# EASY NAC

## CGX ACCESS DEPLOYMENT GUIDE

### Installation and Configuration Guide



www.infoexpress.com

www.easynac.com

V2.4.200928

# Contents

# 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 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.

### 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 Whitelisting
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 flagged as approved. In addition, device profiling can also be used to automate the process of flagging 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, and Hostname. 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.

## Automated Threat Response – Zero-day Behavioral Detection

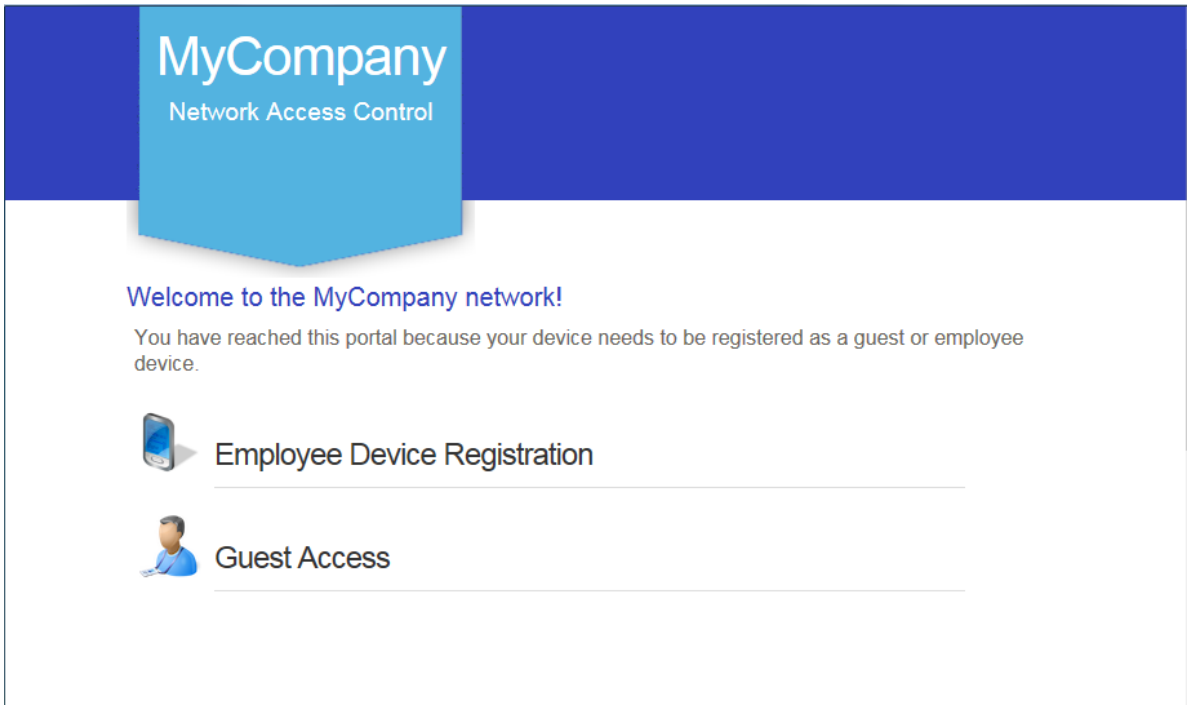
CGX Access unique layer-2 visibility of the network allows for the immediate detection of suspicious behavior, such as devices making excessive connections attempts to endpoints on the same network segment. This real-time detection provides immediate protection against zero-day malware propagating on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

## 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.

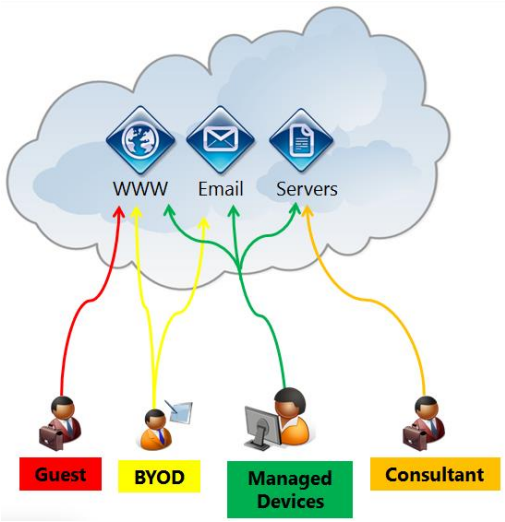
## Guest Access

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 an appliance, mini-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

| Appliance Specifications | Access Mini CGXA-S10 | Access 100 CGXA-S100 | Access 500 CGXA-S500 | Access VM CGXA-V50 | Access VM CGXA-V100 | Access VM CGXA-V200 |
|---|---|---|---|---|---|---|
| Scalability | | | | | | |
| Maximum Devices | 300* | 2500* | 10,000* | 2,500* | 5,000* | 10,000* |
| Maximum Subnets | 10 | 100 | 200* | 50 | 100 | >200* |
| Number of Ports | 4 | 6 | 8 | 8-10 virtual adapters | 8-10 virtual adapters | 8-10 virtual adapters |

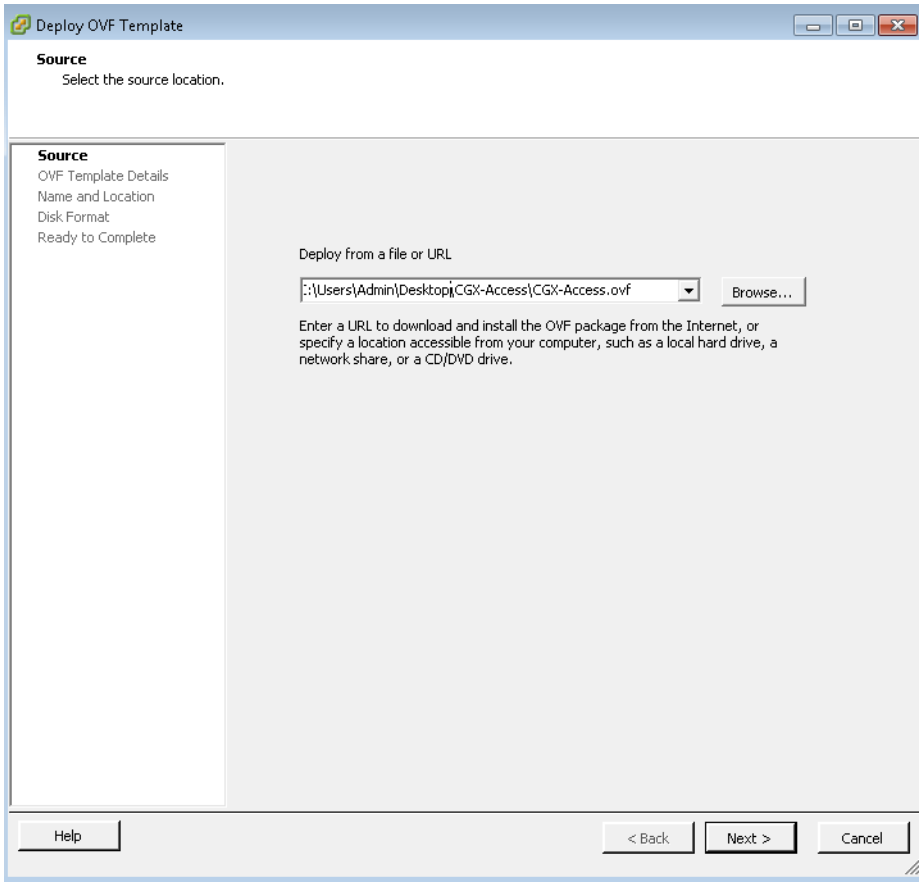
* Capacity is approximate and depends on VLANs protected, endpoints, and features enabled.

# 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

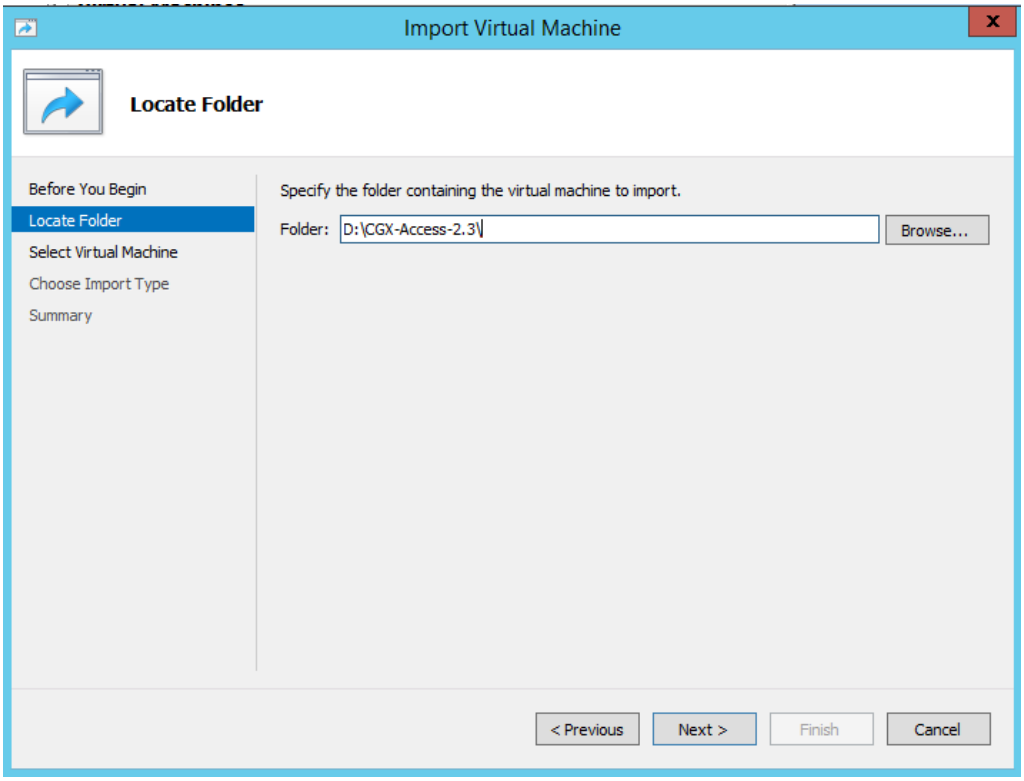



- Click next on the OVF Template Details screen. (There may be a warning screen here, but you can proceed).
- Provide a name and optionally a location for the template and click 'Next'
- Select the datastore where the virtual machine files should be kept and click 'Next'
- Select the desired format for 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.

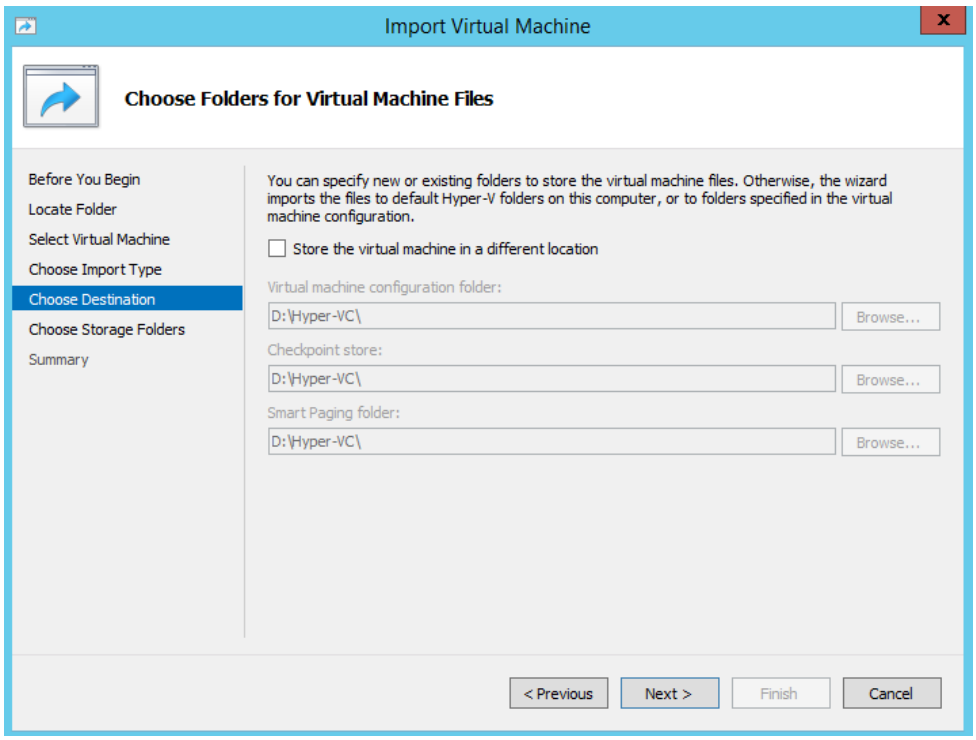
# Installing on Hyper-V server

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.

