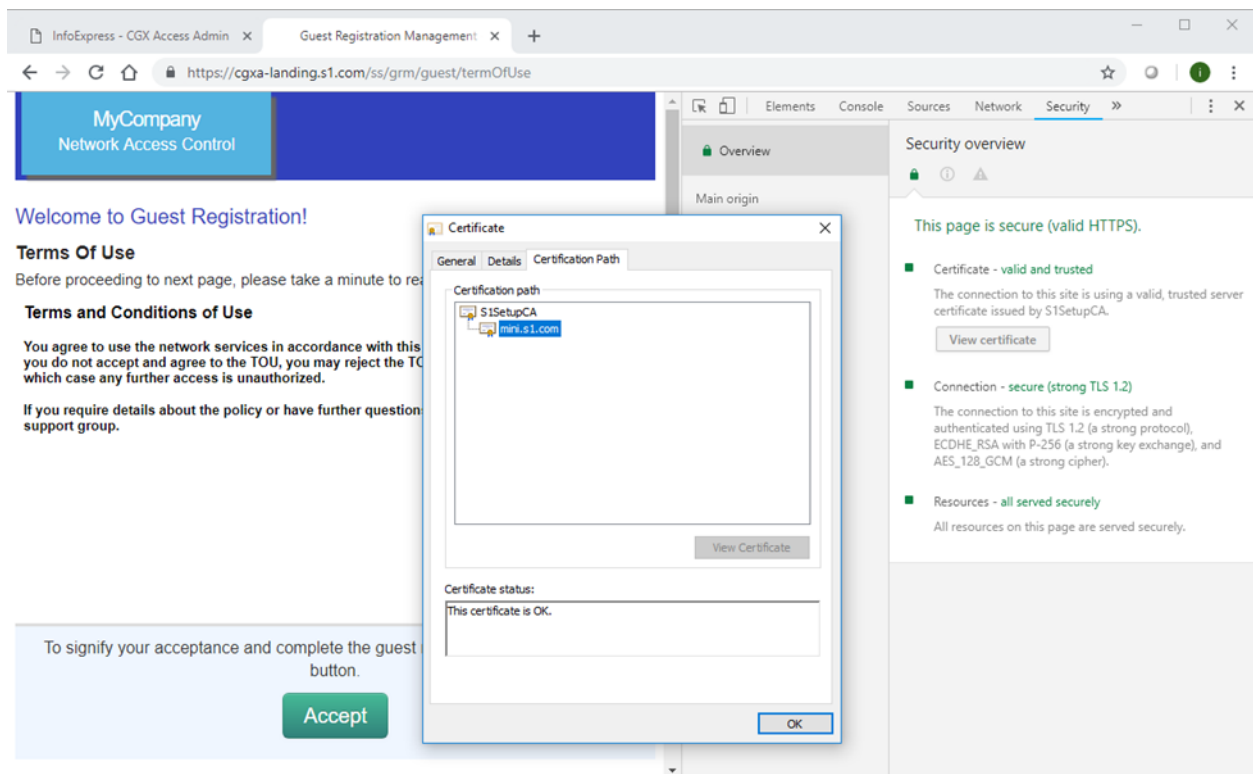
- New certificate will be uploaded and details will be shown



- Reboot CGX Access for new certificate to take effect
- To Check certificate, browse CGX Access using hostname



Note: You can also browse the Captive Portal page (This example used Subject alternative name and hence the same certificate was valid for both hostnames.)



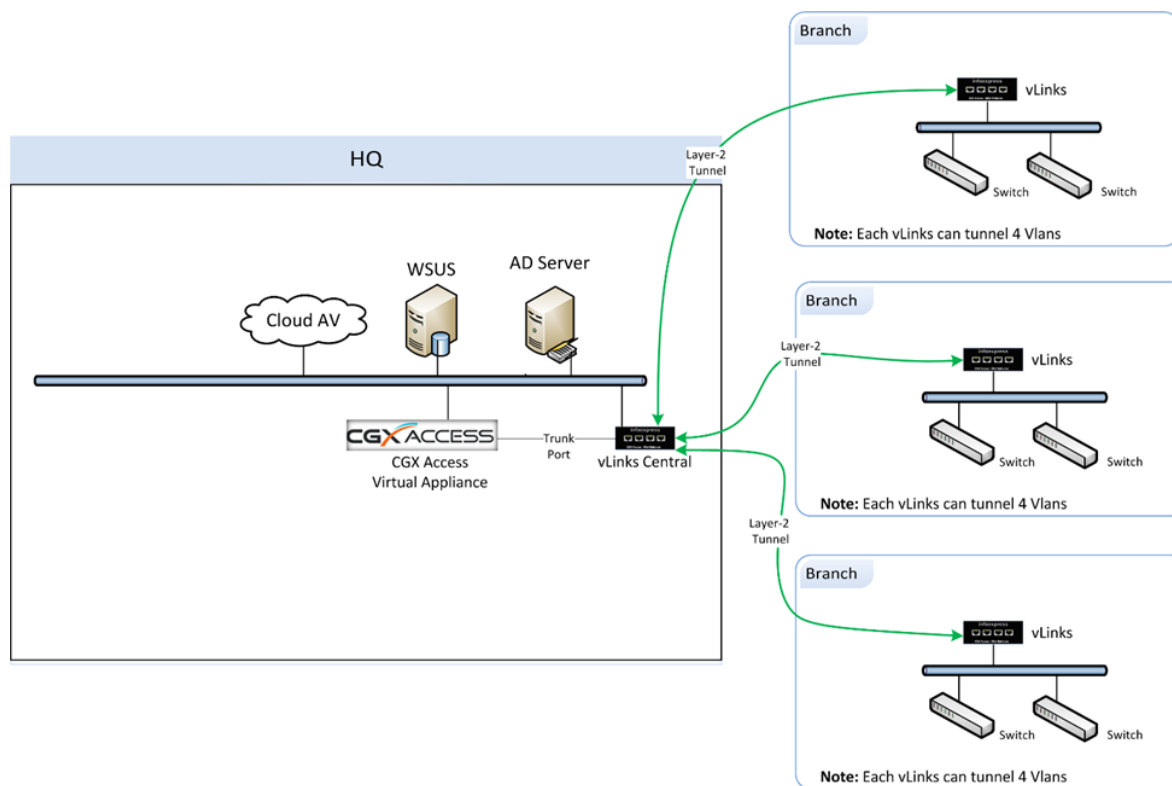
Appendix B – vLinks Deployment

vLinks Overview

The Easy NAC solution uses CGX Access appliances for visibility and protection of the network. To provide visibility and protection, the CGX Access appliance requires layer-2 visibility of the subnets it's protecting. Having layer-2 visibility at the main site can be easily achieved with trunk ports or standard access ports. However, getting layer-2 visibility for remote sites can be more challenging. The vLinks solution is designed to extend the reach of the CGX Access appliances so it can also protect your smaller remote sites with cost effective hardware.

The vLinks architecture is shown below. At remote sites, a vLinks appliance is placed on the network for layer-2 visibility. This layer-2 traffic is then tunneled back to a vLinks Central appliance. This tunneled traffic is sent over the existing corporate WAN, so an existing WAN network is required. MPLS and NAT'd network types are supported.

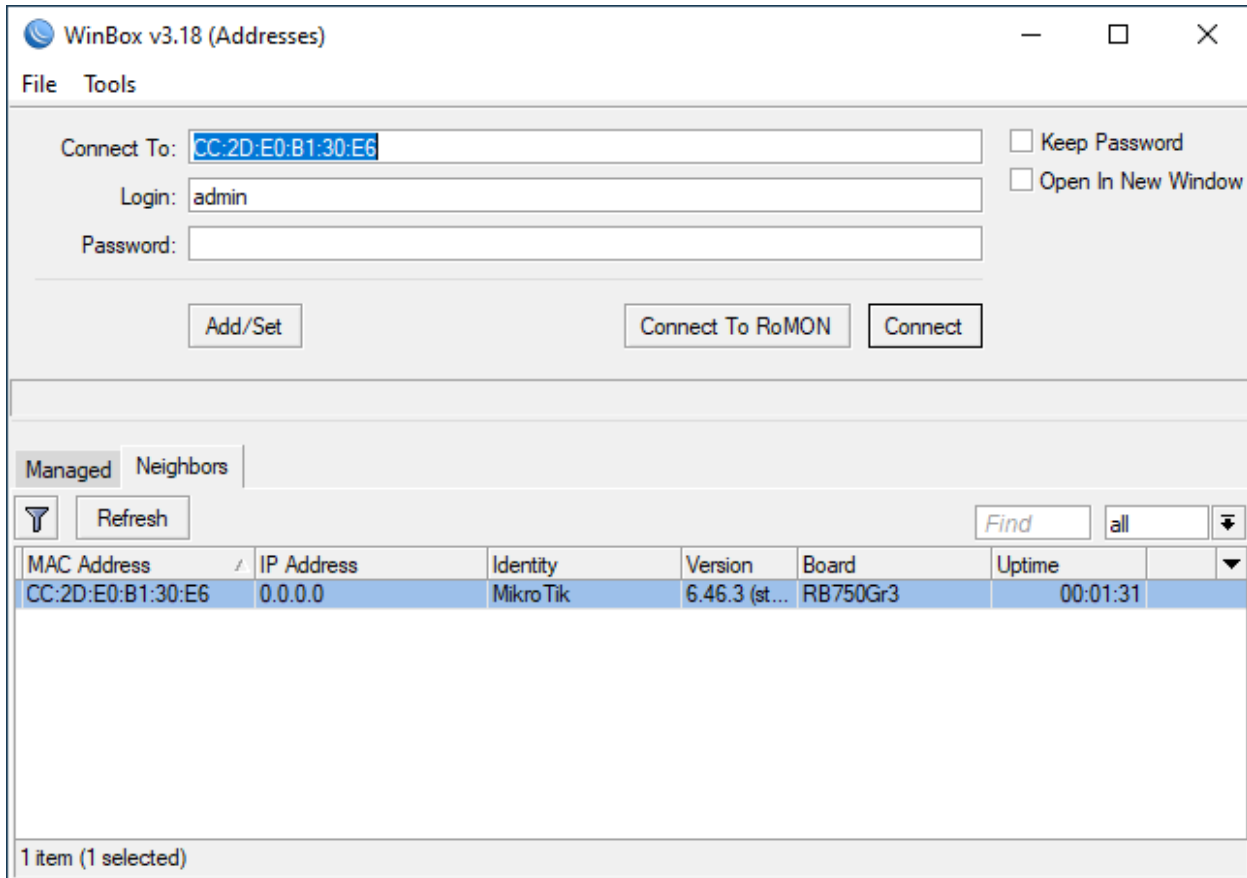
At the main site, a vLinks Central will consolidate the layer-2 traffic from multiple vLinks and share it with the CGX Access appliance using a port directly connected to the CGX Access appliance. With this connectivity in place, CGX Access will detect rogue devices at the branches and quarantine these devices real-time. All Easy NAC features including compliance checks, captive portals, Automated Threat Response, etc., are supported.



Adding vLinks to extended CGX Access protection to remote sites is a two-stage process. Stage one is to configure the vLinks Central appliance. Once the vLinks Central appliance is configured the vLinks Remote appliances can be configured to contact the CGX Access and download their configurations.

vLinks Central Setup

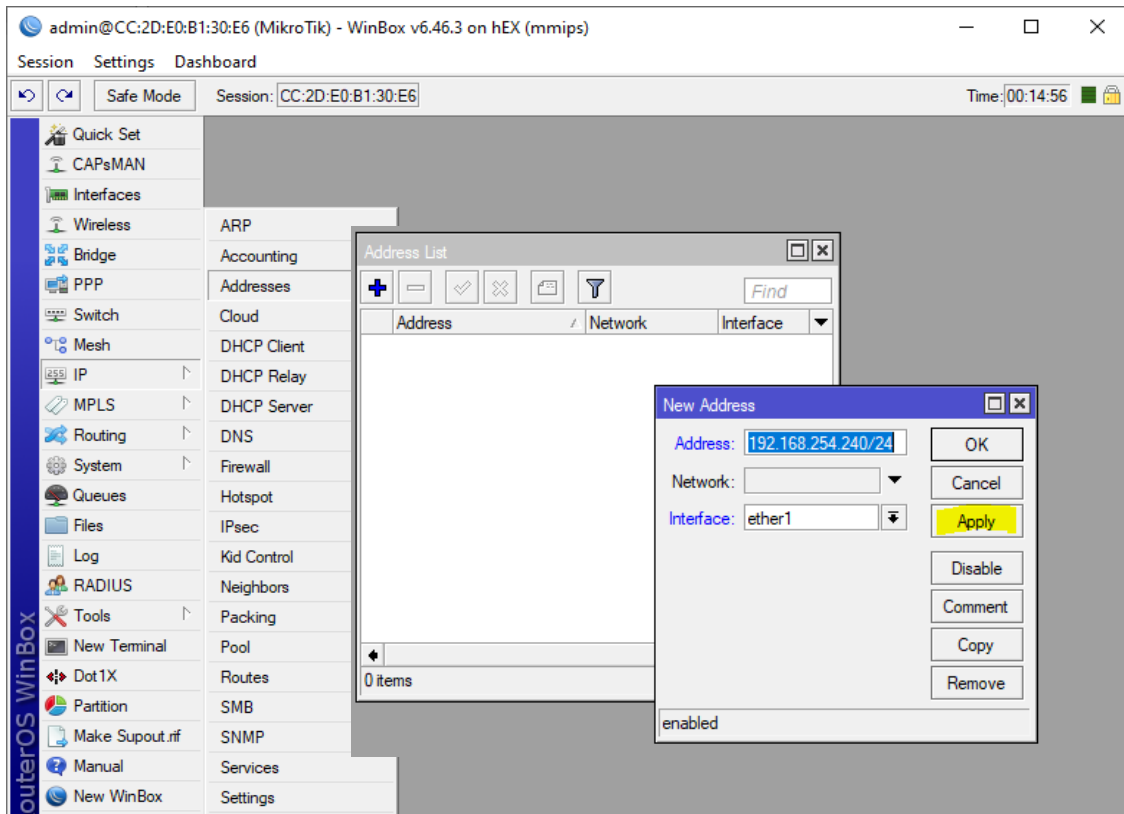
The vLinks Central hardware is manufactured by Mikrotik. To configure this box, download the WinBox application at <https://mikrotik.com/download>. Connect the appliance (adapter 1) to your PC using an RJ45 cable and connect to it via its MAC address or DHCP assigned IP address.