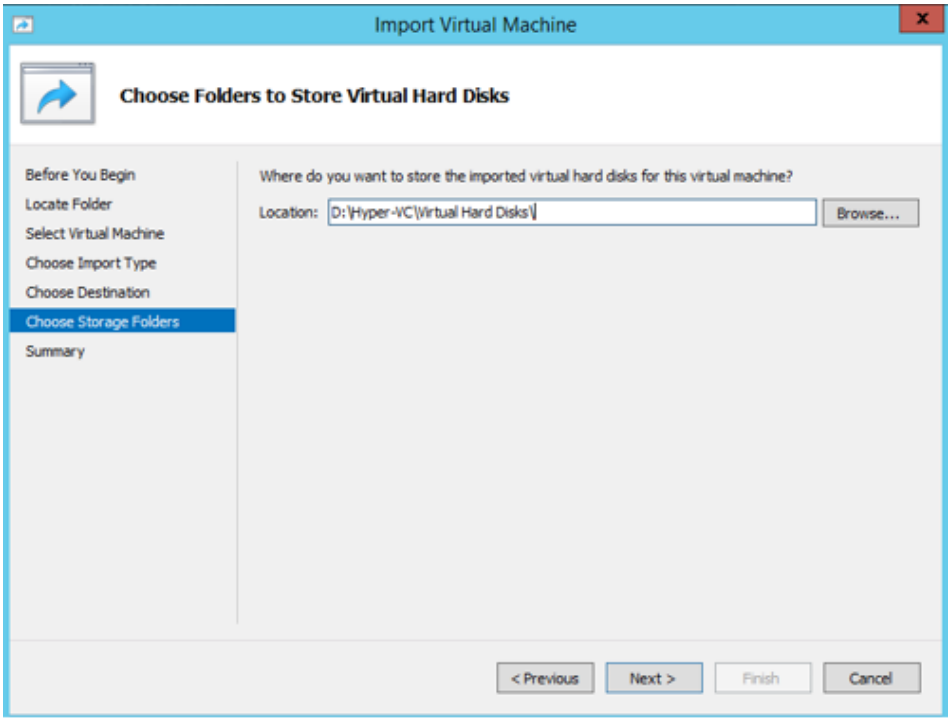
- Unzip the provided file to a location accessible to the Hyper-V Manager.
- In the Hyper-V Manager, Click Action menu and select Import Virtual Machine
- On the first screen, Specify the folder of extracted image and click next




- Select the listed virtual machine ‘CGX-Access-2.4’. Click next.
- Choose Import type as ‘copy the virtual machine (create a unique ID)’
- Click Next and specify the Destination folders for different settings

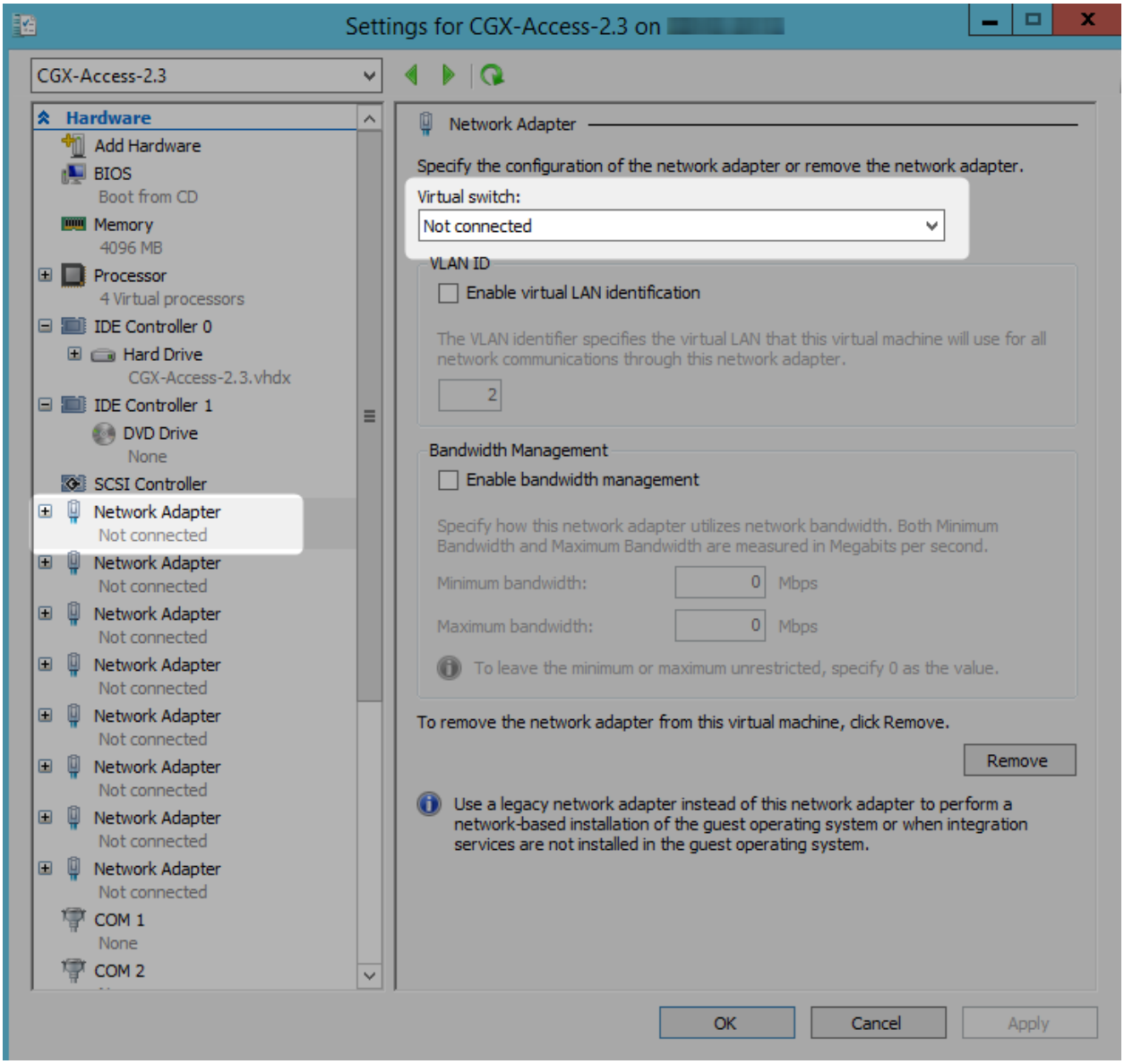



- Select the Virtual Hard Disk destination folder in the next screen.




- 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-2.4’ 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.

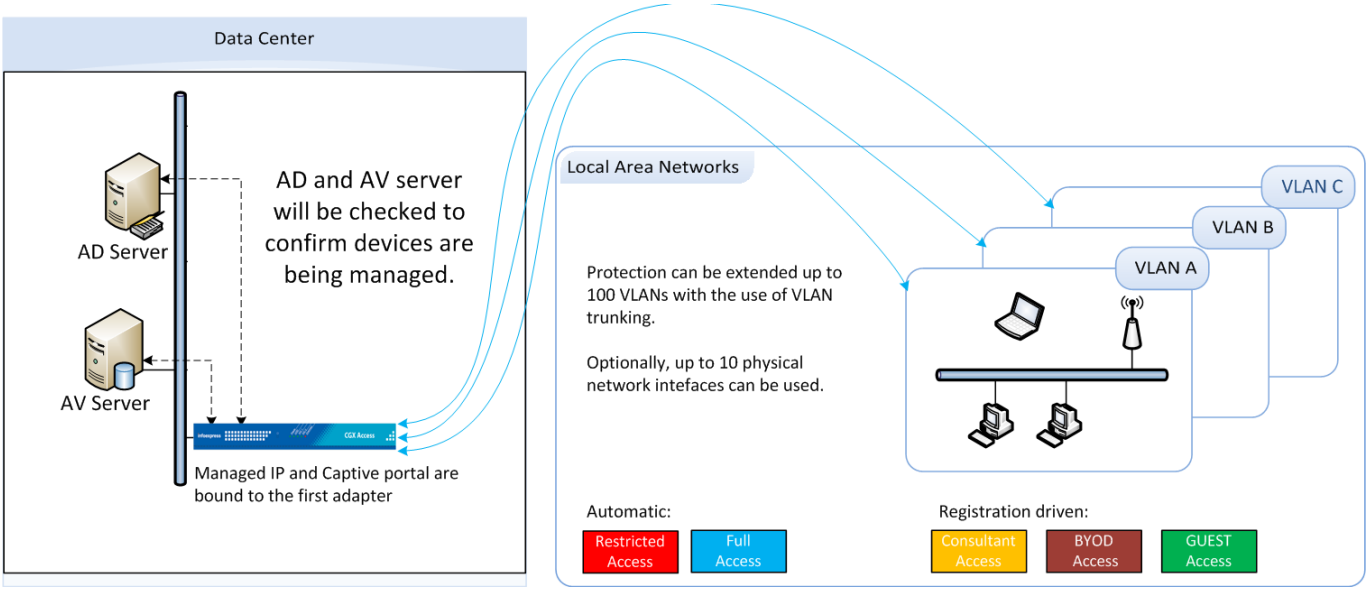


# Configuring CGX Access

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 protects 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 deployments or testing, the Managed IP should therefore 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 require 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 dynamic.

**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:**

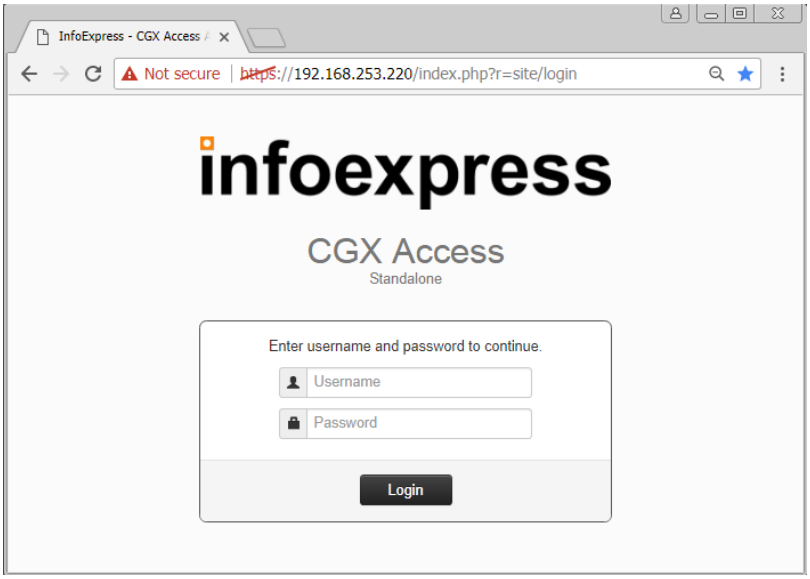
- admin - used for initial setup and configuration as well as ssh access for maintenance tasks
- cguser - used for uploading files through ftp

  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). Compatible browsers include:

  - Internet Explorer 9 or higher
  - Firefox v27 or higher
  - Chrome Version 22 or higher
  - Safari v7 or higher

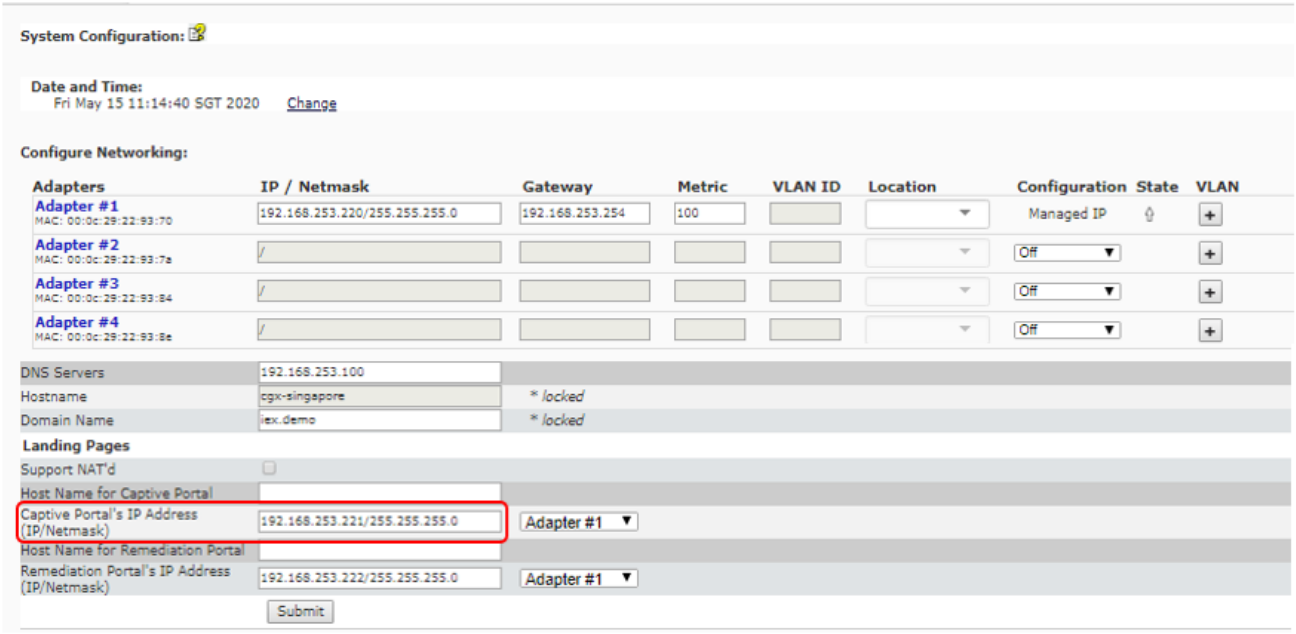


- Login as user admin (default password admin). A modern browser such as Chrome is strongly recommended. Older versions of IE or Firefox may not display the pages correctly.

## Captive Portal IP Address

A separate IP address will be used for the Captive Portal \ Landing pages. To configure this IP address…

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




- Click Submit button

## Remediation Portal IP Address

An additional static IP and 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. The redirection can be enabled via the ACL's.

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

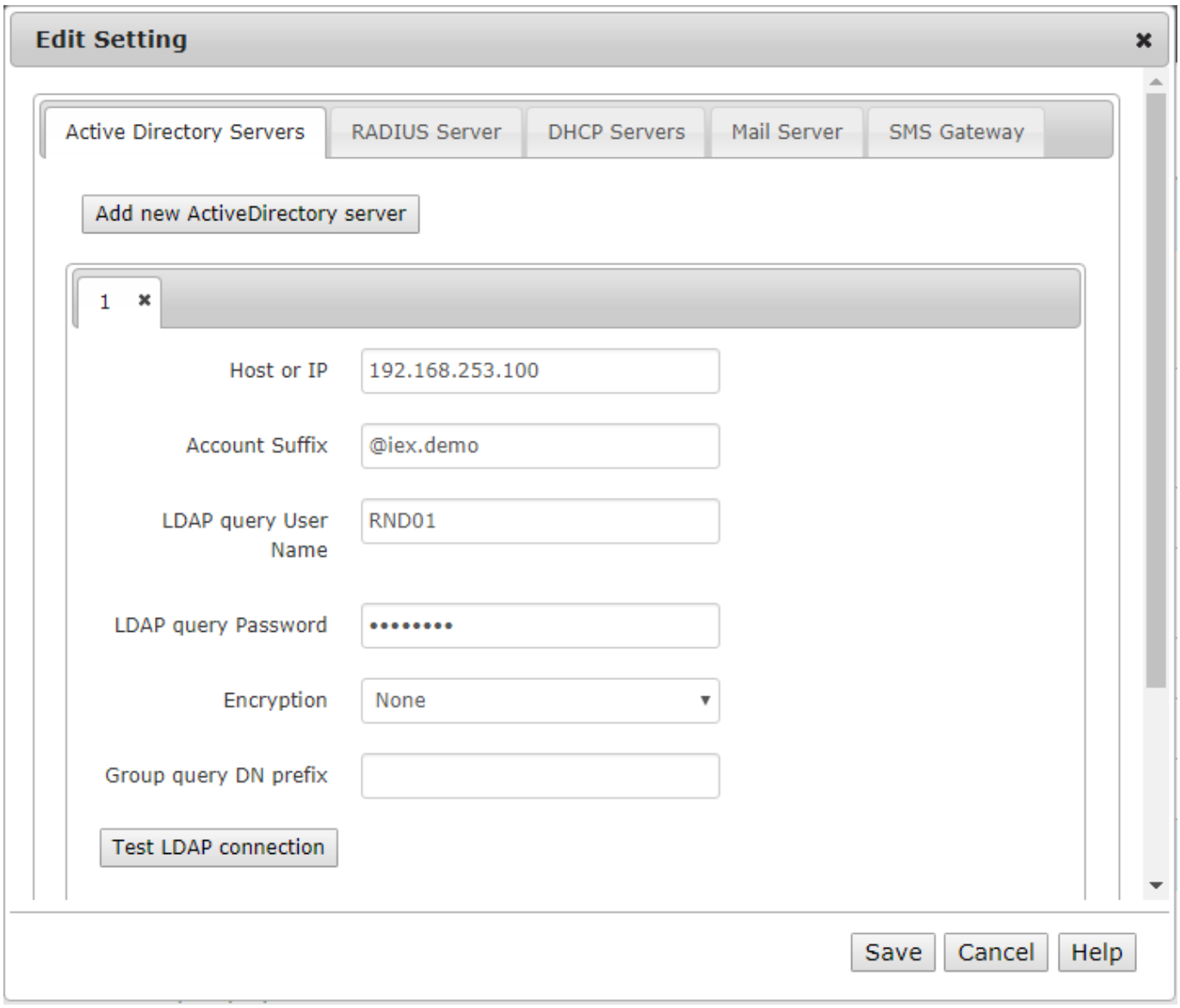
## Connecting to Active Directory

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 Servers:




- 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.

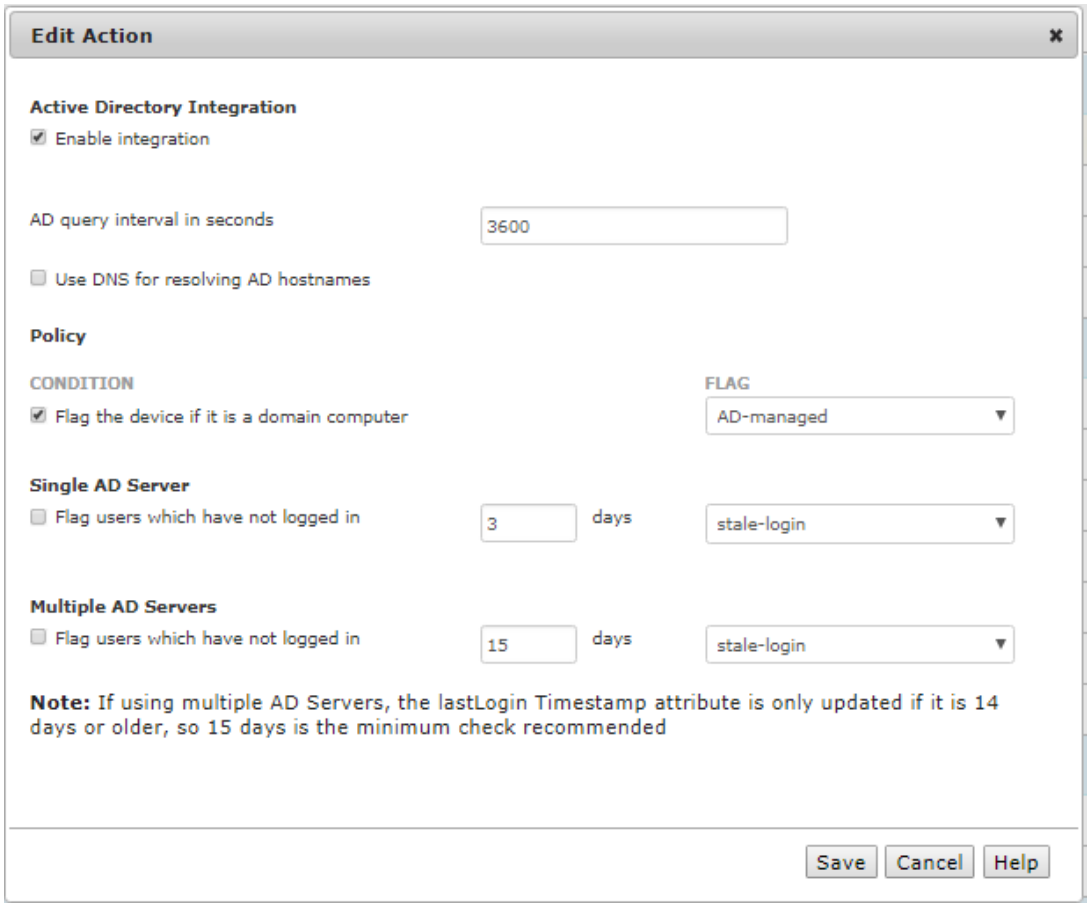
- Use the “Test LDAP connection” button to test the settings

  **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 flagged as AD-managed, and automatically granted full access to the network.

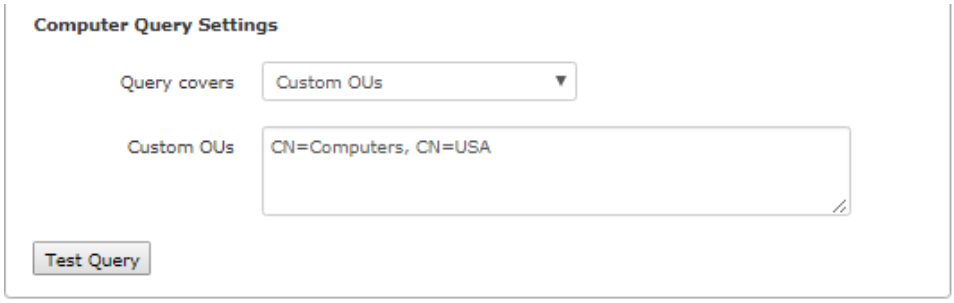
- In CGX Access GUI go to Configuration → Integration
- Click on Active Directory Integration




- Check "Enable Integration"
- Check "Flag device if is AD-managed"
- DNS can sometimes be useful to increase the number of devices flagged as AD-managed. However, if DNS information is stale, it can lead to false positives.

**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

For Example, 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, CN=USA



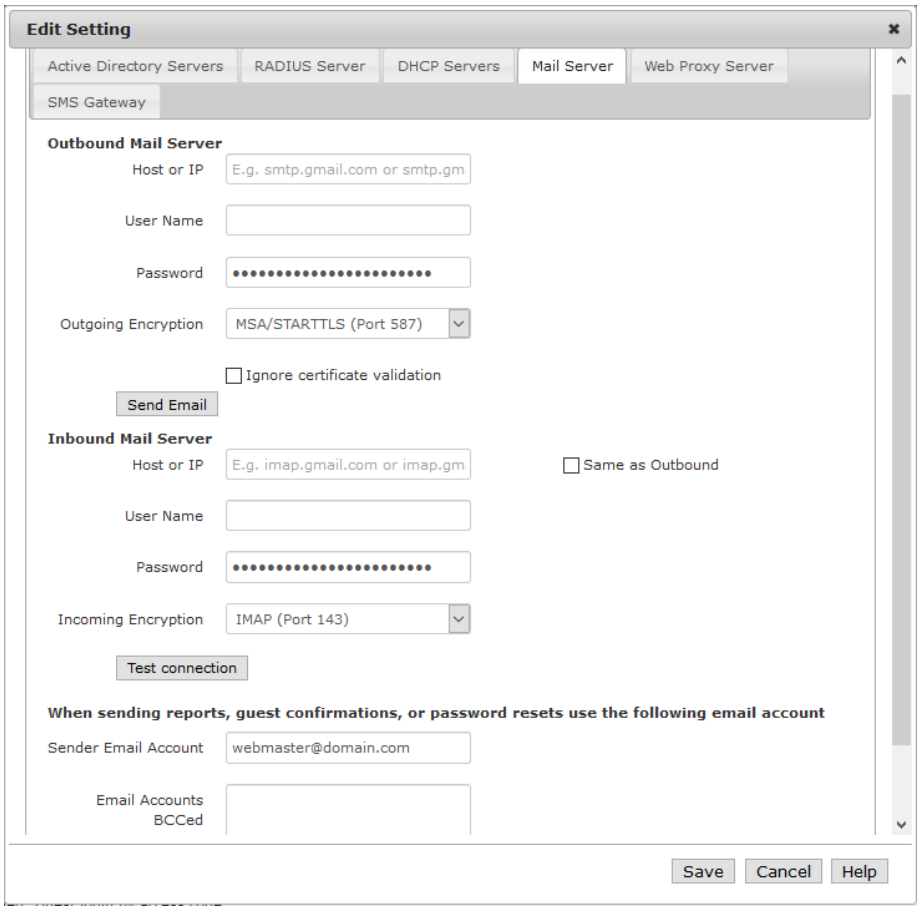

**Tip:** It may be easier to set the Query to cover the Entire Directory.

## Configuring Email and SMS Servers

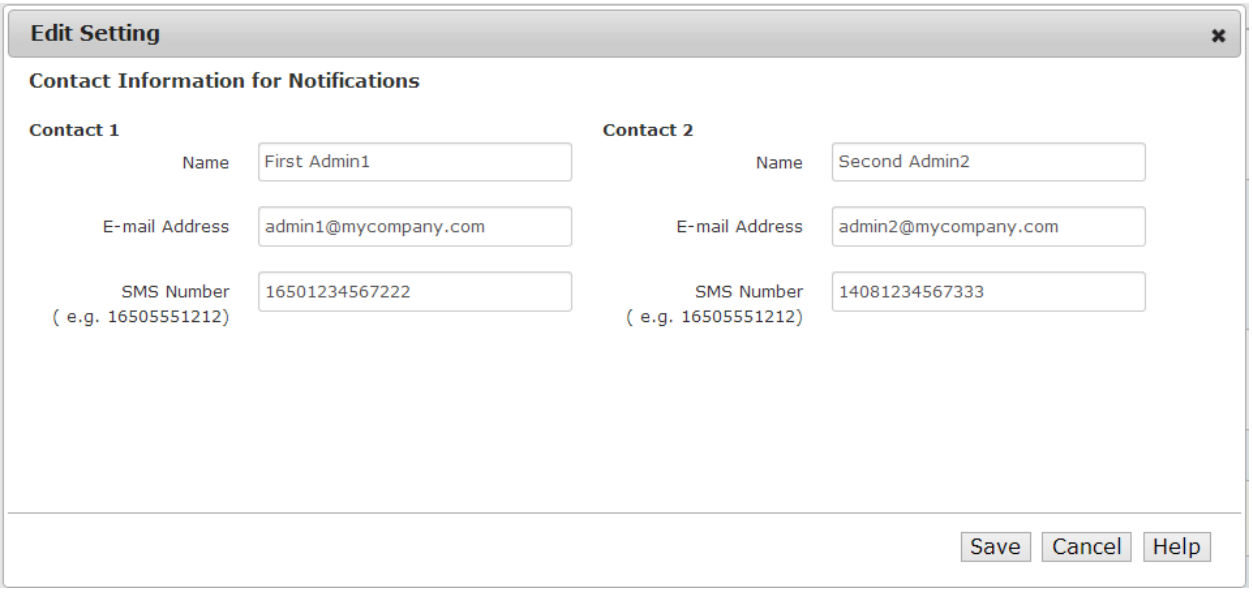
CGX Access can send notification emails and SMS messages when certain events occur. These event triggers are configured with device classifications and monitoring rules (covered in another section), or for guest registration.

To configure the email and SMS servers used by CGX Access:

- Go to Configuration → General Settings and click on the "Servers" section.
- Select appropriate tab

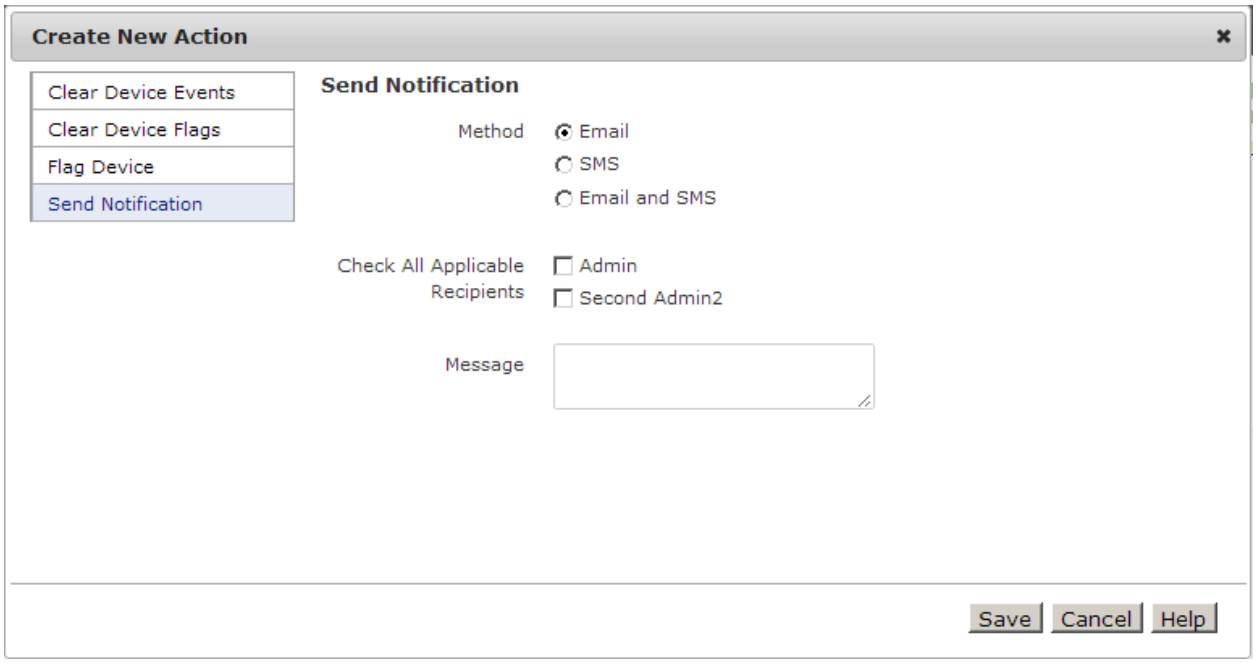


- Enter the needed information and click 'Save'.
- The Inbound Mail Server is for use with Orchestration integrations with E-mail
- Enter an email address used as sender address and optionally one or more addresses that will be Bcc'd on guest registration emails
- Go to Configuration → General Settings and click on the "Contact Information for Notifications" section.