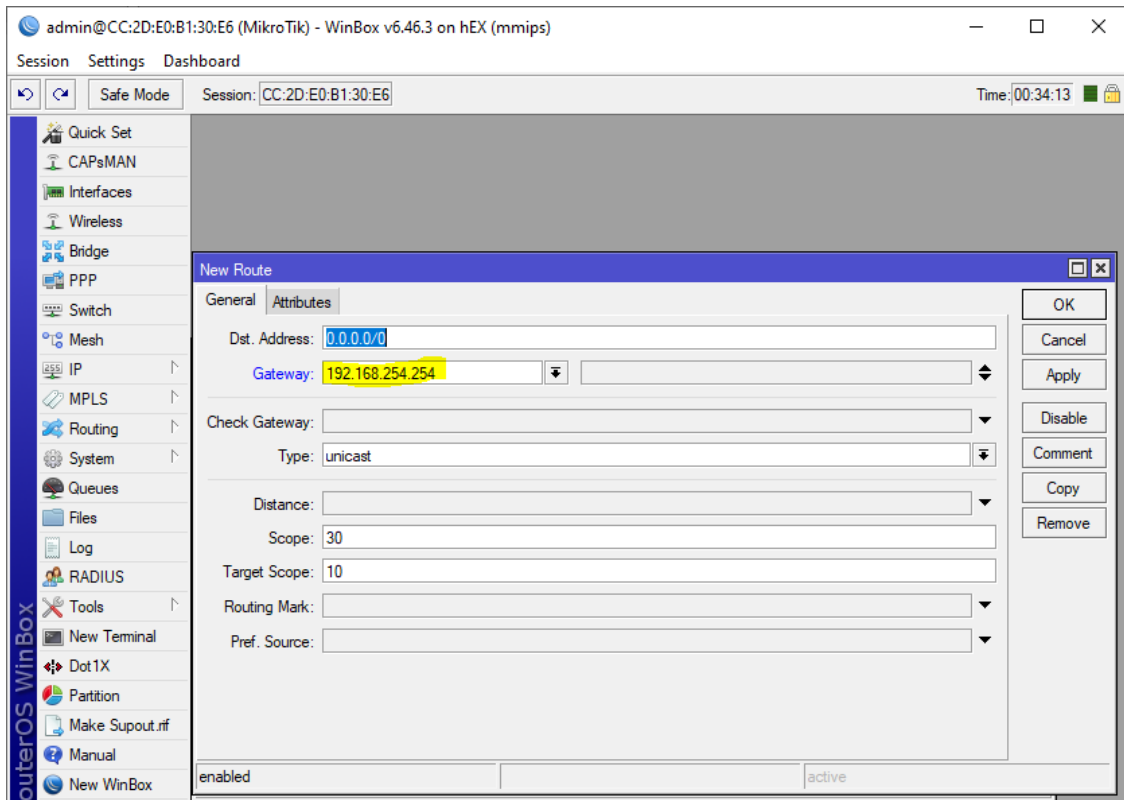
The default account is admin. The default password is blank.

Perform the following steps to assign a static IP, default gateway, and admin password:

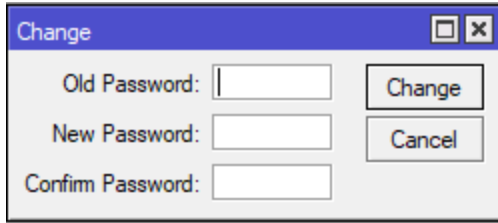
- 1) Configure a Static IP address - Go to: IP > Addresses >



2) Configure a default route - Go to: IP > Routes > Click +



3) Configure a password - Go to: System > Password



Change

Old Password:

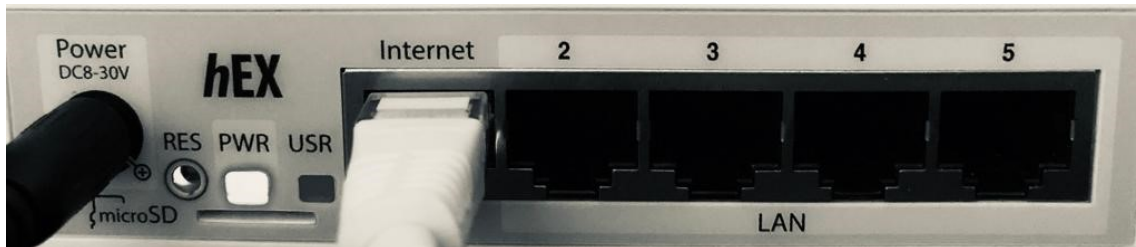
New Password:

Confirm Password:

4) Shutdown box and place on the network: System > Shutdown

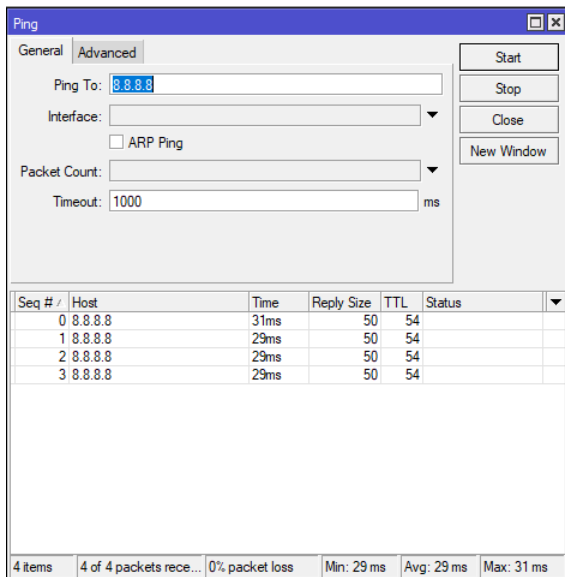
Note: Configurations changes made on vLinks Central take effect immediately, there are no added steps required to save the configurations.

5) Physical Placement - Place the vLinks Central box on the production network using Adapter 1.



Model: VLC-5SM

6) Test connectivity – Using WinBox login into the IP address of the box. Go to: Tools > Ping to test connectivity to default gateway and any off-subnet resource.



Ping

General Advanced

Ping To: 8.8.8.8

Interface: Internet

ARP Ping

Packet Count: 4

Timeout: 1000 ms

Seq # /	Host	Time	Reply Size	TTL	Status
0	8.8.8.8	31ms	50	54	
1	8.8.8.8	29ms	50	54	
2	8.8.8.8	29ms	50	54	
3	8.8.8.8	29ms	50	54	

4 items 4 of 4 packets rece... 0% packet loss Min: 29 ms Avg: 29 ms Max: 31 ms

- 7) Connect a second cable using Adapter 2 directly into any open port on the CGX Access Appliance. Take note of the port used on the CGX Access appliance for later configuration. This is a direct connection between the vLinks Central and CGX Access appliance.



- 8) Once connected to the CGX Access Appliance, Login into CGX Access web interface.

Go to: Configuration > vLinks Manager

vLinks Configuration
Refresh

vLink Servers

[Add New Server](#) | [Manage Server Models](#) | [Manage Certs](#)

Name	IP Address	Port	Model	VLAN ID Range	Username	Action

vLinks

[Add New vLink](#)

ID	Name	Config Key	Source IP	Server	Revision	Action

vLinks Auto-Configuration

Config Key Update

Warning! The Config Key must be set to accept vLink requests.

ID	Name	Config Key	Source IP	Server	Action

9) Select Add New Server and complete the registration process

The screenshot shows a web form titled "Add New Server". The form has the following fields and values:

- Name: vLinks HQ
- IP Address: 192.168.254.240
- Port: 1194
- Model: 5 port small (dropdown menu)
- Trunk Port: ether2 (dropdown menu)
- VLAN ID Range: 1-50
- Username: admin
- Password: masked with dots

Below the fields is a "Change Password" checkbox, which is currently unchecked. At the bottom of the form are two buttons: "Save" and "Cancel".

Name – Use any name to help you distinguish this vLinks Central from other vLinks Central you may deploy.

IP Address – Use the Static IP address that was set in Step 1 above


Port – Port 1194 is the recommended default port

VLAN ID Range – A 5 port vLinks Central can support 50 remote subnets, so you can configure a range of 50 VLAN IDs. You can use any VLAN range desired. To avoid confusion, it is recommended these VLAN ranges be outside the range of other VLAN IDs used on your corporate network. The 12-port vLinks Central can support 200 remote subnets, and can be configured with a range of 200 VLAN IDs.

Username – The default username is admin

Password – The default password is blank. It is recommended you create a secure admin password.

Once saved, the above settings will be pushed to the vLinks Central server and the vLinks Central will be ready to accept connections from vLinks Remote network extenders.

vLink Servers						
Add New Server Manage Server Models Manage Certs						
Name	IP Address	Port	Model	VLAN ID Range	Username	Action
vLinks HQ	192.168.254.240	1194	5 port small	1-50	admin	   

vLinks Remote Setup

The vLinks Remote boxes have minimal configuration requirements. The recommended deployment technique is to leverage the Auto Configuration feature to pull the necessary configuration details from the CGX Access server. This section will detail the steps to use the Auto Configuration method.

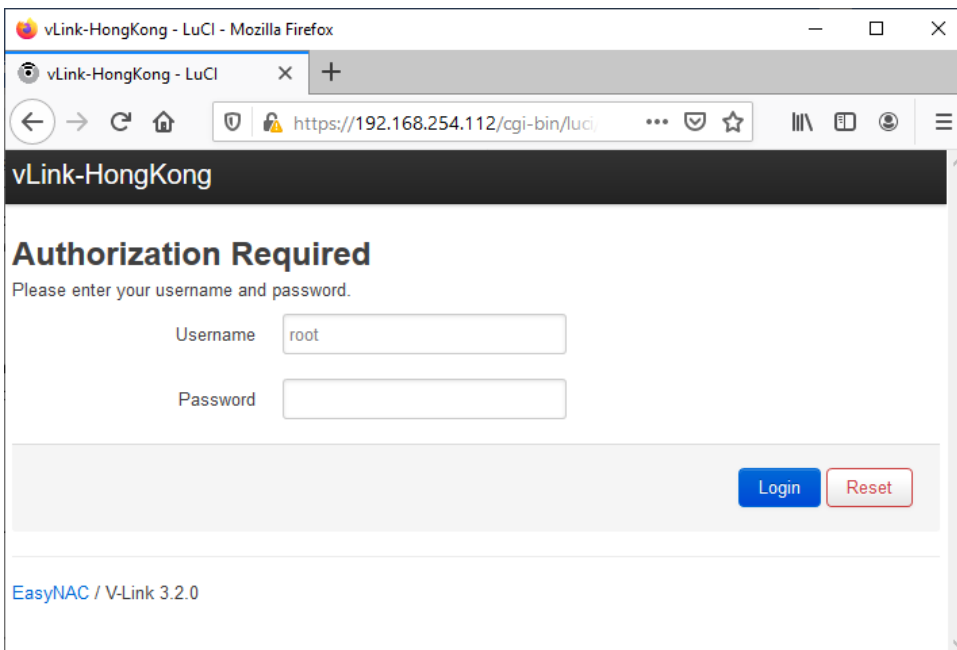
- 1) To allow Auto Configuration a Config Key must be set within the vLinks Manager.

Requesting Configuration

Config Key

ID	Name	Config Key	Source IP	Server	Action

- 2) vLinks Remotes are configure to support DHCP by default. You can attach the vLinks Remote to any DHCP enabled network, and then use the web interface to configure the Auto Configuration.



The default account is root. The default password is GlassDoor2020.

- 3) Configure the basic information required to sync with the CGX Access Appliance – Go to: System > Auto Configuration

[Save & Apply](#) the settings

vLink Name – Any name to help you distinguish this vLinks Remote from other sites

CGX-Access – Provide the Management IP address of the CGX Access that the vLinks Central is attached to. It will use this IP to download the auto configuration.

Config Key – This key must match the key configured in CGX Access to allow the automated configuration downloads

IP Proto – Use this field to change to a Static IP if required. For simplified deployment, DHCP is recommended as each vLinks Remote will have the same configuration and can then be used on any network.

NTP Server – A NTP server is critical to maintain time-sensitive tunnels with the vLinks Central. **Warning:** If time is out of sync, the connection to the vLinks Central will fail.

Auto DNS – It's recommended to use DNS server where available

Static IP - When assigning a Static IP address, it will take a few extra steps to set the configuration.

- A. Configure **all** auto configuration settings including the CGX-Access address and configuration key with the Static IP and prefix (the netmask).

vLink Configuration

CONFIG

VLink Name
 vLink Name
Example: VLINK-NewYork

CGX-Access
 Example: vlink-server.infoexpress.com

Config Key
 CGXA Server Config Key

IP Proto
 Network Configuration

IP Address

Prefix

Gateway

NTP Server
 NTP Server

DNS Server
 DNS Server

- B. Save and Apply Changes. A message will be shown that it Failed to confirm. This is expected if the IP address has changed.



- C. Move the vLinks Remote to a network you can access the new IP address and login again. Verify all the Auto Configuration settings are correct. If not, set all the Auto-configuration settings, and Save and Apply again. This time a confirmation should be shown that the Configuration has been applied.

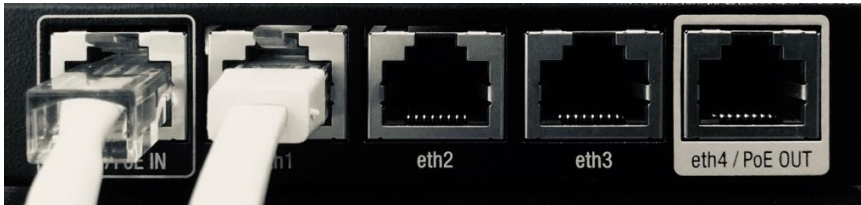


Tip: To perform the verification in step C, it may be useful to set a static IP on your laptop and connect directly to the vLinks remote.

- 4) Physical Placement - Place the vLinks Remote box on the remote network using Adapter 1 (eth0). Adapter 1 is used for tunneling Layer-2 traffic from the remaining 4 ports (eth1-eth4) back to the CGX Access appliance.



Adapter 1 is not protected, so if this subnet needs protection, a second cable should be attached to Adapter 2 (eth1). Each vLinks Remote can protect 4 subnets.



- 5) Accept vLinks Remotes - Once placed on the remote networks the vLinks Remotes will connect to CGX Access to request configurations.

Configuration > vLinks Manager Click the Accept button as shown below.

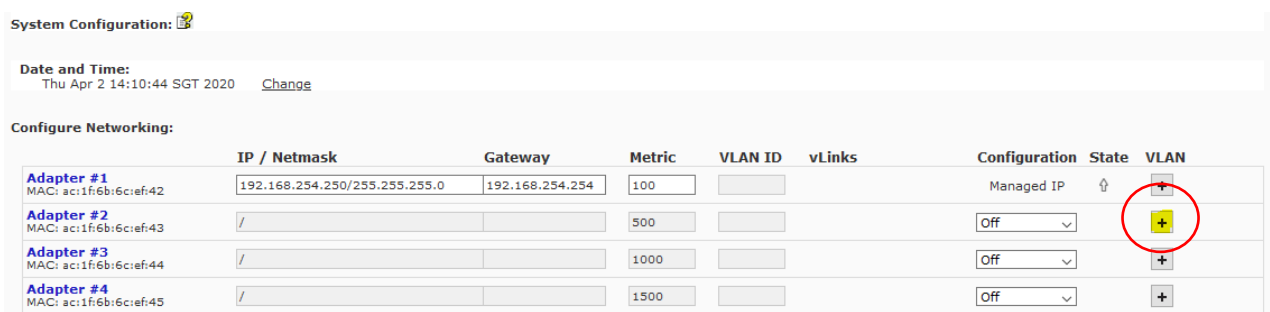


Once Accepted the vLinks Remote will be shown in your vLinks list.