- Fill in the info for at least one administrative contact that should get notified when triggering conditions occur

Notifications can be configured and triggered using Device Classification policies, Monitoring policies, or Device Profiling policies. Different actions are available when a condition is detected:



# Protecting Additional Subnets

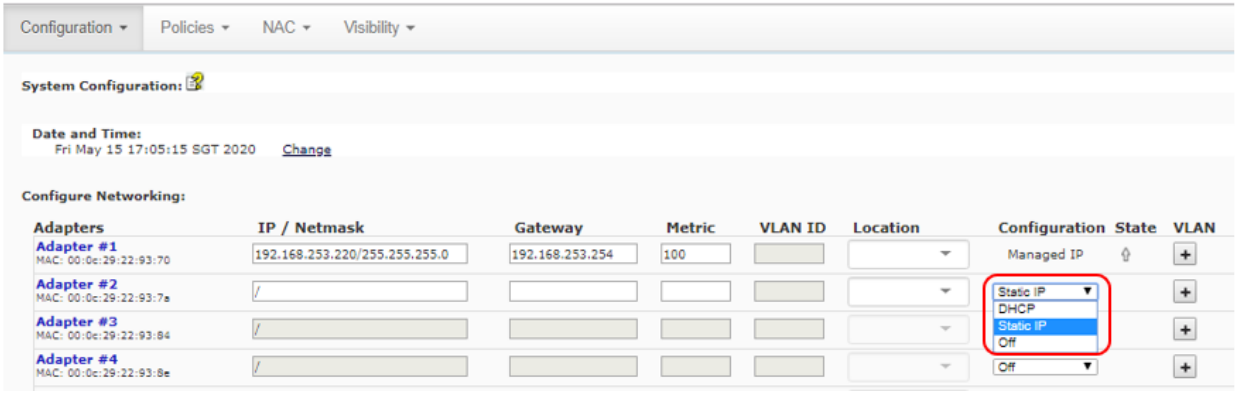
With the use of ARP enforcement, CGX Access requires layer-2 visibility of ARP broadcast traffic to detect and restrict devices. There are two methods that can be used to extend visibility to multiple subnets.

- **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.

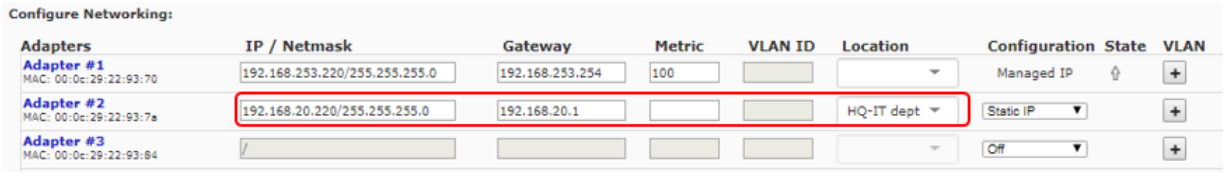
## Adding Network Adapters

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

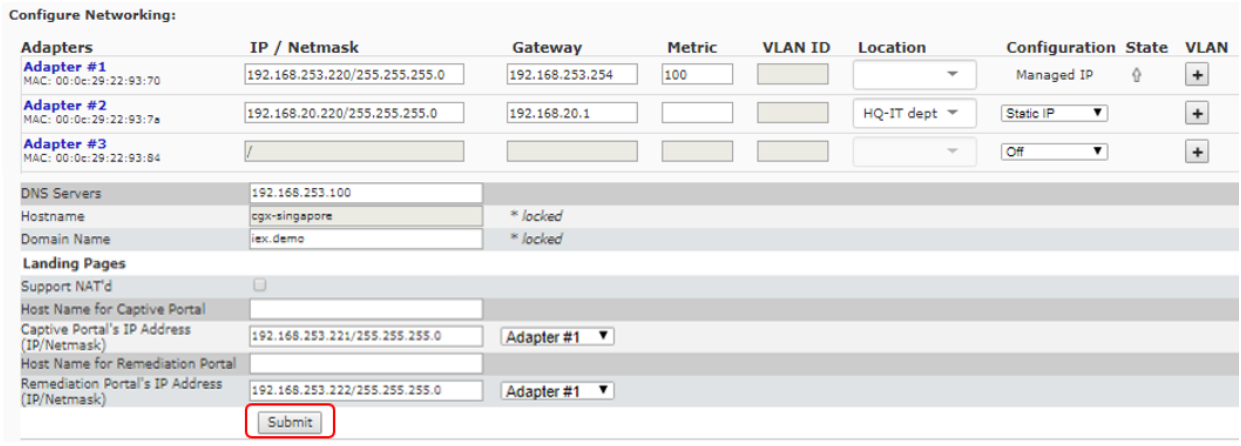
- In CGX Access GUI go to Configuration → Appliance Settings
- Select the method the IP address will be assigned to the adapter




- Complete IP address information if a static IP address will be used. DHCP can also be used.
- Metric field can be left blank (typically not required)
- Location is optional, and can be used in policies




- To confirm the network changes, click the Submit button



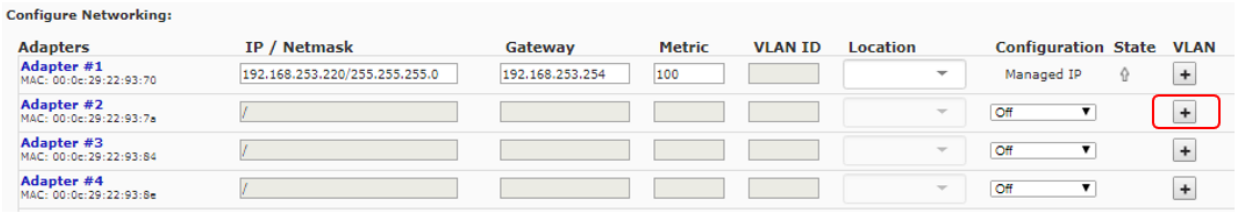

**Note:** When adding adapters to the CGX Access virtual appliance, the adapter must first be provisioned within the VMware host and then connected to the virtual appliance.

## Using 802.1q trunk ports

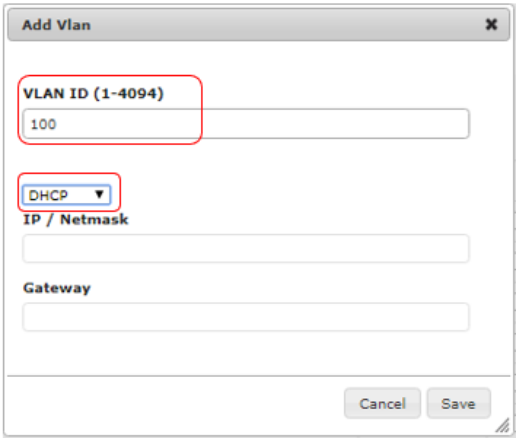
If the network is configured to support VLAN tagging, then adding additional VLANs is simple.

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

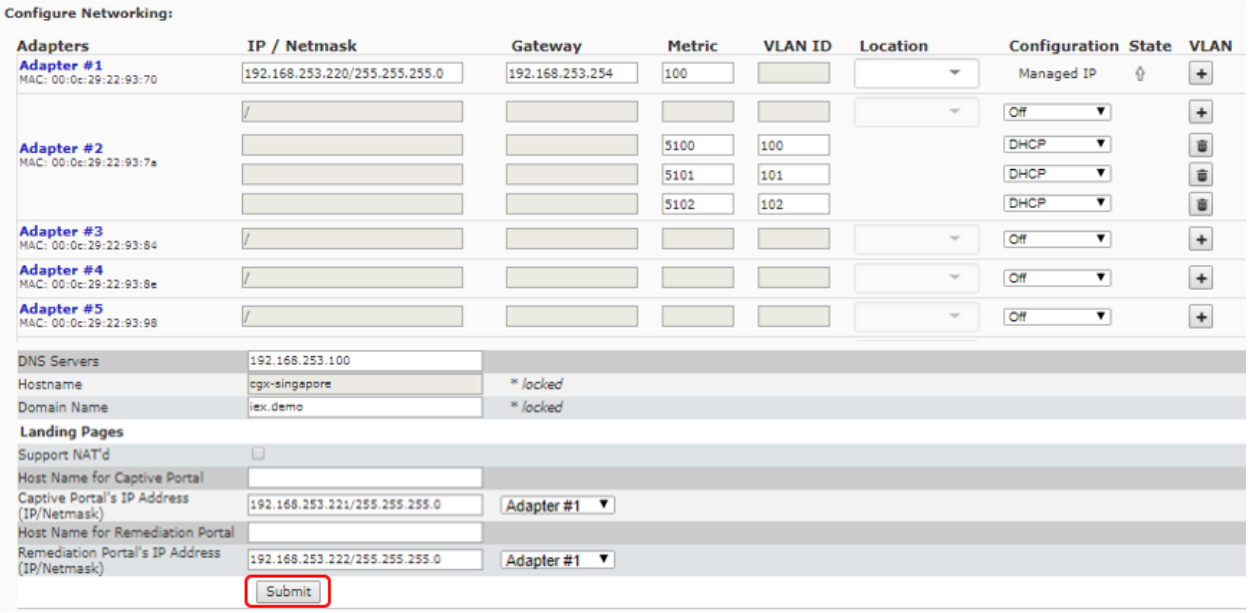
- In CGX Access GUI go to Configuration → Appliance Settings
- Click "+" button on the adapter attached to a trunk port




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



- To confirm the network changes, click the Submit button…

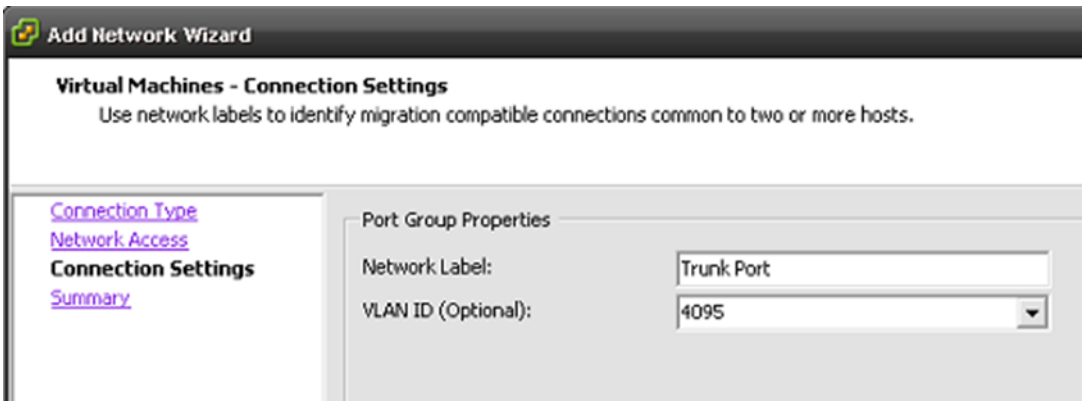



**Note:** One or more adapters connected to the CGX Access appliance must be attached to a switch port(s) configured as a trunk port.

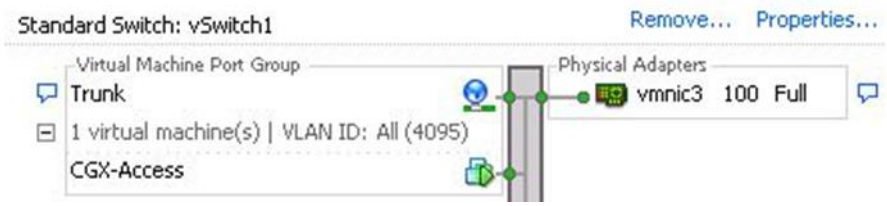
## Additional 802.1q configuration in VMware ESX / ESXi

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 follows 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:

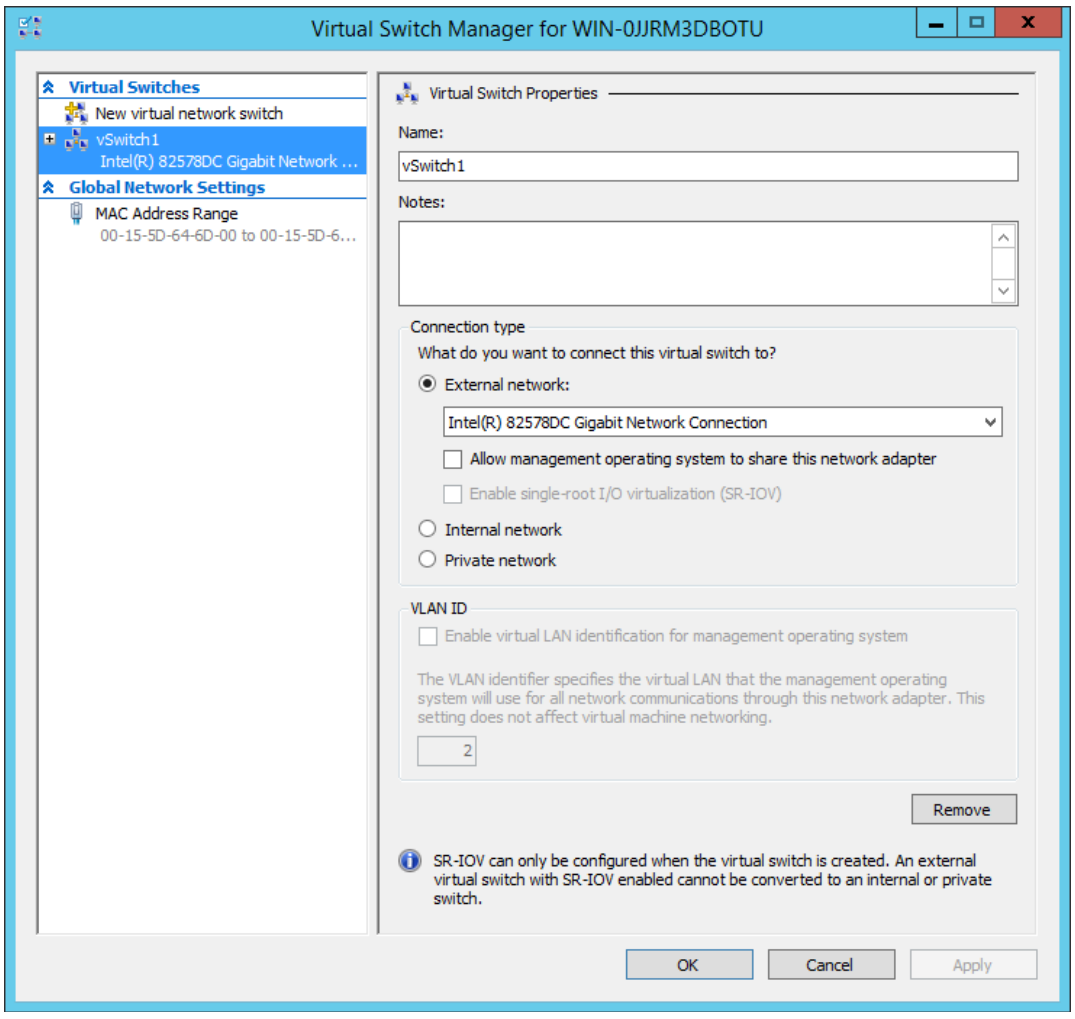



The physical network adapter would be required to connect to the trunk port on the physical networking switch.