- 6) The last step is to configure the CGX Access Adapter settings to protect the remote segments. On the CGX Access appliance take note of which adapter the vLinks Central was plugged into, during Step 7 of the vLinks Central setup.

On the web GUI - Go to: Configuration > Appliance. Click the + button next to the appropriate adapter to add a VLAN



VLAN ID – Specify any unique VLAN ID that was defined during the vLinks Central. Normally 1-50 by default. On vLinks Remote each Adapter(eth1-eth4) that is active will use a VLAN ID.

DHCP \ Static – Each adapter(eth1-eth4) will use an IP address if the port is active. If using DHCP this address will be auto assigned. If using a Static environment, the Static IP is configured in this step.

vLinks – Use the dropdown box to select the appropriate vLinks for this remote network. If the vLinks box is not shown, confirm it has been accepted during the Auto Configuration stage.

Note: This process would be repeated for each remote subnet that is be to protected. Up to 4 subnets per vLinks.

Once network additions have been made, click the Submit button to activate changes. There will be a delay as each subnet using DHCP will requests an IP assignment.

System Configuration:

Date and Time:
Thu Apr 2 14:21:10 SGT 2020 [Change](#)

Configure Networking:

	IP / Netmask	Gateway	Metric	VLAN ID	vLinks	Configuration	State	VLAN
Adapter #1 MAC: ac:1f:6b:6c:ef:42	192.168.254.250/255.255.255.0	192.168.254.254	100			Managed IP	↑	+
Adapter #2 MAC: ac:1f:6b:6c:ef:43	192.168.253.51/255.255.255.0	192.168.253.254	5001	1	vLink-HongKong	DHCP	↑	+
Adapter #3 MAC: ac:1f:6b:6c:ef:44	/		1000			Off	↓	+
Adapter #4 MAC: ac:1f:6b:6c:ef:45	/		1500			Off	↓	+

If successful you will see an IP address has been obtain, and device monitoring will be active.
Go to: NAC > Network Map

Network Map

CGX Access

Enabled

Default configuration (applied to all subnets) [Show Configuration](#)

Subnets

Network	Last seen	Mode	
192.168.254.0/24	0 second ago	Monitor	Show Configuration
192.168.253.0/24	0 second ago	Monitor	Show Configuration

Deployment is complete and devices from the remote sites will now be shown in the System Overview and the Device Manager, just as other devices are.

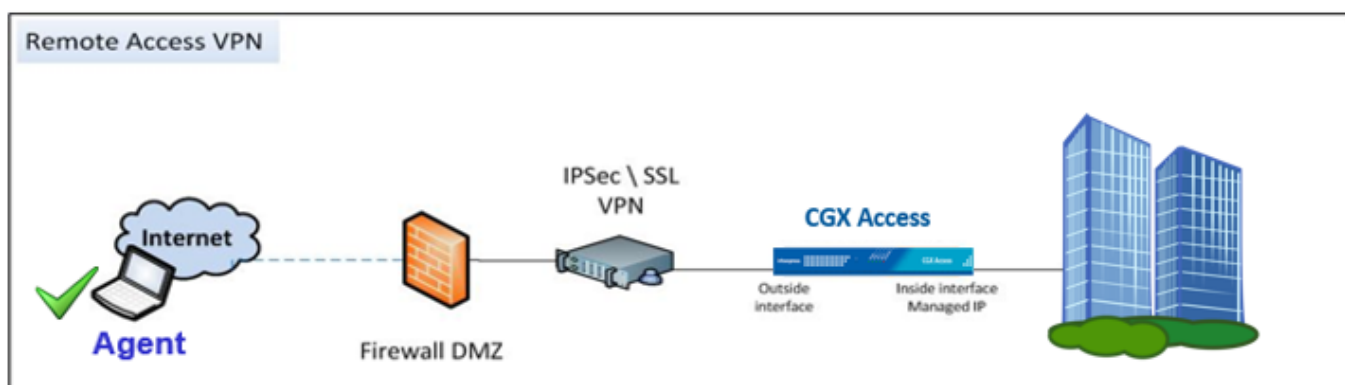
Warning: A NTP server is critical to maintain time-sensitive tunnels with the vLinks Central. If time is out of sync, the connection to the vLinks Central will fail.

Appendix C – Inline Enforcement

Inline Enforcement Overview

The Inline Enforcement Module (Inline EM) controls access to the network through an Access Control List associated with the outside NIC. This module can be used to control access for remote access servers, remote access VPNs, and site to site VPNs.

The Inline EM is available in the EasyNAC product family with CGX Access appliances. When using the Inline EM, the CGX Access appliance is placed in between the network and the network access device, such as a remote access VPN server.



Features

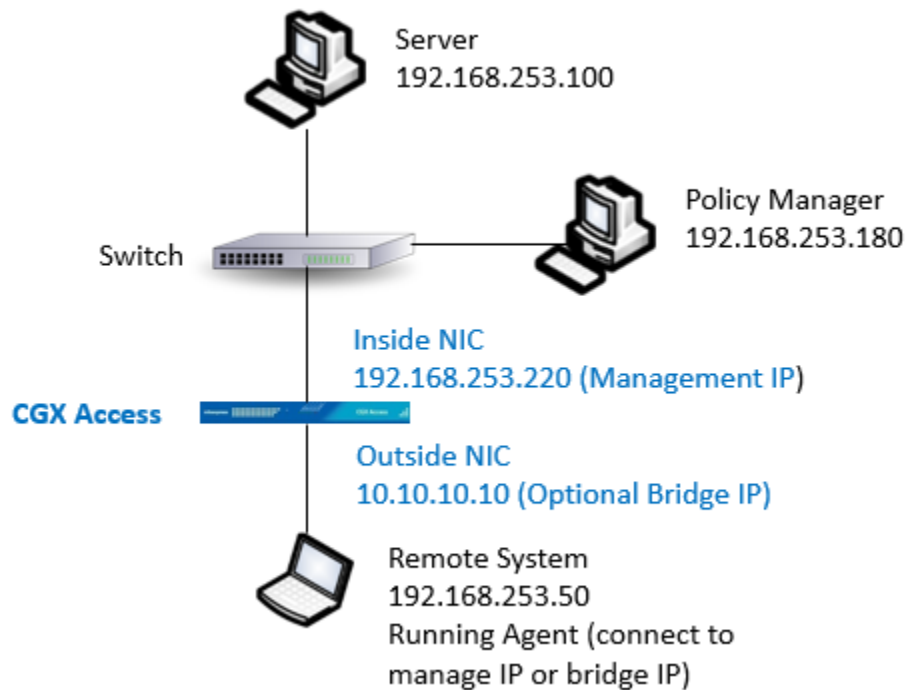
The Inline EM supports the following features:

- Bridges traffic to avoid network topology changes
- Optimized to handle continuous high traffic loads
- Option for automatic failover through STP or KSTP if a redundant server is present

Requirements

- CGX Access must be physically placed between the inside (trusted) network and the remote access gateways such as VPN concentrators.
- Physical Appliance or virtual appliance with a least two network interfaces
- Endpoint Systems must use agents to pass a compliance check.
- VPN must pass TCP 11698 into the network (Agent uses TCP 11698)
- VPN Server must use an IP Pool, so every connected device has a unique IP address.

Sample Test Network



This is a minimal configuration to test and evaluate the Inline EM. Although company networks are not this simple, it can be used to test the features in a controlled test environment. All systems in this configuration are connected to the same subnet.

CGX Access is placed between a single PC which simulates the remote system, and the rest of the LAN which represents the inside network. The inside NIC is connected to the switch closest to the internal network, and the outside NIC is connected to the remote system.

The agent communicates with the Managed IP or the bridge virtual IP address.

Note: If the remote PC is connected directly to CGX Access, a crossover cable may be required.

Configuration

This Configuration steps for the Inline EM consist of:

- Choose the proper location to connect the inline appliance
- Configure the network interfaces
- Set Bridge IP (recommended when using multiple inline appliances)
- Set Access Control List (ACL) rules
- Set the Enforcement Ranges
- Enable Enforcement Mode

Location

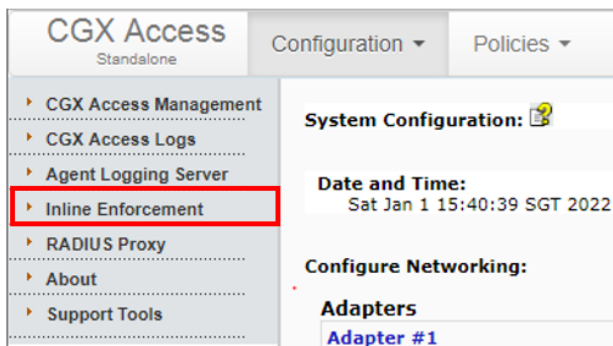
The Inline EM restricts traffic from remote systems, so the outside NIC must face the remote access servers and the inside NIC must face the internal network. When using the Inline EM, CGX Access is usually placed between the VPN and the default router on the network. The Inline EM bridges traffic so network routing tables do not need to be changed.

With this configuration, remote agents communicate to CGX Access Management IP or bridge IP address. The bridge IP is virtual and is recommended for deployments where multiple inline appliances have been deployed to ensure scalability and compatibility with other addresses.

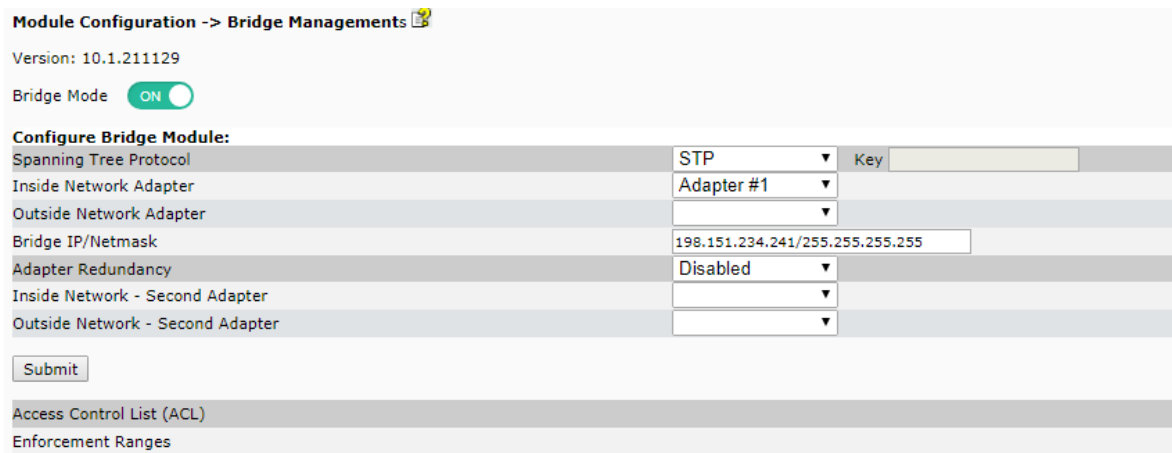
Network Interfaces

To Setup the Inline Enforcement

- In CGX Access, go to Configuration → Appliance Settings
- Click on Inline Enforcement:



- Enable Bridge Mode



- Use STP to protect against network loops from misconfigured networks
- Select the Inside Network Adapter

- Select the Outside Network Adapter
- Set a Bridge IP address or maintain the default value (See below for more details)

Module Configuration -> Bridge Managements

Version: 10.1.211129

Bridge Mode ON

Configure Bridge Module:

Spanning Tree Protocol	STP	Key
Inside Network Adapter	Adapter #1	
Outside Network Adapter	Adapter #2	
Bridge IP/Netmask	198.151.234.241/255.255.255.255	
Adapter Redundancy	Disabled	
Inside Network - Second Adapter		
Outside Network - Second Adapter		

Access Control List (ACL)

Enforcement Ranges

- Submit Changes (reboot will be performed)

Note: by default, inline enforcement will be disabled so unintended enforcement will not occur.

Note: Adapter Redundancy could be useful in environments with VPN concentrators configured in an Active \ Passive configuration.

Bridge IP

When endpoint access is controlled by the Inline EM, agents should audit with either the CGX Access Management IP or the Bridge IP address.


The Bridge IP allows for optimal scalability. Traffic to the bridge IP address is transparently intercepted when received on CGX Access appliances through the outside NIC. Using the same bridge IP address is important when there are multiple CGX Access servers deployed in Inline mode. Larger organizations may have dozens or even hundreds of remote access points. Keeping track of all the corresponding CGX Access addresses for each entry point would be a management burden. By using the same bridge IP address for all audits, CGX Access avoids this problem.

The bridge IP address can be any IP address that the VPN will route to the inside (trusted) network through the bridge interface on the CGX Access server. This ensures connections from agents can audit with the CGX Access appliances. The default bridge IP address is 198.151.234.241/255.255.255.255

Note: It's not typically required to change the default Bridge IP.

Access Control List

The Inline EM has its own ACL that is optimized for wire speed through-put. To edit the ACL click the Configure button.

Module Configuration -> Bridge Managements 

Version: 10.1.211129

Bridge Mode ON Enforcement Mode OFF

Configure Bridge Module:

Spanning Tree Protocol	STP	▼	Key	
Inside Network Adapter	Adapter #1	▼		
Outside Network Adapter	Adapter #2	▼		
Bridge IP/Netmask	198.151.234.241/255.255.255.255			
Adapter Redundancy	Disabled	▼		
Inside Network - Second Adapter		▼		
Outside Network - Second Adapter		▼		

Access Control List (ACL) [Configure](#)

Enforcement Ranges [Configure](#)

For ease of setup, the ACLs are pre-configured with settings that should address most organization requirements.

Global ACL - Devices without agents or not yet auditing is assigned the “global acl”.

```
# The global ACL is applied for all endpoints in the enforcement ranges. Other ACLs have priority
and can override the global ACL.
global acl
allow udp any any = 53
allow udp any any = 67
allow tcp any host $BridgeIP = 11698
deny tcp any any = 11698 redirect $BridgeIP 11698
deny tcp any any = 80 redirect $RemediationPortal 80
deny tcp any any = 443 redirect $RemediationPortal 443
```

- DNS and DHCP traffic are also allowed to pass through the appliance, even when restricted.
- Agent audit traffic (TCP 11698) will be redirected to the Bridge IP, so agents can audit with the inline appliance, even if the agents are configured to audit with a different IP address.
- The Global ACL will also redirect web browsers to the Remediation portal to allow for the download of agents or end-user communications.