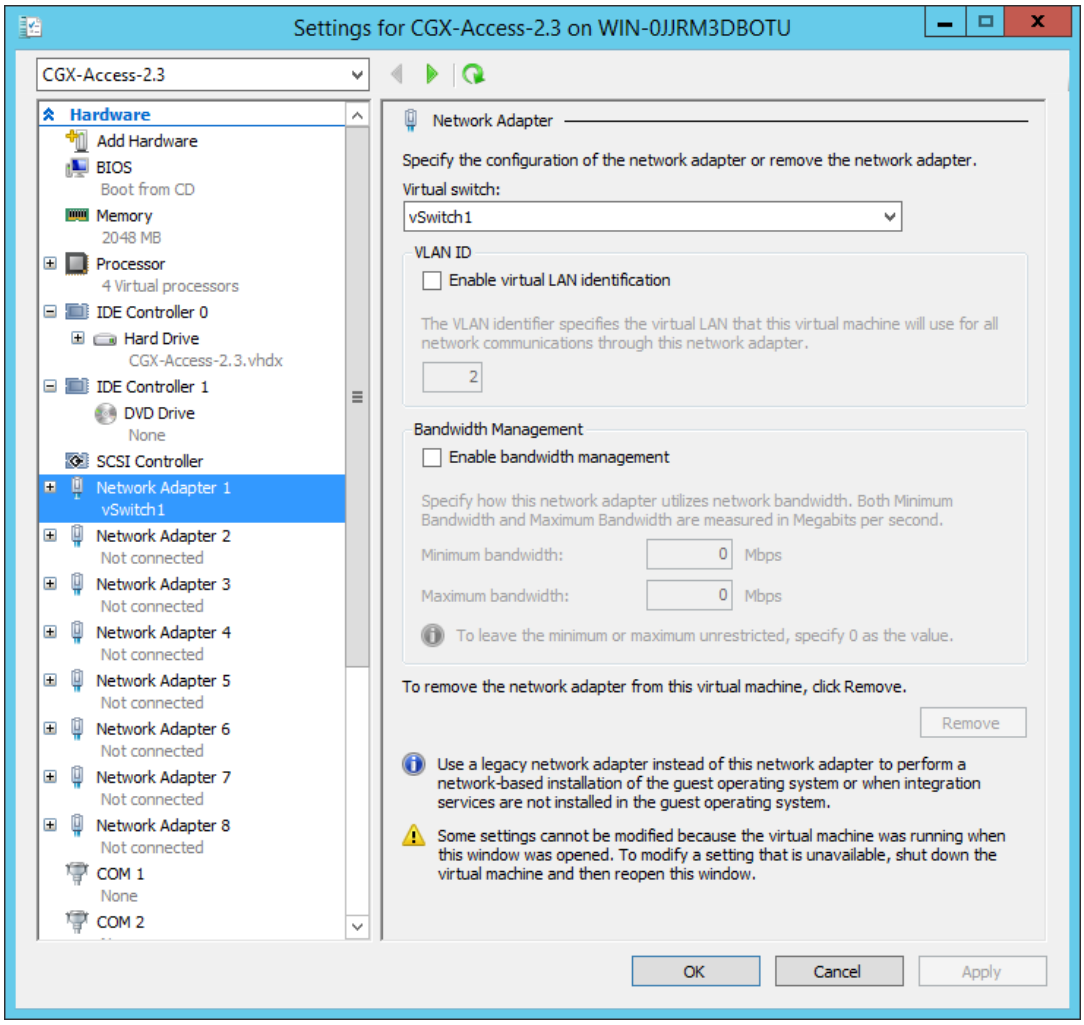
## Additional 802.1q configuration in Hyper-V server

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-2.3 (or vmname) and from right hand pane, click on settings. Assign virtual switch to the network adapter on CGX Access.

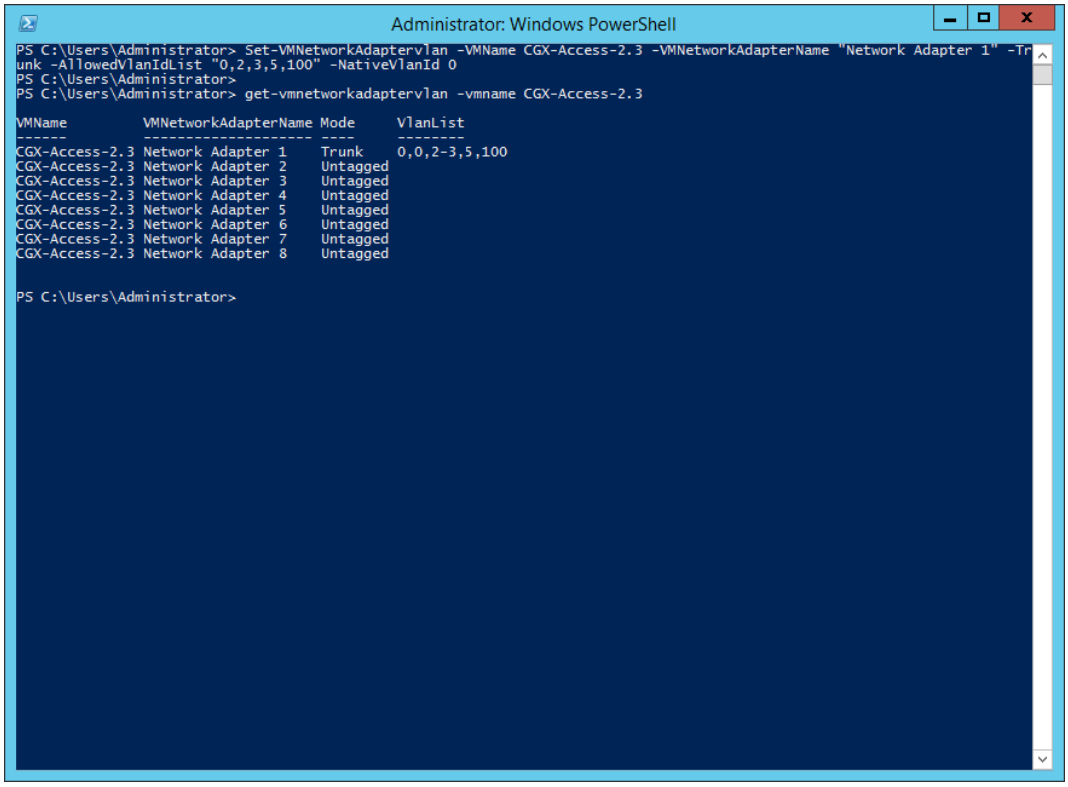



- Start Windows PowerShell and enter following command to configure “Network Adapter 1” as trunk port with allowed vlans 0,2,3,5,100 and Native Vlan as 0 (1 on cisco)

*Set-VMNetworkAdaptervlan -VMName CGX-Access-2.3 -VMNetworkAdapterName "Network Adapter 1" -Trunk -AllowedVlanIdList "0,2,3,5,100" -NativeVlanId 0*

- To verify enter following command.

*Get-VMNetworkAdaptervlan -VMName CGX-Access-2.3*

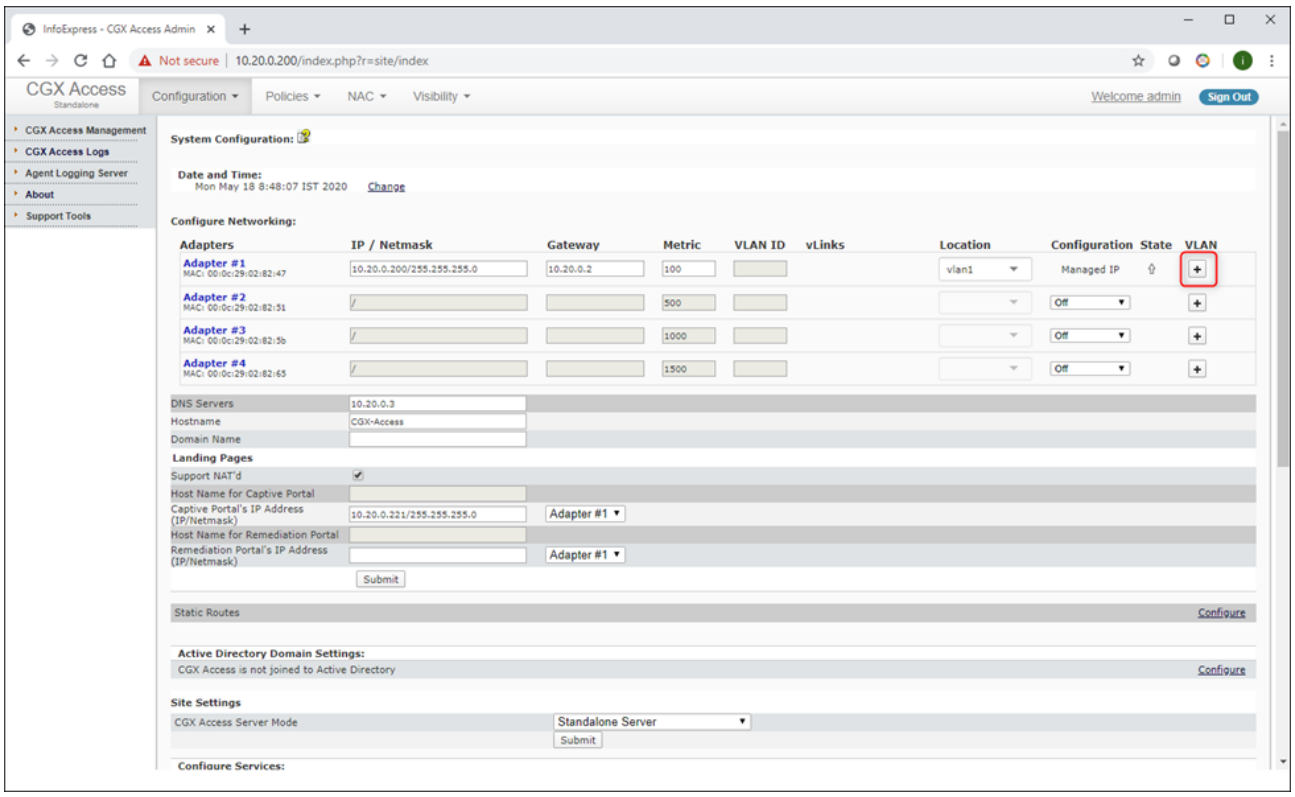



**Configuration required on Switch port.** ***(cisco switch configuration used in example)***

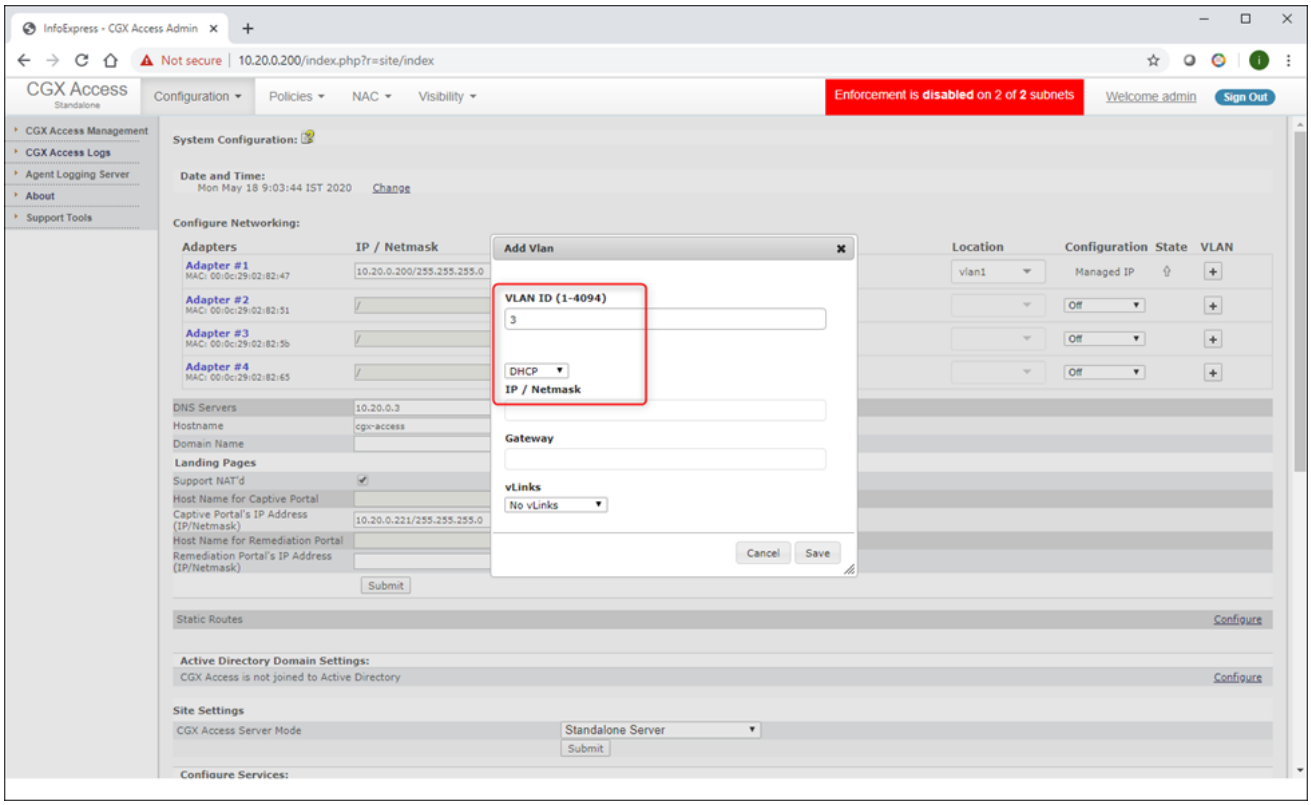
In this example, we will allow vlans 2,3,5,100 with native vlan 1 *(Cisco vlan1 = HyperV-vlan0)*
**Switch#**configure terminal
**Switch(config)#**interface fastEthernet 0/3
**Switch(config-if)#**switchport trunk encapsulation dot1q
**Switch(config-if)#**switchport mode trunk
**Switch(config-if)#**switchport 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**

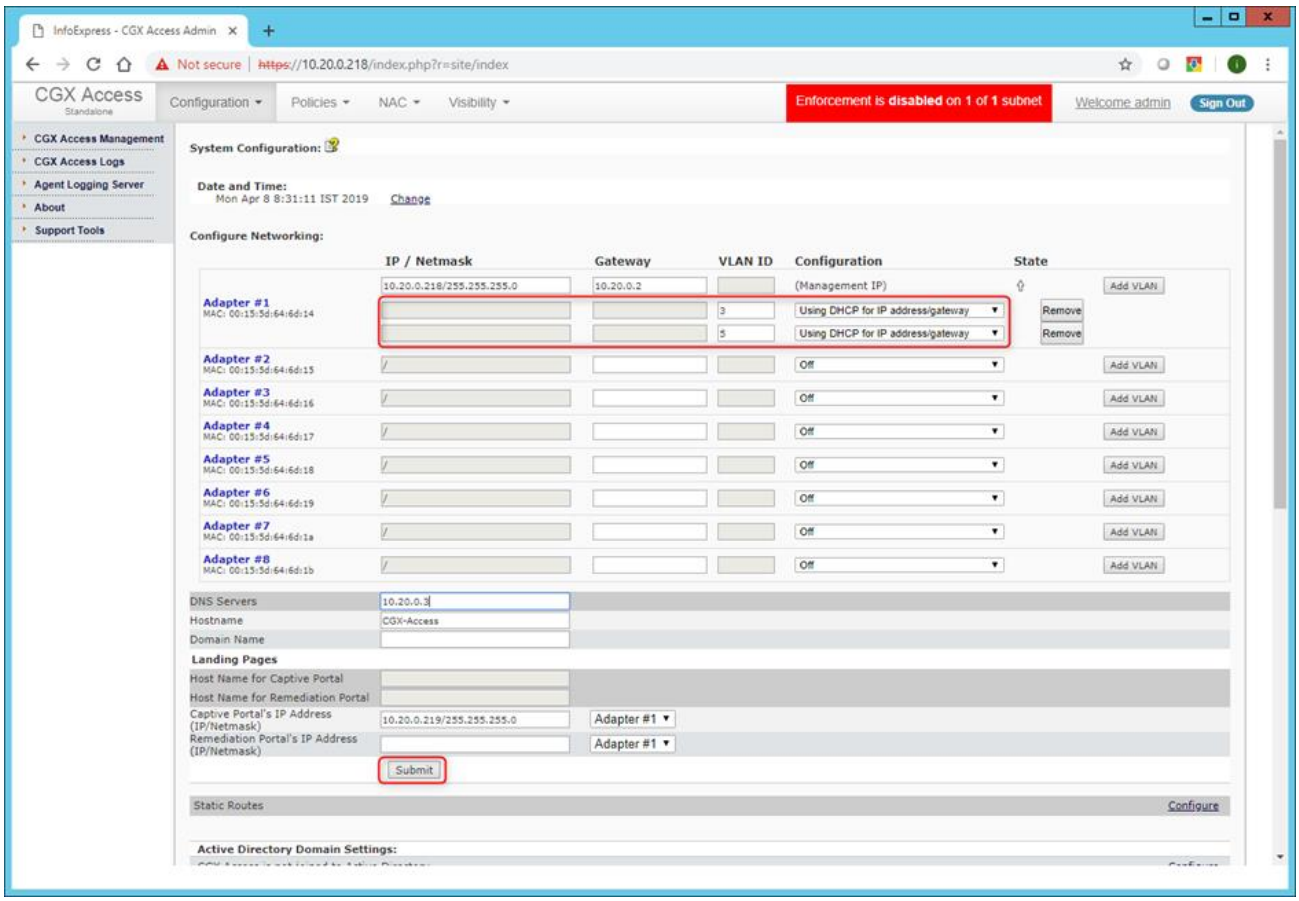
- Start CGX Access VM
- In CGX Access GUI go to Configuration → Appliance Settings
- Click "Add VLAN" button on the adapter attached to a trunk port



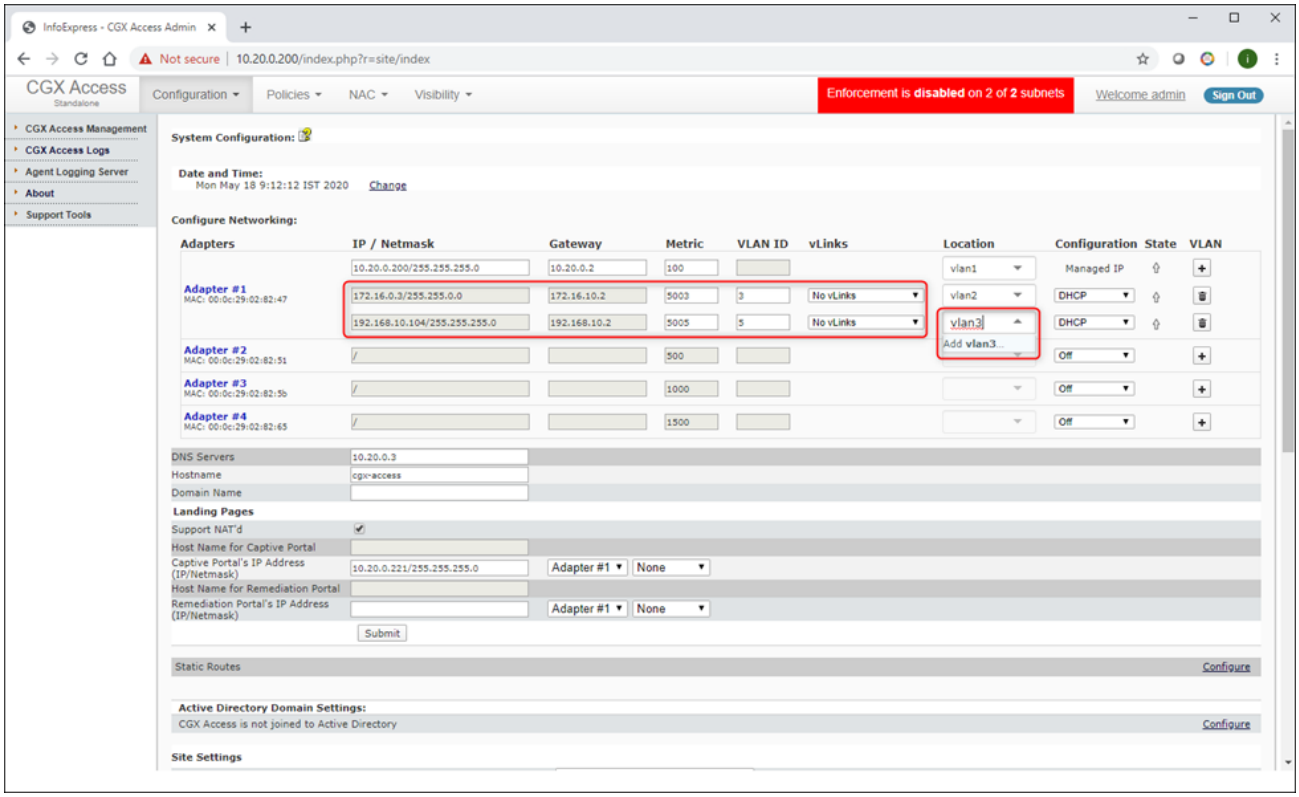

- Complete VLAN ID and IP address information. Static IP addresses or DHCP can be used.




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



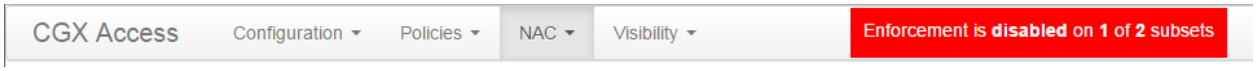

- If DHCP is configured, you should see IP address assignments to Vlan NICs



# Enforcement Overview

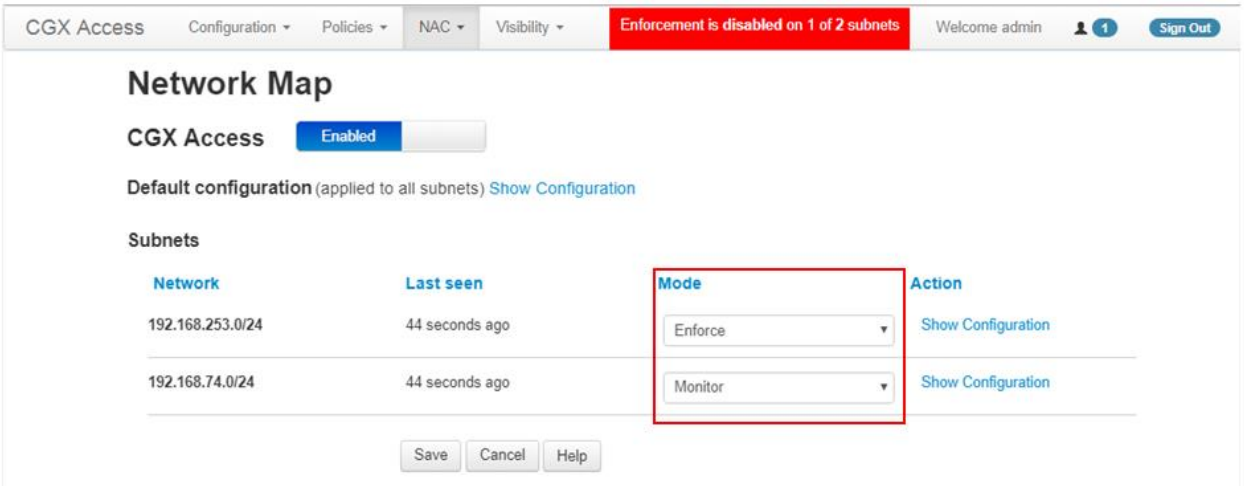
CGX Access uses ARP enforcement to restrict access with landing page redirection. The use of ARP enforcement greatly simplifies the deployment of CGX Access, as no network changes are required. ARP enforcement is also used to provide role-based control. To provide role-based control, CGX Access supports Access Groups, such as: restricted, limited, full-access, guest-access, consultant, and byod-access, etc. Each access group will have a configurable ACL to allow for the role-base 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 white 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 NAC → 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 NAC → Network Map
- Find the desired subnet and click on the "Show Configuration" link

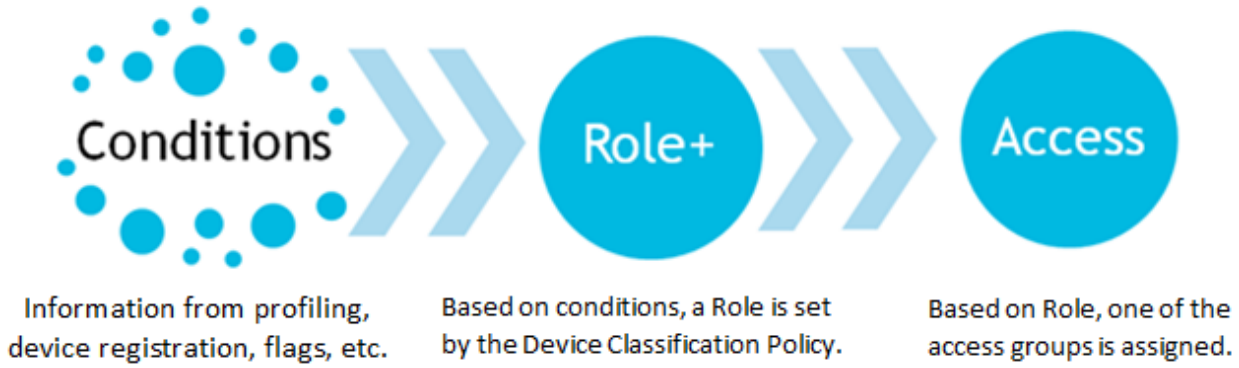
# Configuring Access Policies

CGX Access includes default Access Groups. Customized Access Groups 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-FB – Provides access to Facebook while restricted to enable Guest Access authentication using Facebook credentials.
8. Restrict-Azure - Provides access to Microsoft while restricted to enable BYOD authentication using MS Azure credentials.
9. Restrict-Agent – Restricts a device failing an agent audit to remediation resources only

Each access group has a customizable ACL associated with it. Every device joining a protected subnet will be assigned an access group. 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 Device Classification Policy so a role can be assigned. Second, roles are then assigned one of the six access groups.