Full-Access ACL - When a device is passing an agent audit, it will be assigned the “full-access” ACL.

```
# ACL for "full-access" endpoints
acl full-access
allow tcp any host $BridgeIP = 11698
deny tcp any any = 11698 redirect $BridgeIP 11698
allow ip any any
```

- The full-access ACL will allow Any IP traffic. This will override the Global ACL.
- The Agent audit traffic (TCP 11698) will continue to be redirected to the Bridge IP for continuous compliance checks.

Restrict-agent ACL - When a device is failing an agent audit, it will be assigned the “restrict-agent” ACL.

```
# ACL for "restrict-agent" endpoints
acl restrict-agent
allow tcp any host $RemediationPortal = 80
allow tcp any host $RemediationPortal = 443
```


You can customize the “restrict-agent” ACL to allow remediation resources. In the example above, a restricted devices can still access the remediation portal over port 80 and 443. This portal can be used to host automatic remediation scripts. The default “restrict-agent” doesn’t conflict with the “global-acl” so the global-acl will also be applied.

Restricted ACL - When a device is Blocklisted, it will be assigned the “restricted” ACL.

```
# ACL for "restricted" endpoints
acl restricted
```

This default “restricted” acl is blank. No lines override the “global-acl” so the global-acl will also be applied.

For additional help with the ACL, you can click the Help button.

[Module Configuration -> Bridge Management -> Access Control List](#) 
[Configure ACL:](#)

Enforcement Ranges

When working with Inline enforcement it’s common to need to limit the range of IP addresses that are subject to enforcement. For example, if deployed behind a Firewall \ VPN, you would want to set the enforcement range to only include the IP ranges of the VPN IP pool. When this is setup, only remote VPN users would be required to pass an agent audit. Note: For Testing purpose, you may want to limit the range to just one IP.

To Setup the Enforcement Ranges

- Click on Configure

Module Configuration -> Bridge Managements

Version: 10.1.211129

Bridge Mode ON Enforcement Mode OFF

Configure Bridge Module:

Spanning Tree Protocol	STP	Key
Inside Network Adapter	Adapter #1	
Outside Network Adapter	Adapter #2	
Bridge IP/Netmask	198.151.234.241/255.255.255.255	
Adapter Redundancy	Disabled	
Inside Network - Second Adapter		
Outside Network - Second Adapter		

Access Control List (ACL) [Configure](#)

Enforcement Ranges [Configure](#)

- Choose the Add Action

CGX Access Standalone Configuration Policies Control Visibility Welcome admin [Sign Out](#)

Module Configuration -> Bridge Management -> Enforcement Ranges:

Configure Enforcement Ranges:

Action	ID	Start IP	End IP	Submit
Add				Submit Action

- Complete the Start IP and End IP of the range and Click Submit

Module Configuration -> Bridge Management -> Enforcement Ranges:

Configure Enforcement Ranges:

Action	ID	Start IP	End IP	Submit
Add		192.168.253.50	192.168.253.99	Submit Action

- When all ranges have been specified – Click “Upload to Server” button
- Once Enforcement range is set, turn on Enforcement to test.

Enforcement Mode ON

Agent Requirement

The Inline Enforcement Module requires the use of agents on the remote endpoints.

Easy NAC virtual appliances come with default agents and default policies that can be used for testing or as a baseline to start building your custom compliance policies. An agent license is required to use the agents.

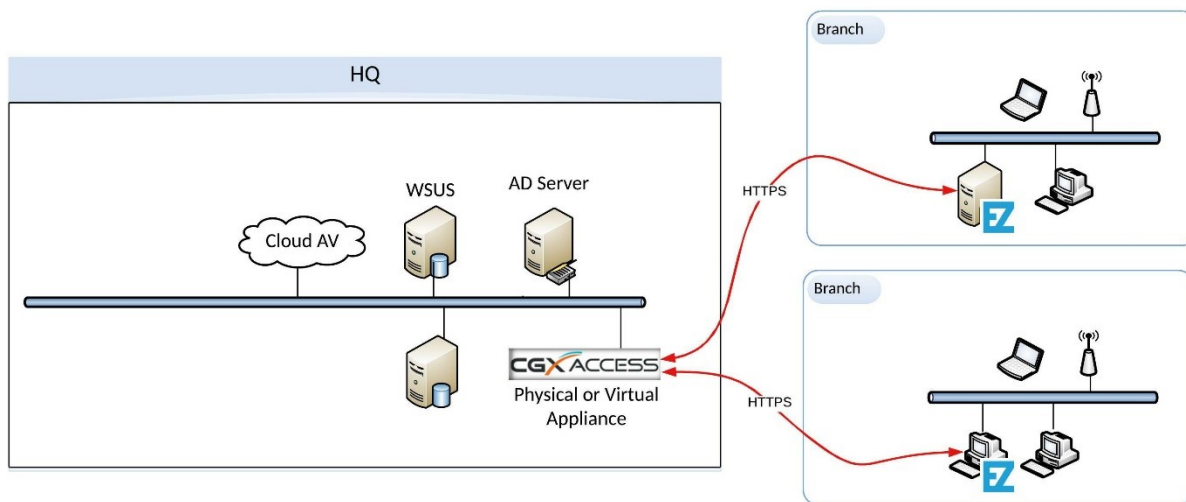
To customize the policies or agent, you will need to install the CyberGatekeeper Policy Manager (CGPM). Contact InfoExpress or your partner for the CGPM installer.

Appendix D – Enforcer Agents

Enforcer Agents Overview

The Easy NAC solution uses CGX Access appliances for visibility and protection of the network. To provide visibility and protection, the CGX Access appliance requires layer-2 visibility of the subnets it's protecting. Having layer-2 visibility at the main site can be easily achieved with trunk ports or standard access ports. However, getting layer-2 visibility for remote sites can be more challenging. At the remote sites, the Enforcer Agent can be deployed on Windows platforms to get this visibility and local enforcement at remote sites.

The Enforcer Agent architecture is shown below. At remote sites, the Enforcer Agent software is installed on a Windows 64-bit OS. The agent would then communicate back to the CGX Access appliance to report in real-time what devices are on the network. The CGX Access appliance would then profile these devices and tell the Enforcer Agent what access should be assigned. The Enforcer agent would then apply the ARP enforcement. Both MPLS and NAT'd network types are supported. However, with NAT'd networks only rogue prevention features are supported, as the CGX Access appliance may not be able to fully profile the remote devices. If using NAT'd subnets, the vLinks solution may be a better approach to extend the protection.



Adding Enforcer Agents to extended CGX Access protection to remote sites is a simple process that consists on installing the Enforcer Agent and then accepting this agent in the CGX Access management interface.

Enforcer Agent Install

Contact your InfoExpress partner, representative or support for a copy of the EZ-Defaults Enforcer Agent Installer. This Enforcer Agents will work with CGX Access Appliances version 3.1.220317 and above that are using default shared settings. Enforcer agents are licensed separately.

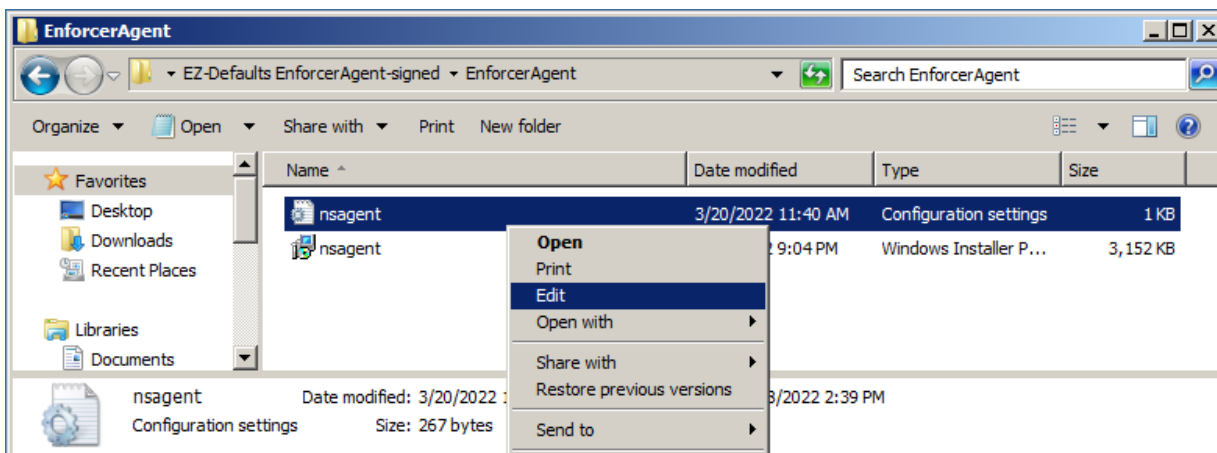
Note: If your organization is using the CyberGatekeeper Agents, with unique shared settings, then it may be necessary to build an Enforcer Agent in the CyberGatekeeper Policy Manager so it's compatible with your organization's unique shared settings.

The Enforcer Agent is supported on Windows 10 or higher and Windows Server 2012 or higher; 64-bit OS is required. The agent is light-weight and works with the minimum OS requirements.

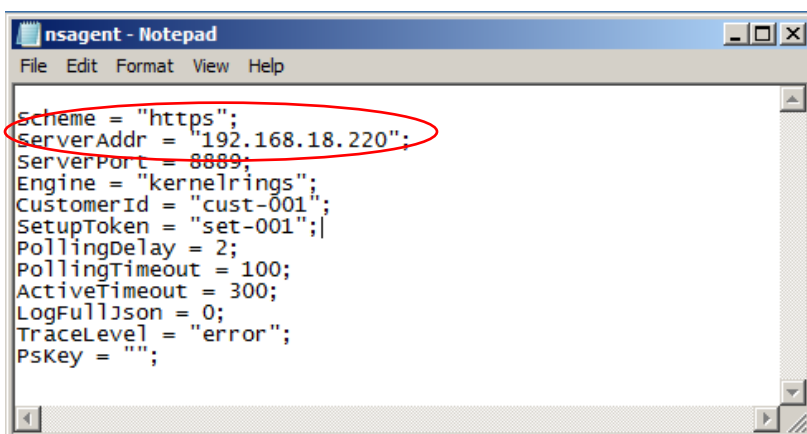
The Enforcer Agent installer will be provided as a compressed folder that contains two files. An MSI installer (nsagent.msi) and a configuration file (nsagent.ini).

Step 1 – Unzip the package

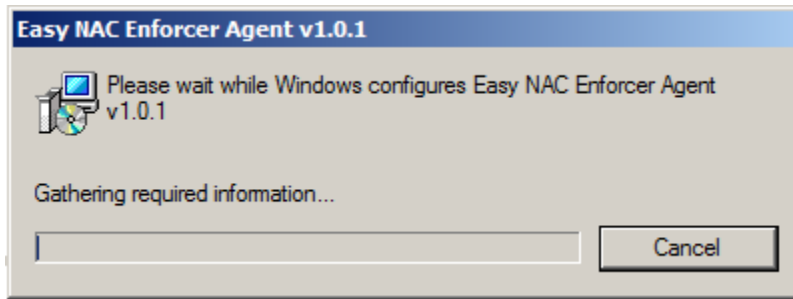
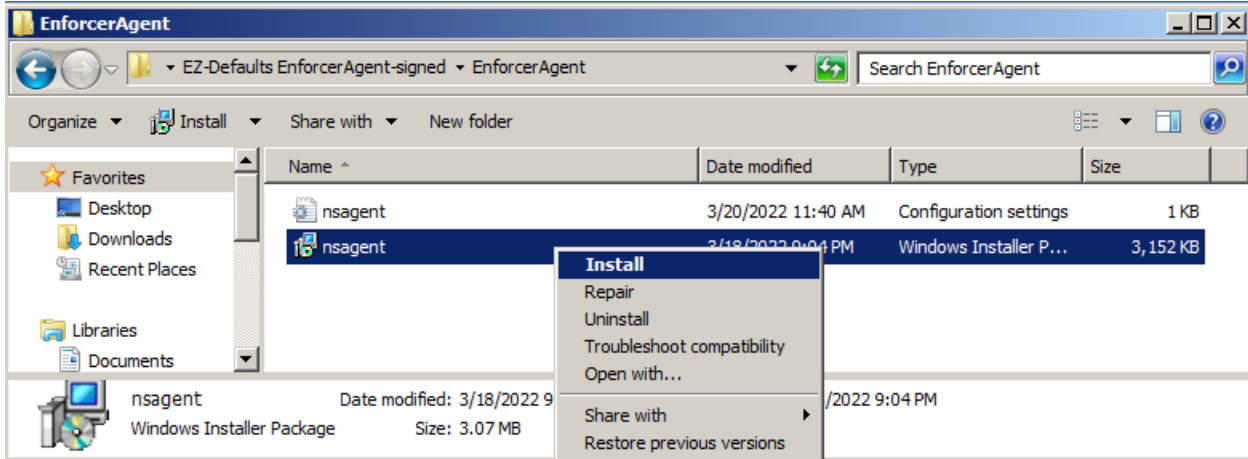
Step 2 – Edit the Configuration settings (nsagent.ini). **Right click** and select **Edit**.



Step 3 - Change the ServerAddr value to point the Management IP of your CGX Access appliance. Alternatively, you can add a domain name entry for CGX-Access in the DNS server.

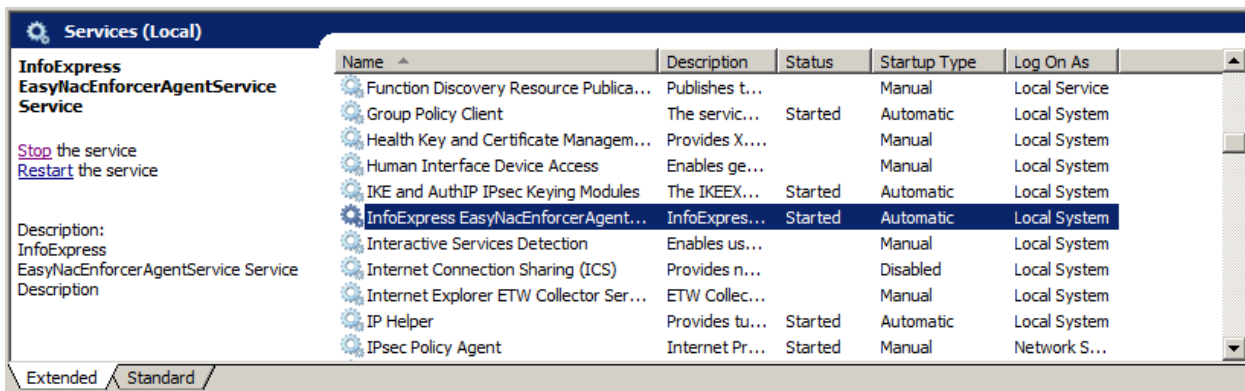


Step 4 – Install the Agent – Right Click and select Install (Administrative Rights Required)



Note: The install process will take only take about a minute to complete, and the dialog box will close itself automatically.

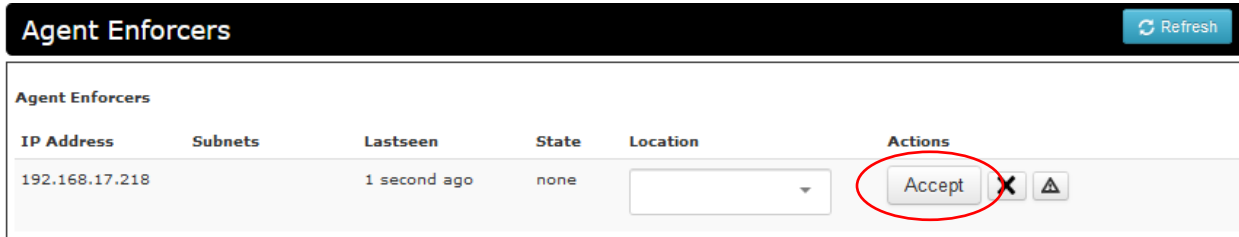
To confirm the Enforcer Agent was installed properly, Run Services.msc and confirm the following process is started and Startup type is Automatic.



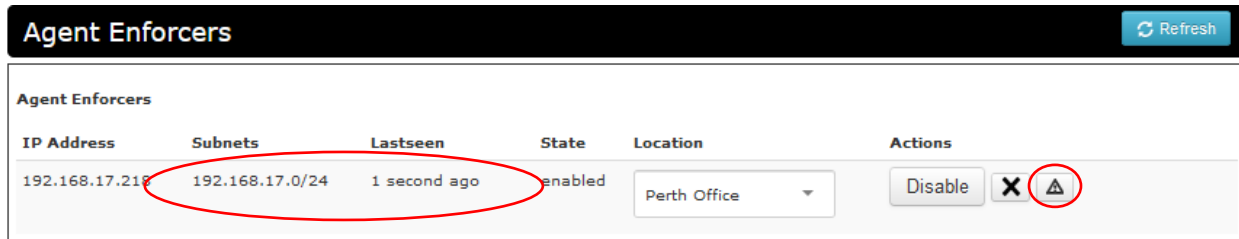
Accepting the Enforcer Agent

Once the agent is installed, go to the CGX Access Appliance, Login into CGX Access web interface.

- Go to: Control > Agent Enforcers



- Click Accept
- Add a descriptive name in the Location box
- Click Refresh, you will see the subnet range that is being protected and when the agent was last seen.



Tip: It's recommended to configure an alert so if the agent stops communicating back to the appliance you will receive an email alert.

Verify Network and Devices are Visible

Once the Enforcer Agent has been Accepted it will be managed like other subnets in your system, and should be seen in the Network Map. By default, it will be in Monitor mode.

- Go to: Control > Network Map

Network Map

CGX Access

Enabled

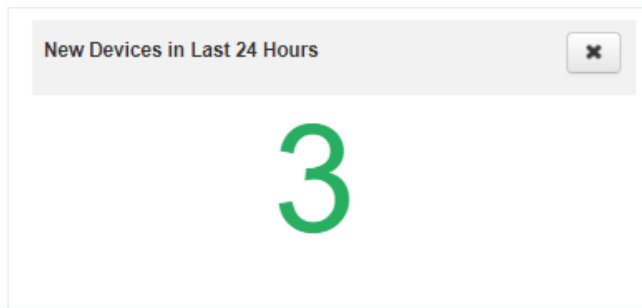
Default configuration (applied to all subnets) [Show Configuration](#)

Subnets

Network	Last seen	Mode	
192.168.18.0/24	9 seconds ago	Monitor	Show Configuration
192.168.17.0/24	27 seconds ago	Monitor	Show Configuration

Save Cancel Help

- Go to Visibility > Dashboard
- Check the Widget for Device seen in the last 24 hours



If you have the expected visibility with devices shown from the remote subnet, the Enforcer Agent is working. The existing Policies and Access Groups will now be applied at this remote site.

Appendix E – WhatsApp Integration

CGX Access can send administrative notifications via WhatsApp and also can be used for guest access approval.

Notifications

In an effort to prevent spam on the WhatsApp network, Meta (formally known as Facebook) requires the use of 3rd party API providers. The CGX Access solution was designed to work with Twilio as this API provider. Therefore, in order to use this WhatsApp integration feature, it does require a Twilio account and Facebook Business Verification. Below is the list of prerequisites steps:

WhatsApp Prerequisites Steps

1. An account on Twilio - <https://www.twilio.com/whatsapp>
2. A Twilio phone number (Credit Card required)
Note: using a USA number is the most cost-effective option. \$1 per month for the number, with \$0.0135 per WhatsApp message sent. Pricing varies by county. For current pricing, check <https://www.twilio.com/whatsapp/pricing>
3. Facebook Business Manager ID - <https://business.facebook.com>
[Facebook's instructions on setting up a business manager account.](#)
Note: Need Facebook Profile (can be personal) to create Facebook Business Manager ID. Organizations can have more than one Business Manager ID, so IT department can create their own.

WhatsApp Registration Process

Step 1: Request access to enable your Twilio number(s) for WhatsApp

In order to enable your Twilio number(s) for WhatsApp, you will need to fill out "[Request Access](#)" [form](#) with accurate and up-to-date information, including your Facebook Business Manager ID

Note: When asked if working with an ISV or 3rd-party, answer NO

After you submit the "Request Access" form, you will receive an email confirming the form submission. Once Twilio reviews your account, you will receive an email with subject "You are now pre-approved to use Twilio APIs for WhatsApp". Final approval is provided by WhatsApp after you submit your sender profile (next step).

Step 2: Submit a Sender Profile

[Click here](#) or navigate to the Messaging > Senders > WhatsApp Senders section in the Twilio Console. Click the "Submit a WhatsApp Sender" button to create a new sender profile.

WhatsApp Enabled Senders

To use a number with WhatsApp, you need to register it as a WhatsApp sender. You can use your own number or provision one from [Twilio Phone Numbers](#).
To send notifications, you will also need to use WhatsApp approved [message templates](#). [Learn more about creating a sender](#)

Submit your first WhatsApp Sender

- The submission process takes about 5 minutes.
- WhatsApp will approve or reject the sender in 2-5 business days.
- WhatsApp allows a maximum of 25 approved senders per account (up to 120 upon request).

[Submit a WhatsApp Sender](#)

Note: Your Sender "Display Name" must be the business name used in the Facebook Business Manager account.

Step 3: Approve Twilio to send messages on your behalf

When you receive notice that Twilio has submitted your Display Name and number to WhatsApp, you will need to approve Twilio to send messages on your behalf. You will receive an email to "Approve Twilio to message on behalf of" in Facebook Business Messenger.

Go to the Facebook Business Manager console (the one that you submitted in Step 1) and approve Twilio to "message on behalf of." You can find this request by [following this link](#), or navigating to [business.facebook.com](#) > Business Settings > Requests section. Once there, click the **Approve** button.

Step 4: Verify your Facebook Business Manager account

After you have "Approved" Twilio to send messages on your behalf, you will be able to verify your Facebook Business Manager account. In the [Facebook Business Manager > Settings console](#), click the **Start** or **Continue** button under in the **Verification** section to complete Facebook Business Verification Process.

You may be required to upload supporting documents to verify your business. See Facebook's [guide on uploading official documents to verify your business](#) for more information.

Note: Approval can take several days

Step 5: Twilio completes your WhatsApp Sender registration

After you approve Twilio to message on your behalf, Twilio will complete the registration process to register your WhatsApp sender. You will receive an email confirmation that Twilio has finalized the registration of your profile.

Step 6: Submit Message Templates

To prevent spam only specific pre-approved message templates can be sent via WhatsApp. To submit a message template, navigate to Messaging > Senders > [WhatsApp Templates](#).

For Easy NAC integrations, the following four message templates needs to be created.

Template 1: System Notifications

Template Name: system_notifications	Template Category: Alert Update
Message language: English	Buttons: None
Message Body:	
Admin alert on system:	
{{1}}	
EasyNAC IP: {{2}}	

Template 2: Device Profiler Notifications

Template Name: device_profiler_notification	Template Category: Alert Update
Message language: English	Buttons: None
Message Body:	
Admin alert on device {{1}}	

Template 3: Device Notifications

Template Name: device-notification	
Template Category: Alert Update	
Message language: English	
Buttons: None	
Message Body:	
Admin alert on device	
IP: {{1}}	
MAC: {{2}}	
Hostname: {{3}}	
Location: {{4}}	
Access Group: {{5}}	
Role: {{6}}	
OS: {{7}}	
First Seen: {{8}}	
Tags/Lists: {{9}}	
EasyNAC IP: {{10}}	
Message: {{11}}	
See Visibility - Alerts and Notifications for details.	

Template 4: Guest Notifications

Template Name: guest-notification
Template Category: Alert Update
Message language: English
Buttons: None

Message Body:

{{1}} just sent you a network access request.
MAC: {{2}}
IP: {{3}}
Fullname: {{4}}
Email: {{5}}
Phone: {{6}}
Company: {{7}}
To grant guest access:
Please enter: {{8}}
To deny guest access:
Please enter: {{9}}

Note: Additional guest templates may be necessary depending on the guest registration process implemented in your organization.

Enabling WhatsApp Alerts

Once the registration process is complete, it's simple to enable CGX-Access to send admin alerts.

- Go to Configuration → General Settings and click on **Other Servers**

Here you can input the WhatsApp number that has been approved as WhatsApp Sender.

Note: The Account ID and Auth Token, can be found in your Twilio Console under Account > General Settings

The screenshot shows the 'WhatsApp Provider' configuration page. At the top, there are tabs for 'RADIUS Server', 'Radius Clients', 'DHCP Servers', 'Web Proxy Server', 'SMS Gateway', 'WhatsApp Provider' (selected), 'Slack App', and 'Teams App'. The page is divided into two main sections: 'Twilio WhatsApp API' and 'Query Settings'. Under 'Twilio WhatsApp API', there are three input fields: 'From Contact' with the value '+1800000000', 'Account ID' with the value 'AC03753642c0ef8d748379b34ec6', and 'Auth Token' which is masked with dots and has an eye icon to toggle visibility. A 'Send Message' button is located below these fields. The 'Query Settings' section includes a checked checkbox for 'Enable approve guest from WhatsApp', and two input fields for 'Approve guest when matching pattern' (with the value 'Approve') and 'Reject guest when matching pattern' (with the value 'Reject').

- Go to Configuration → General Settings and click on **Contact Information for Notifications**

Here you can input the WhatsApp number of your admins

#	Name	E-mail Address	SMS Number	WhatsApp Contact	Slack Channel/User ID	Teams Channel/User ID	Action
1	Admin	admin1@mycompany.com					<input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	Second Admin2	admin2@mycompany.com					<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Enabling WhatsApp for Guest Approval

To enable WhatsApp for Guest approval a few extra configuration steps are required.

- Go to Configuration → Server Settings and click on **Servers**

In the same section the WhatsApp number was specified, click the **Enable Guest Access from WhatsApp** and specify the keywords to be used for Approval or Rejection

- Go to Configuration → Device Registration Templates >> **Guest Registration Templates**

In these desired guest templates, add the WhatsApp number that Guest Requests should be sent. Each template can use a different WhatsApp approver.

Edit Action ✕

Confirm Guest Flag Guest

Allow guest to provide sponsor email

Approval Email

WhatsApp

Appendix F – 802.1x RADIUS Proxy

Radius Proxy Overview

For customers using 802.1x authentication, the Easy NAC appliance can act as a RADIUS proxy. With this setup, an end-user's 802.1x user name can be captured at login time. In addition, the switch and port the device is connecting from is also monitored for reporting purposes. This information can be then be used to enhance our ability to detect and prevent MAC spoofing real-time, and can also be used for Multi-factor Authentication.

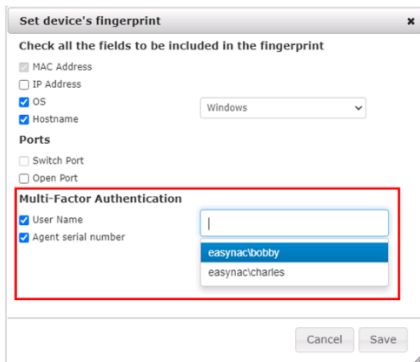


Requirements

- A third-party RADIUS Server
- A working 802.1x environment. Before adding CGX Access as a RADIUS Proxy, first have your wireless controller or switches configured and working with 802.1x and/or MAB.
- Once 802.1x is working as expected, then CGX Access can be added into the RADIUS stream. On the switches, CGXA would be configured as the primary Radius server, and the real RADIUS server as the secondary server, for fail-open purposes.

Features

- Captures the end-user name which can be used for [Multi-Factor Authentication](#)



- Captures the switch IP and switch port info, which can be included in a Fingerprint to strength security of Mac Address Bypass (MAB). When enabled a trusted MAC address must be attached to the correct switch and port.

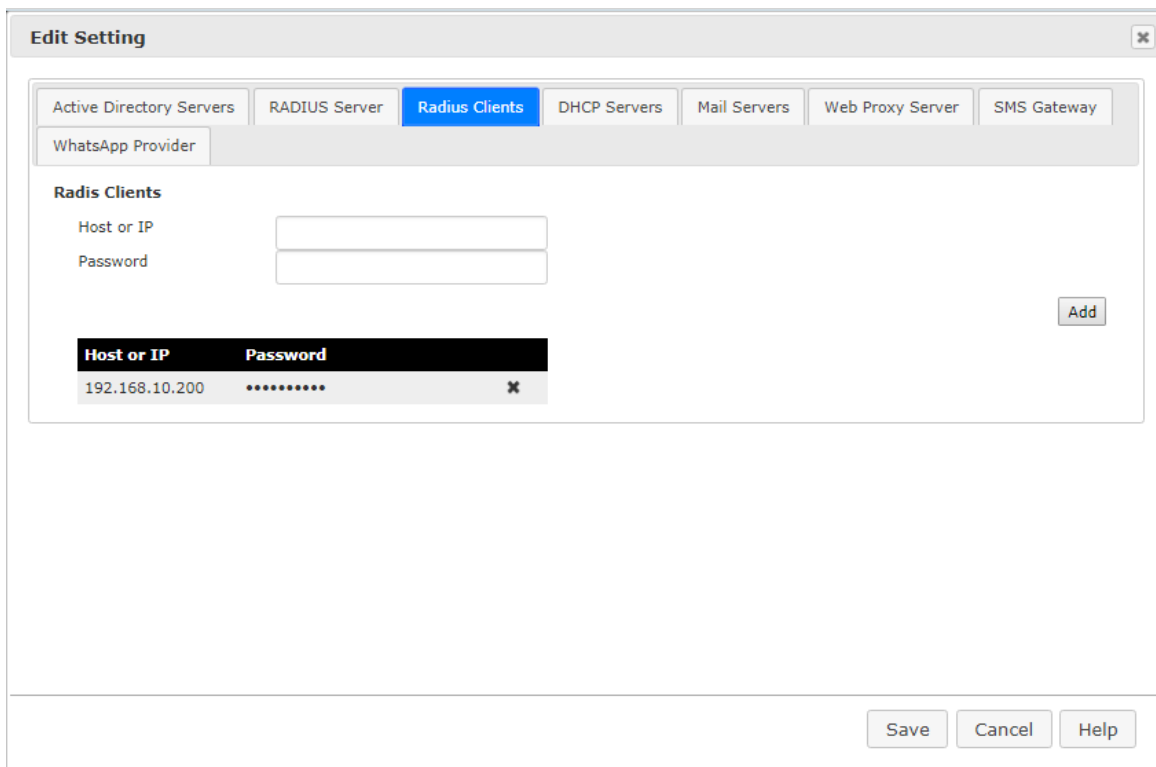
Configuring Radius Proxy settings on CGX Access

- In CGX Access GUI go to Configuration → General Settings.
- Click on Servers

- Under “Radius Server” tab, enter the Hostname or IP address of the Radius server

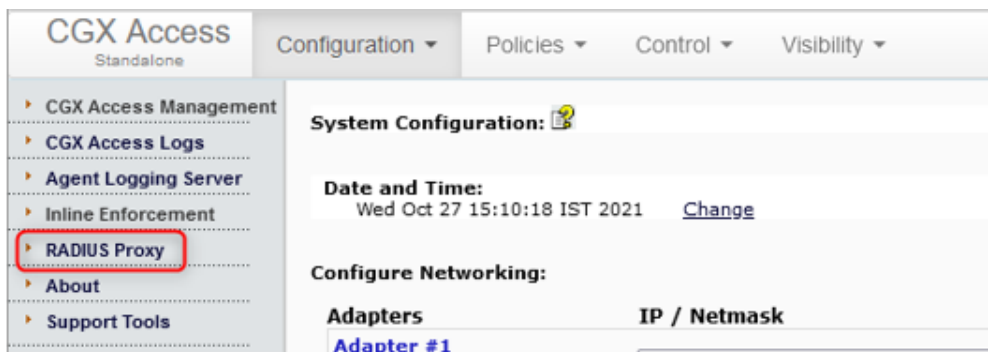
- Enter the shared secret. It should be the same as configured for this CGXA IP under “Radius clients” on the Radius server.