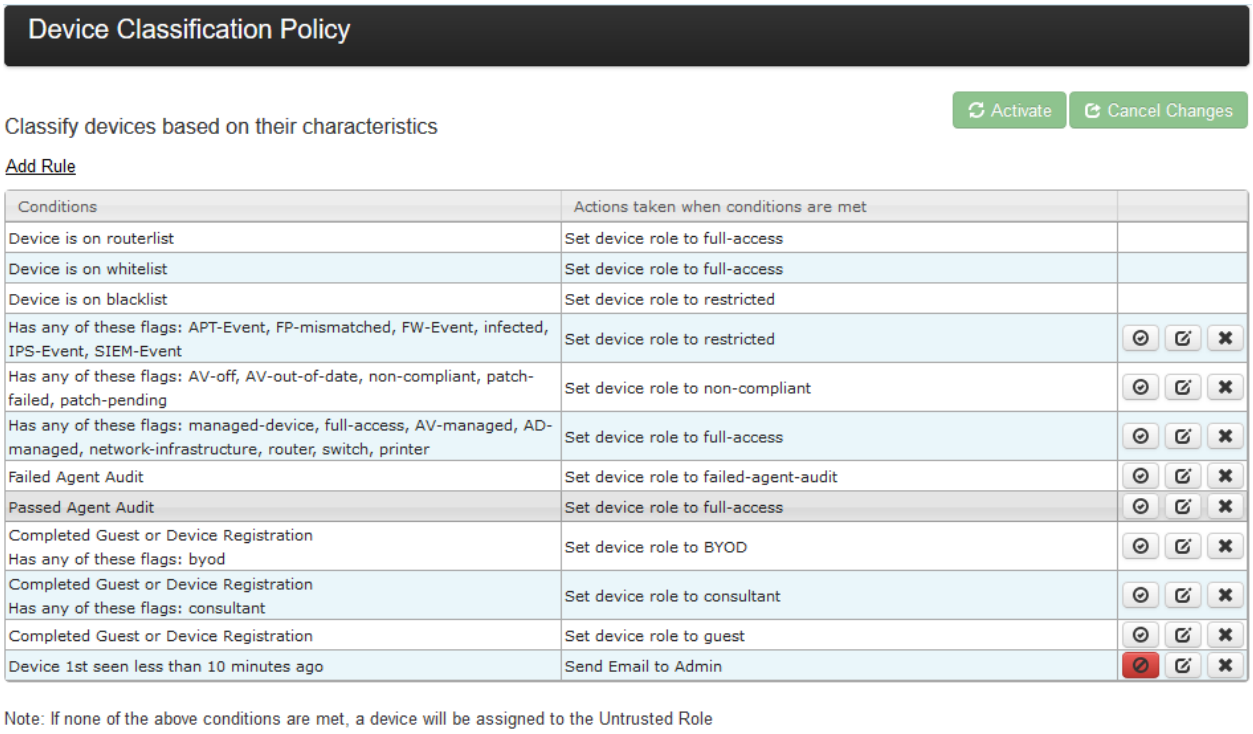



## Device Classification Policies

In CGX Access GUI:

- Go to Policies → Device & Role Classification.

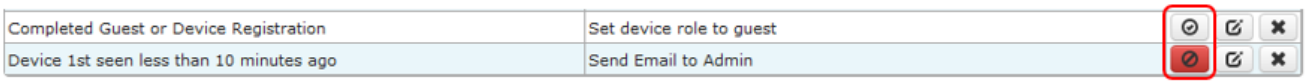
CGX Access has a set of preconfigured device classification rules which will address typical requirements but can be modified to suit unique needs.




The classification rules are evaluated top-down. The device role is assigned by the first rule with matching conditions. Other allowable actions such as sending a notification will be executed by all rules that have matching conditions.

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.



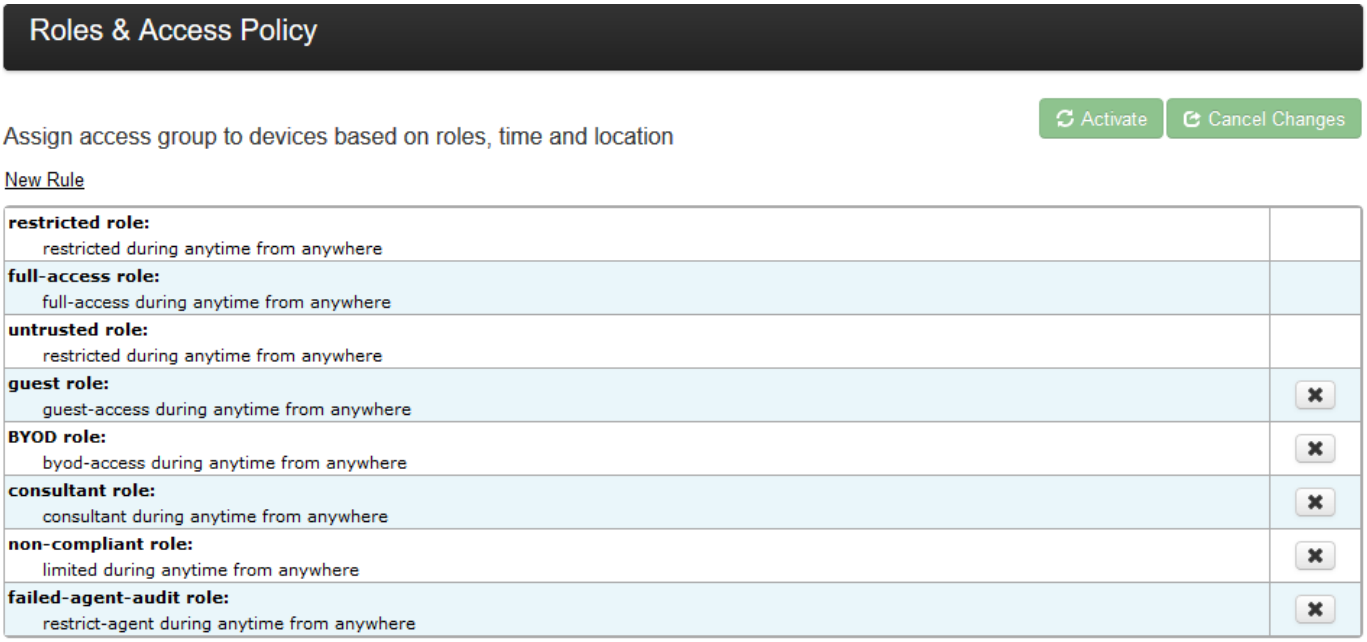

If changes are made, click the “Activate” button for the changes to take effect. 


## Roles & Access Policy

In CGX Access GUI:

- Go to Policies → Roles & Access

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




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 up multiple roles even if these different roles get the same access group.

It is also possible to set time and locations when access groups 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

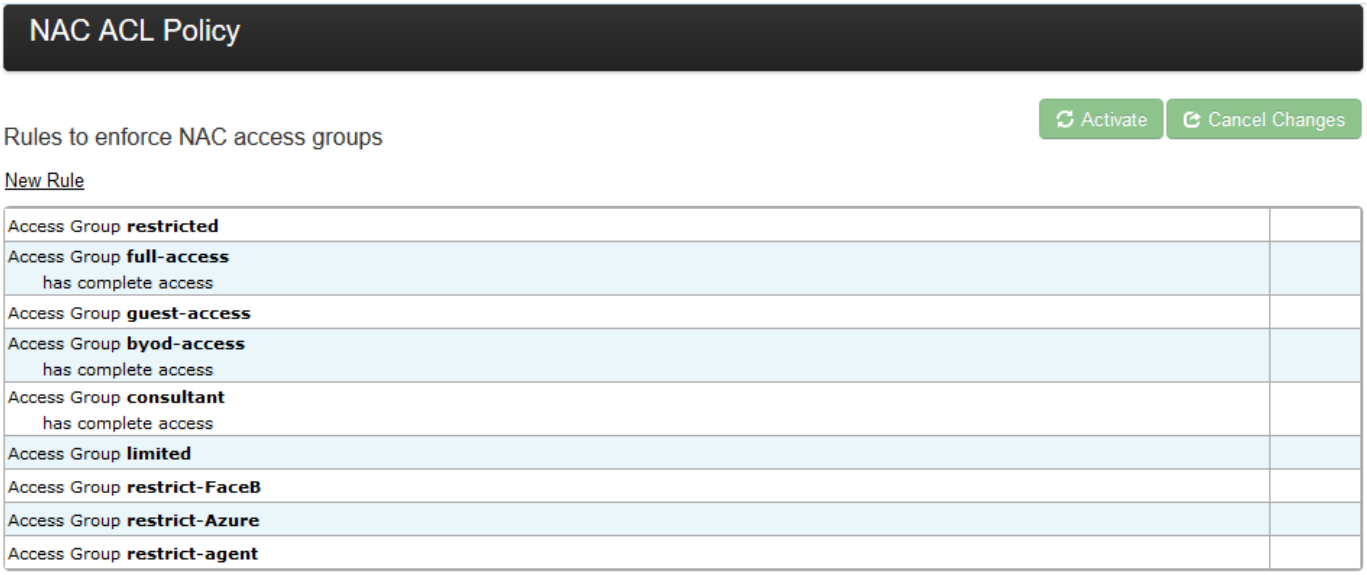
If changes are made, click the "Activate" button for the changes to take effect. 

## Access Control Lists

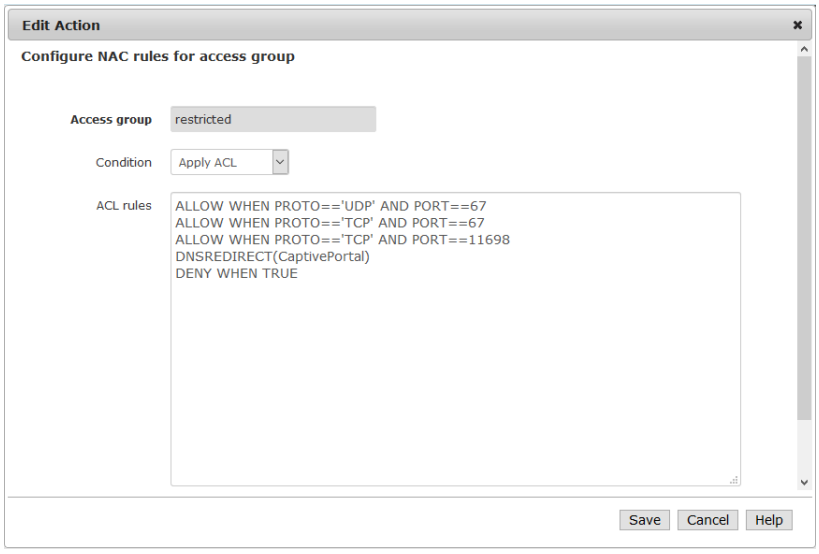
Each of the access groups has a customizable ACL that is associated with it.

In CGX Access GUI:

- Go to NAC → ACLs




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.




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 landing page. 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("facebook.com")
This command allows both DNS replies and traffic to the Facebook site. It should be placed above the DNSREDIRECT rule

10) ALLOWSUBSITE("facebook.com")
This command allows both DNS replies and traffic to the Facebook 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')

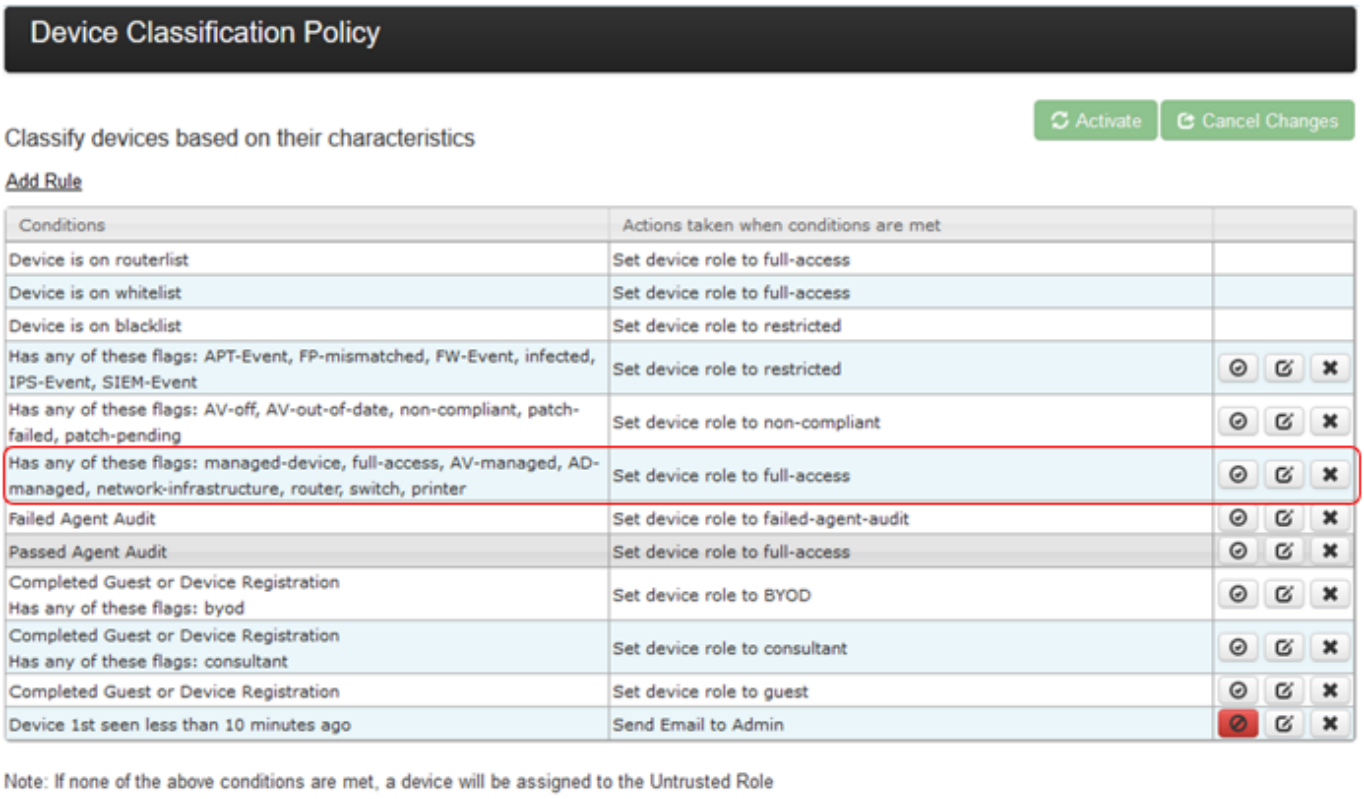
**<addr_or_subnet>** can contain IP-address range, like '192.168.0.1-192.168.0.100'
All strings should be quoted using single-quotes: 'example'

# Flagging Devices and Whitelisting

In NAC deployments, it is a common requirement to grant access (whitelist) 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 Flagging. The CGX Access solution supports the ability for administrators to create and set flags on specific devices. Then using device classification policies, devices with specific flags can be granted full-access, blacklisted or assigned some other access.