Next, click on “Radius Clients” tab

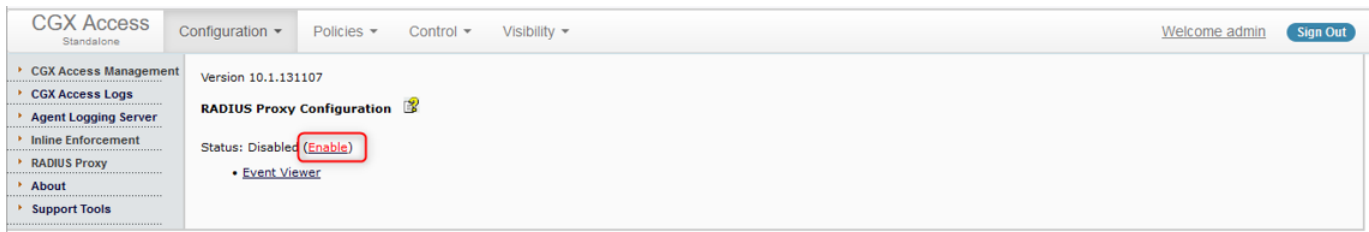


- Enter Radius client (Wifi controller/Switch controller) hostname or IP.
- Enter radius password. This password should match the radius secret configured on the radius client.

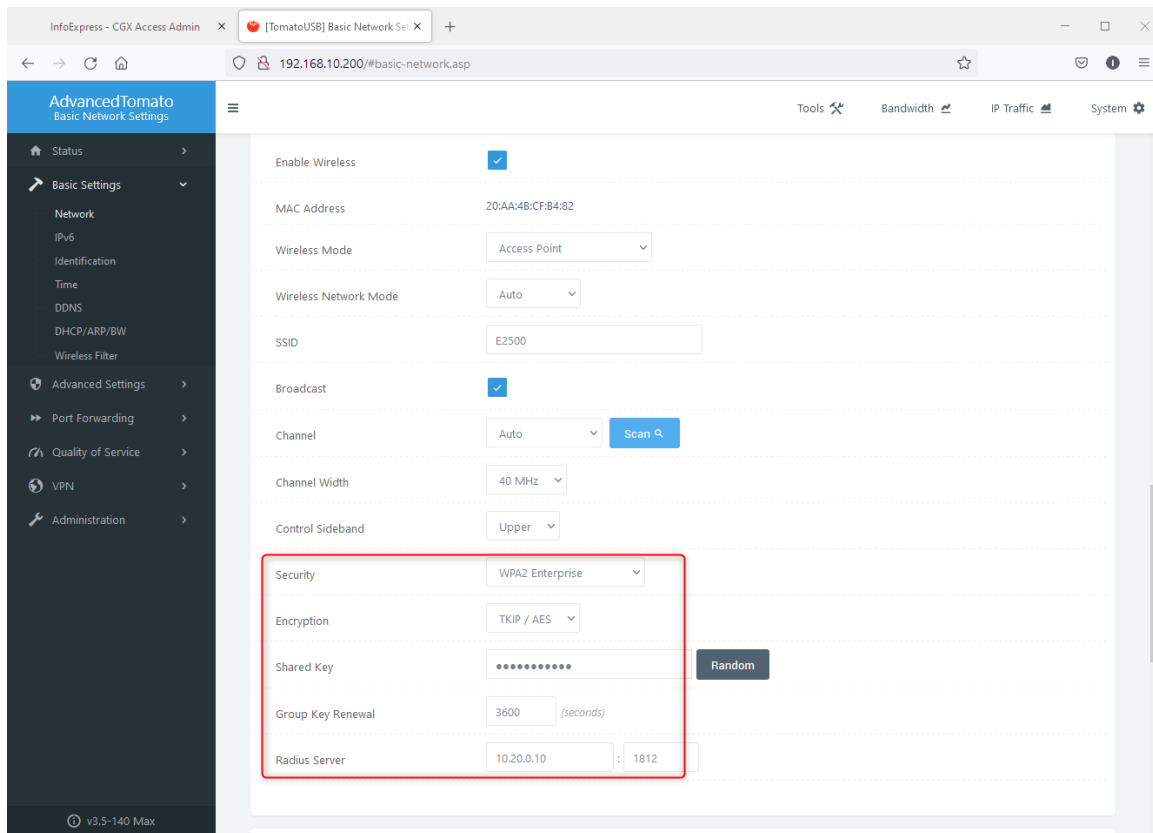
In CGX Access GUI go to Configuration → Appliance Settings → Radius Proxy



Enable Radius Proxy Module



- Configure your Wifi Controller or Switch with CGXA IP as the radius server
- Configure the same shared secret as configured in “Radius clients” on CGXA earlier.



Connect a wireless end point and enter user credentials configured on Radius Server.

Confirm details on Device manager page on CGXA

Device Manager

All Unique Devices Identified by CGX Access Back Refresh Export Help

Updated at Mon Jan 10 2022 11:32:50

Cover Devices Active in: Past 24 Hours

Show Report Filter

Select an Action Apply to selected devices

Total # of Devices: 6

Make it a Custom Report Add a Scheduled Report Devices per Page 100 Page 1 of 1. First << [1] >> Last

<input type="checkbox"/>	MAC	Hostname	User	Access Group	Roles	OS	Vendor	Flags / Lists	IP Address	Last Seen	Comment	Access Status	Grant Access	
<input type="checkbox"/>	00:1E:58:A9:C2:AF	win10x64-2004	zeeshan (from Radius) s1zeeshan (from Agent)	full-access	full-access	WinX64 10 Enterprise 6.3 Build 19042 Service Pack None	D-Link Corporation	webserver	192.168.10.7	2022-01-10 11:32:21	●	ON OFF Auto	

Device Detail Data ✕

General
NMAP
DHCP
Web
Radius
State
CGA
DPM
Last Audit

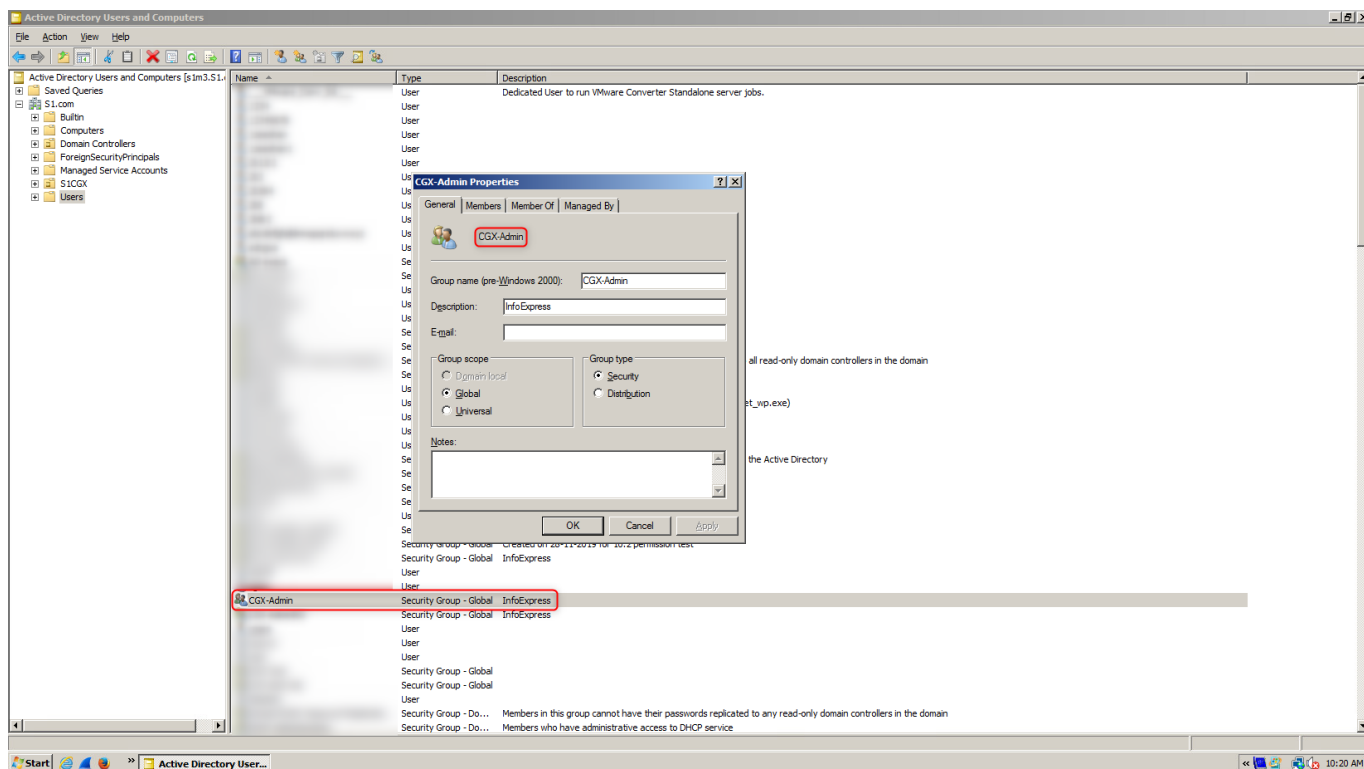
```
{
  "NAS-IP-Address": "192.168.10.200",
  "NAS-Port-Type": "Wireless-802.11",
  "NAS-Port": 4,
  "User-Name": "zeeshan",
  "Called-Station-Id": "20aa4bcfb482",
  "Calling-Station-Id": "001e58a9c2af",
  "NAS-Identifier": "20aa4bcfb482",
  "Accept-Vendor-Specific": {
    "MS-CHAP-Domain": "\u0001S1"
  }
}
```


Appendix G – Using NPS to Authenticate CGX-Access users

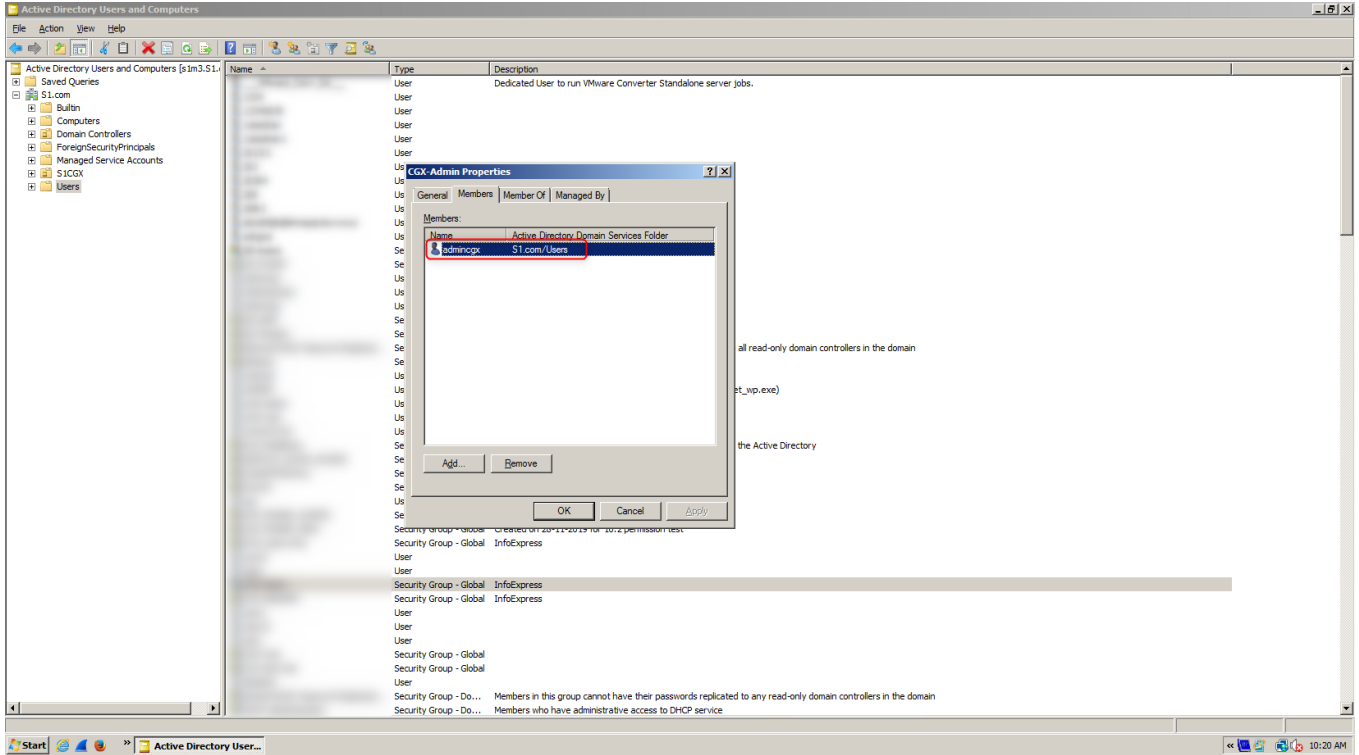
CGX Access can leverage Microsoft Network Policy Server (NPS) and other Radius servers for Management and/or BYOD authentication. The steps below are specific to NPS.

Add admin group/users to Active Directory

1.1 Create a security user group in Active Directory named “CGX-Admin”

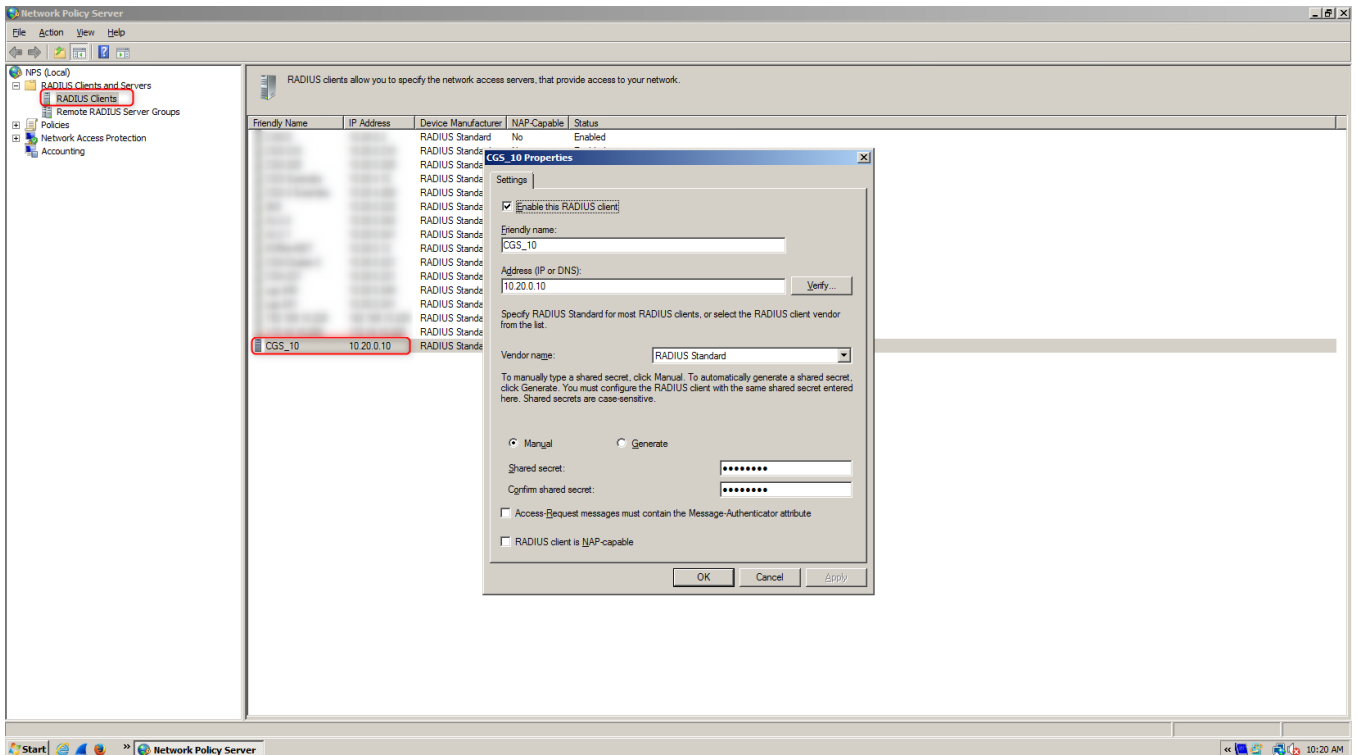


1.2 Add members to this group who should have admin read-write access to CGX-Access

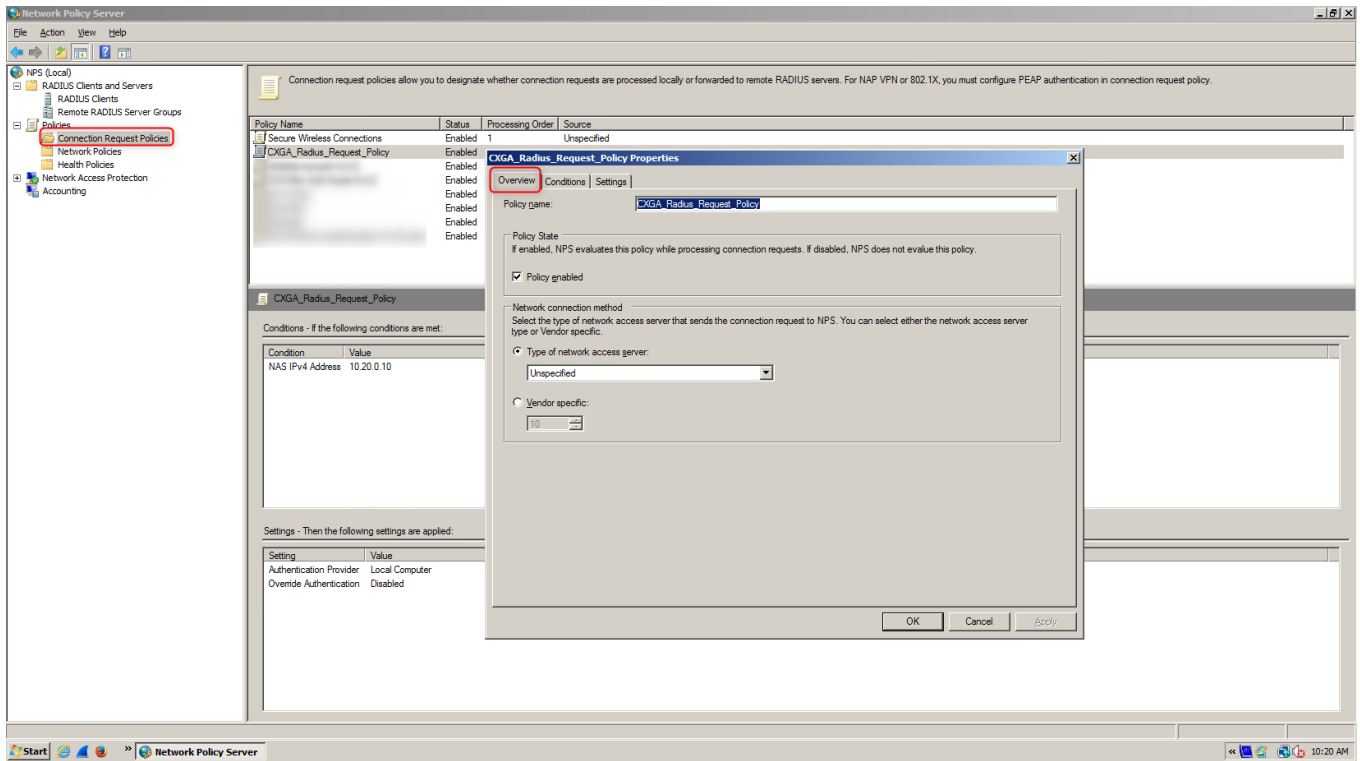


Configure Network Policy Server

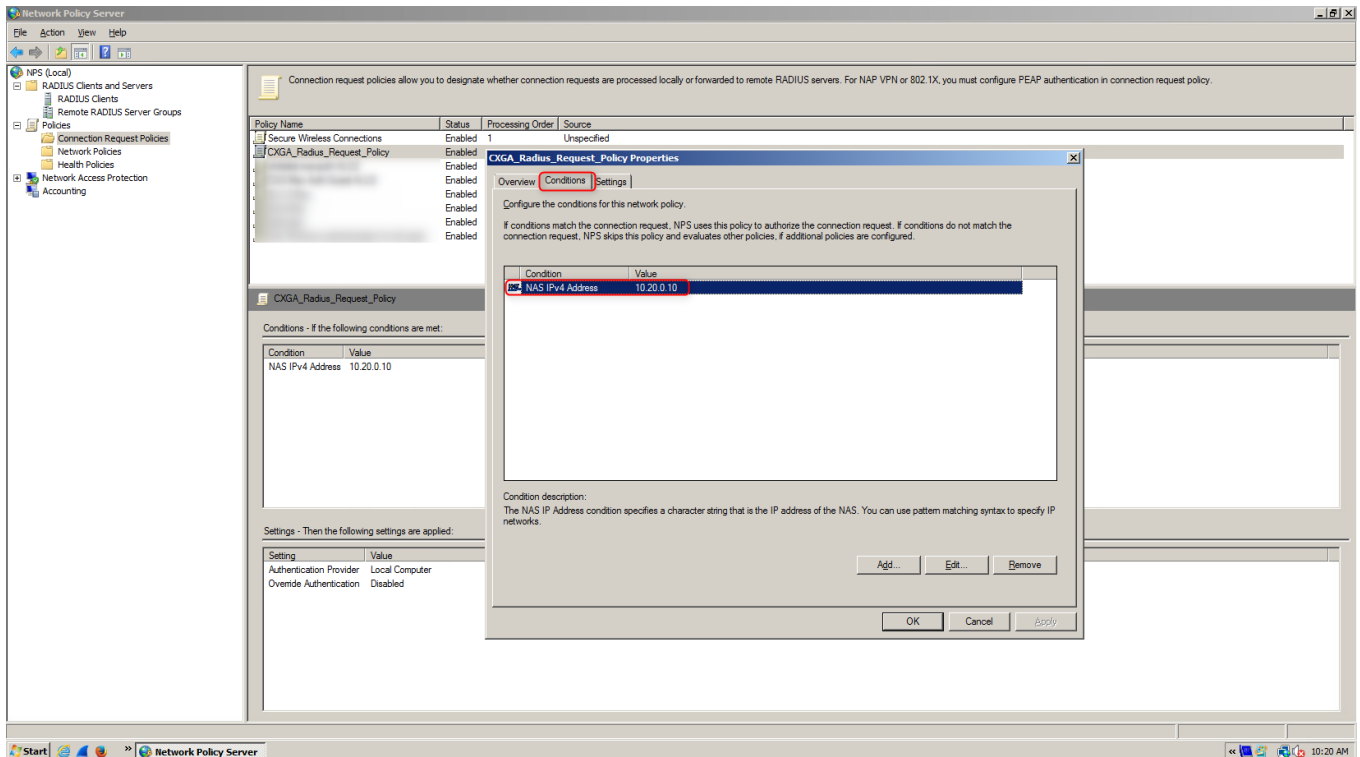
2.1 Open "Network Policy Server" and add CGX-Access as a radius client.



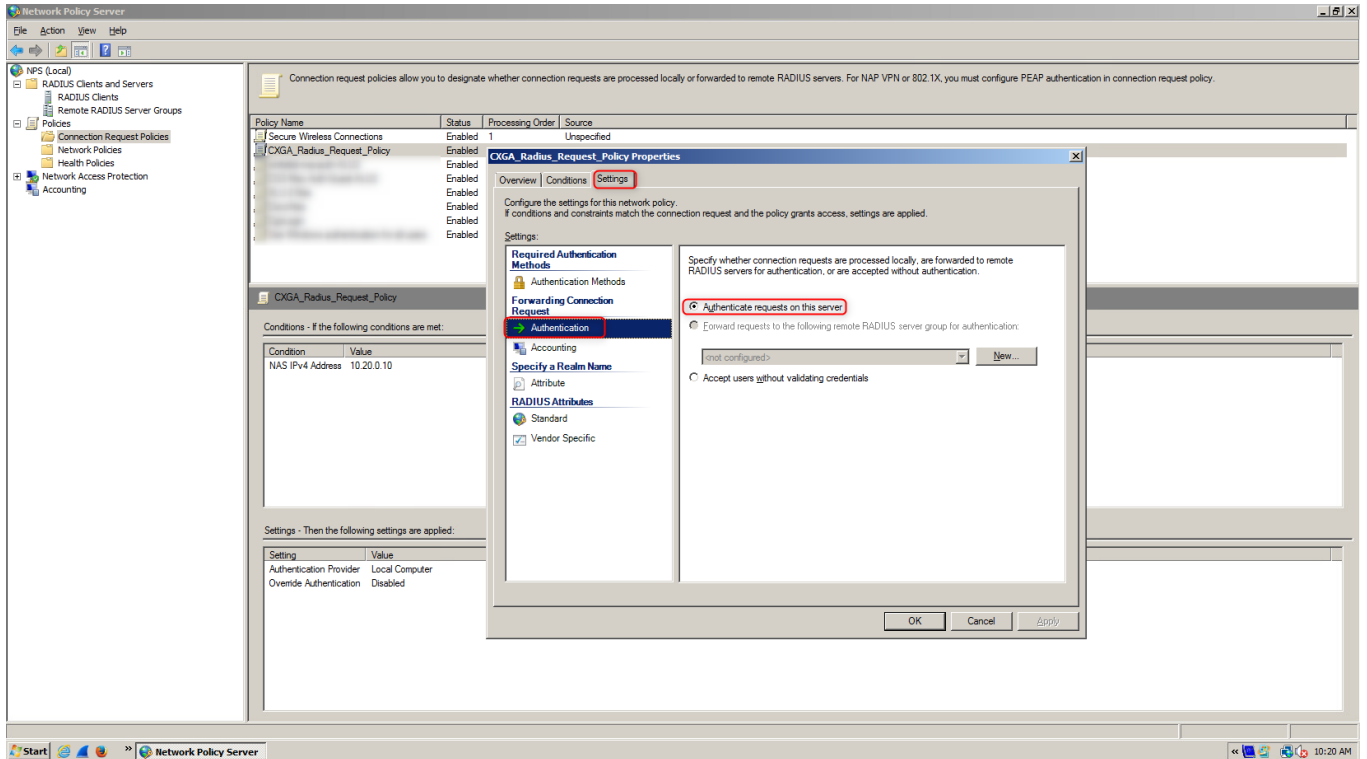
2.2 Create a new Connection request policy with parameters as shown in screenshots below.



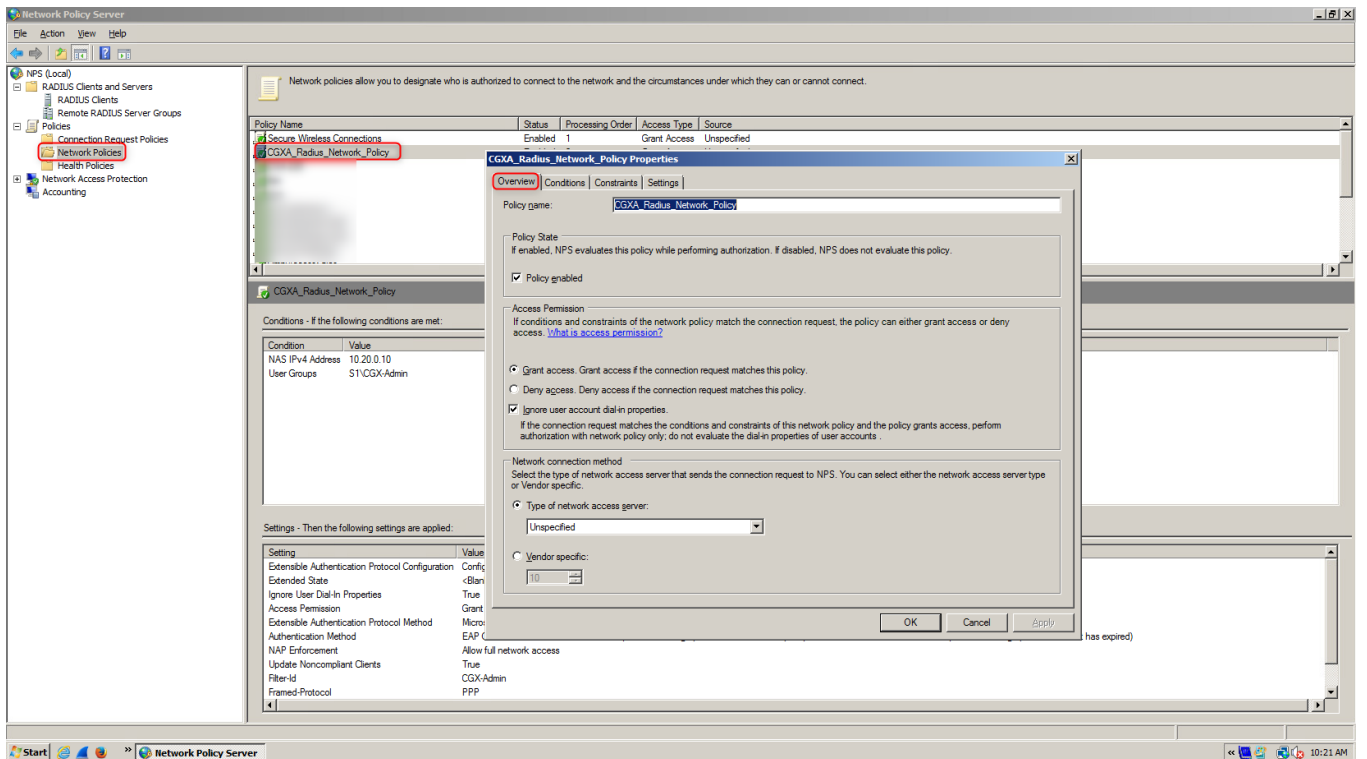
2.3 Add CGX-Access IP address in "Conditions" tab as "NAS IPv4 address"



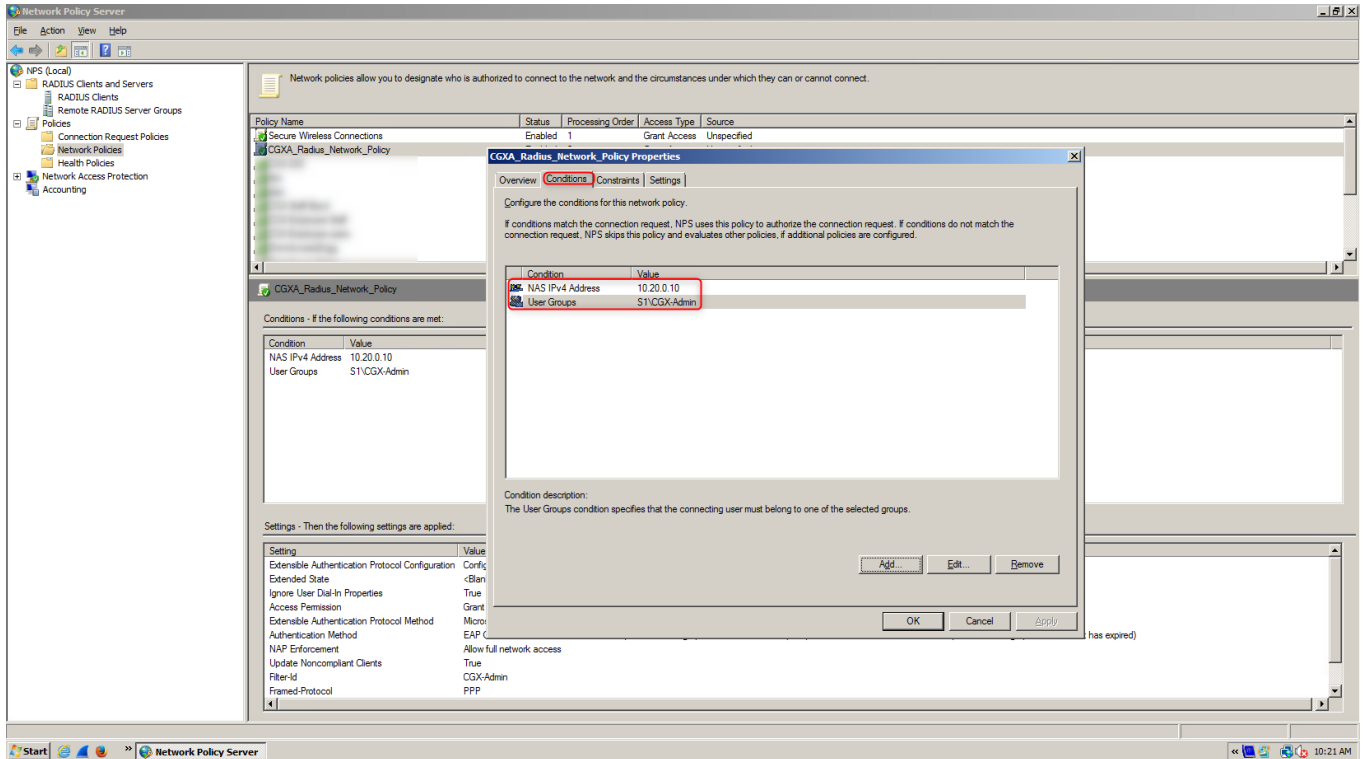
2.4 Under “Settings” tab select “Authenticate requests on this server”



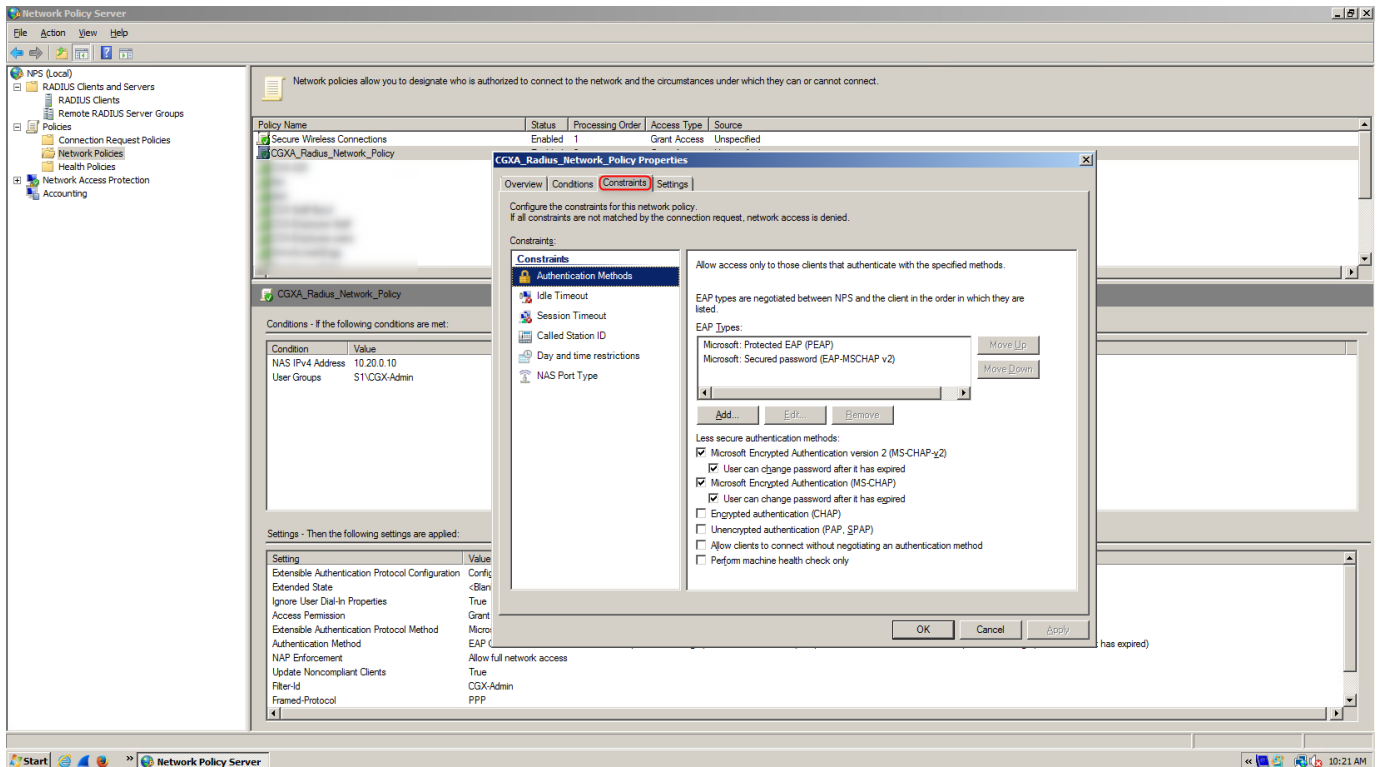
2.5 Add a new Network policy for CGX-Access



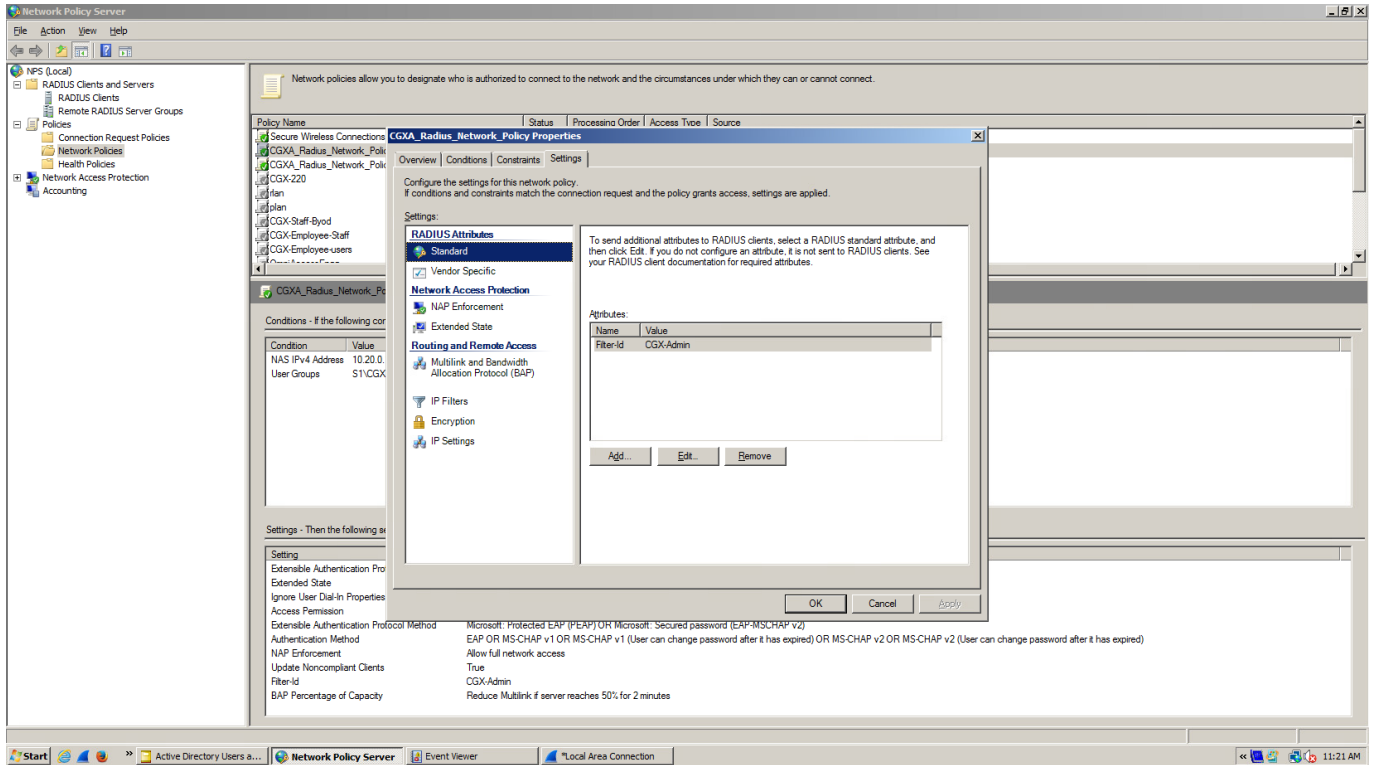
2.6 Under “Conditions” Tab add “NAS IPv4 address” and “User Groups” (Domain\CGX-Admin)



2.7 Under “Constraints” select the “Authentication Methods”

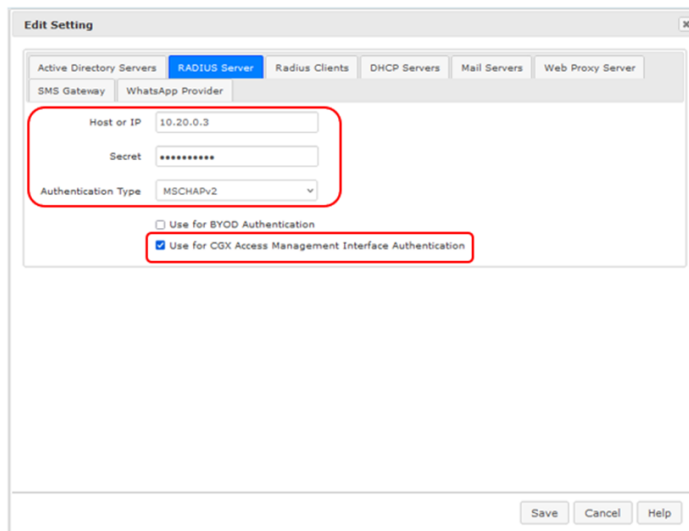


2.8 Under “Settings” tab Select “Standard” and add “Filter-id” as CGX-Admin



Configure CGX-Access to allow login using radius

- 3.1 Go to CGX-Access > Configuration > General Settings > Servers > Radius Server
- 3.2 Add the NPS server IP and configure same secret as configured on NPS server.
- 3.3 Select “Use for CGX Access Management Interface Authentication”



- 3.4 Save
- 3.5 Logout of CGX and login using the username that was added to AD group CGX-Admin.

To authenticate BYOD users via Network Policy server

Follow the steps above, however in steps

- # 1 You can use existing groups or create a new one and add users to that group.
- # 2.5 Create new policy to authenticate BYOD users, and add byod user group in #2.6.
- # 2.8 Skip this step.
- # 3.3 Select "Use for BYOD Authentication"

Tip: For any troubleshooting logs on NPS server

Start Event Viewer > Custom Views > Server Roles > Network Policy and Access Services

End of Document