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

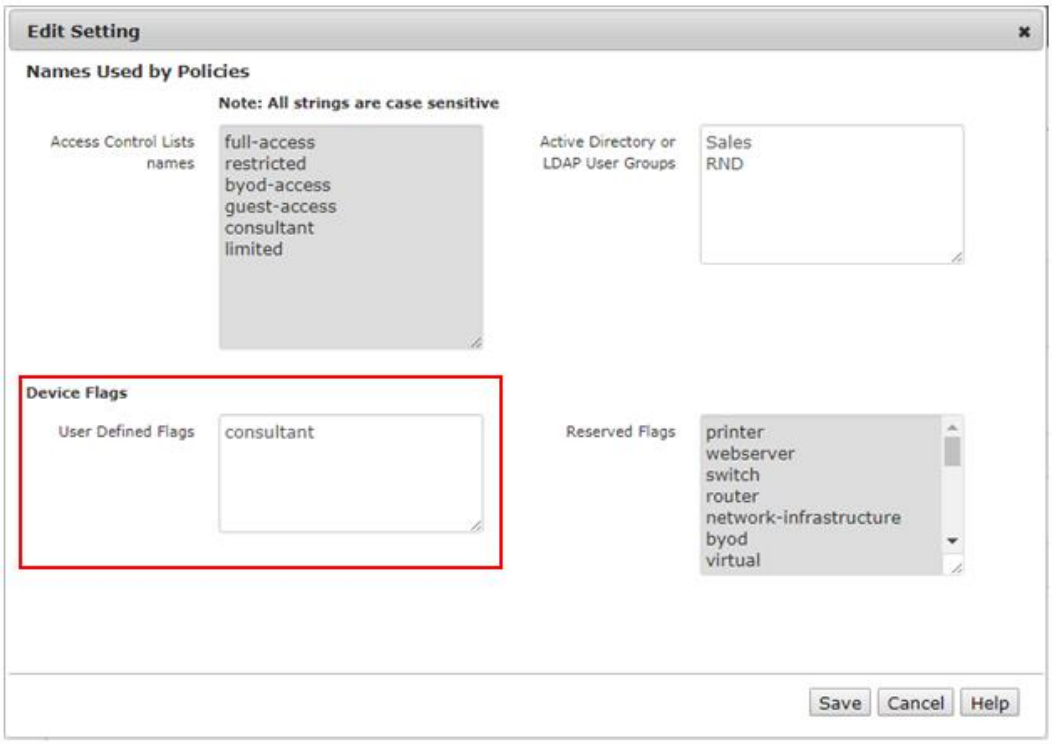



CGX Access automates the process of flagging. The CGX Access solution will automatically flag a device based on the results of device profiling. If CGX detects that a device is a printer, it will flag the device as a printer. If using the default Device Classification Policy, the printer would then be granted full-access. The same is true for network infrastructure like switches and routers.

## Flags

CGX Access supports two types of flags, User Defined Flags and Reserved Flags. User Defined Flags can be created and changed as required. The Reserved Flags are set automatically by the CGX Access device profiling system and cannot be deleted.

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




These two types of flags 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 flagged as a printer shows up on the network. Once the printer has been inspected, the administrator can then assign a User Defined Flag, i.e., approved-printer, which would allow it access to the network.

## Setting Flags

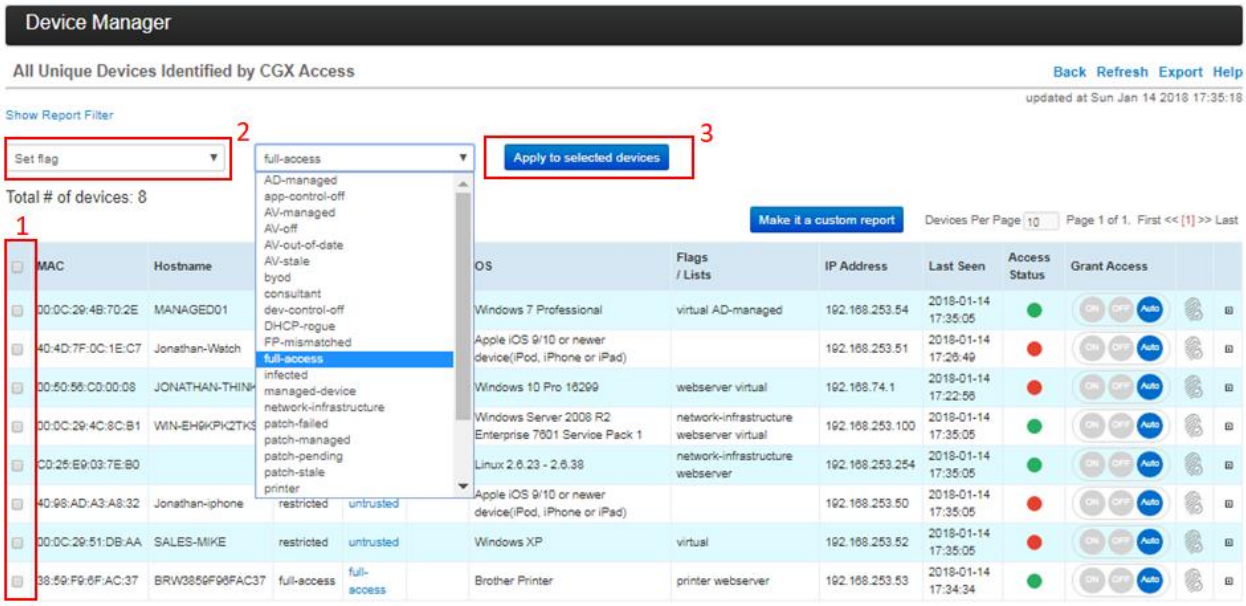
Flags can be manually assigned to devices via the Device Manager.

- 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 flags manually can be done for one or more devices in a few steps.

- 1. Select the device(s) where a flag is desired
- 2. Select the action → Add flag to selected device(s) → Select Flag
- 3. Click Apply to selected devices

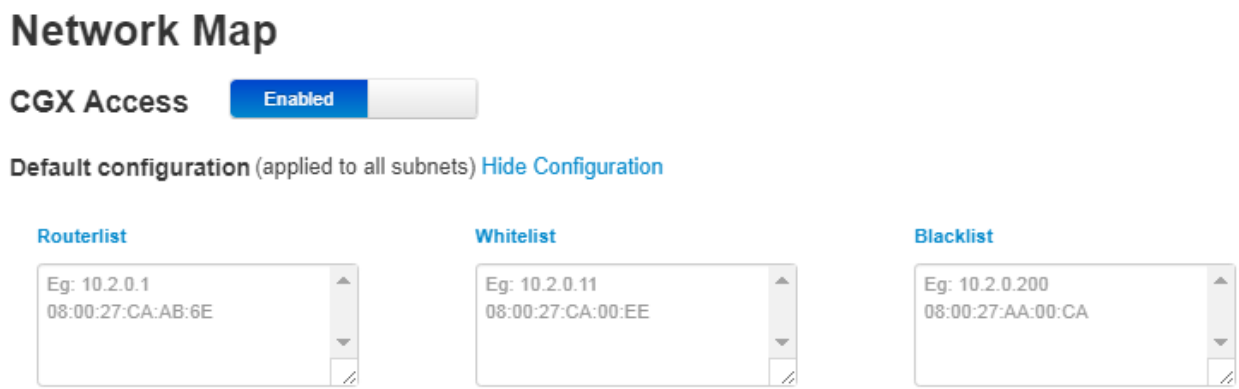



## Whitelisting \ Blacklisting

CGX Access also supports adding a device(s) to a manual whitelist or blacklist. The examples below will assume whitelisting, but blacklisting works the same way.

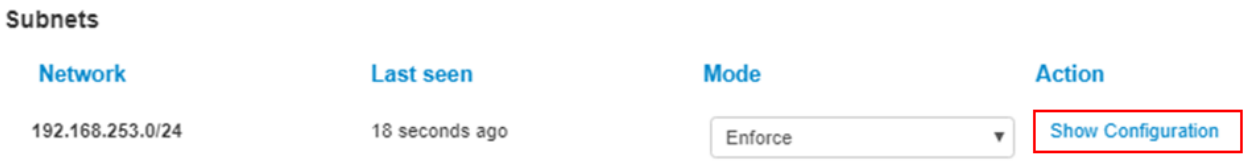
In the Network Map, devices can be added by MAC Address or IP Address to the global whitelist or to a whitelist specific to a subnet. If entered into the Default Configuration, the whitelisting would be configured for all subnets. When adding devices to the Default Configuration, it's best to use MAC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

- Go to NAC → Network Map → Show Configuration

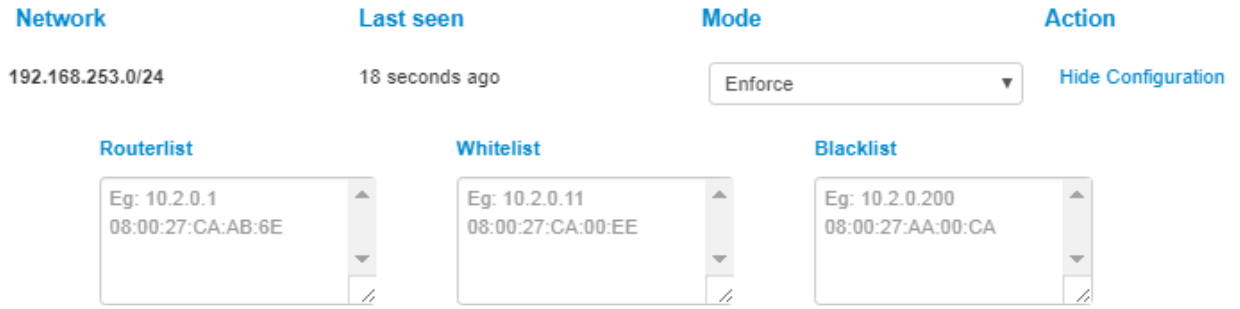



The Network Map can also be used to configure IP addresses or MAC addresses that should only be whitelisted on specific subnets.

- Go to NAC → Network Map
- Find the desired subnet and click on the "Show Configuration" link




Once the "Show Configuration" link has been clicked, the view will expand to show the Whitelist box specific to this subnet. Both IP Addresses and MAC Addresses can be added.

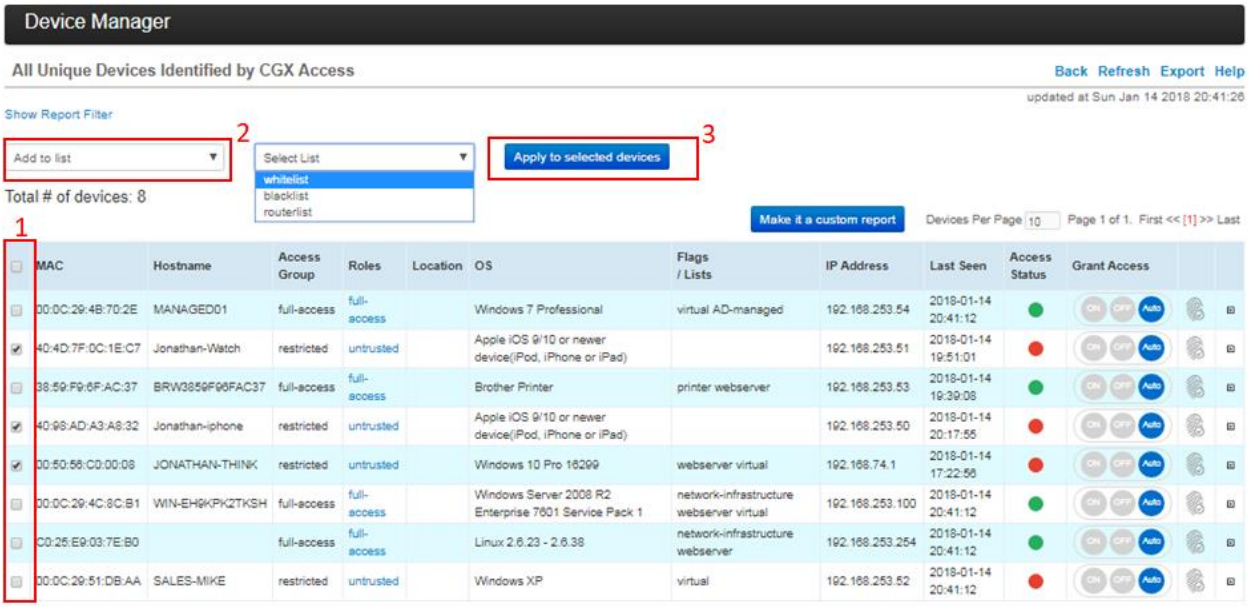



## Adding Devices to the Whitelist or Blacklist

For quick additions to the Whitelist or Blacklist you can click the ON | OFF controls in the Device Manager. ON is the technical equivalent of being on the Whitelist, while OFF is the equivalent of being on the Blacklist. Auto means access is set automatically following the policies defined under Device and Role Classification.


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

- 1. Select the device(s) to be whitelisted
- 2. Select the action → Add to list → Select whitelist
- 3. Click Apply to selected devices




Note: Devices that are in the whitelist will be shown as ON. Devices in the blacklist will be shown as OFF. Their respective list will also be shown in the Flags / Lists column.

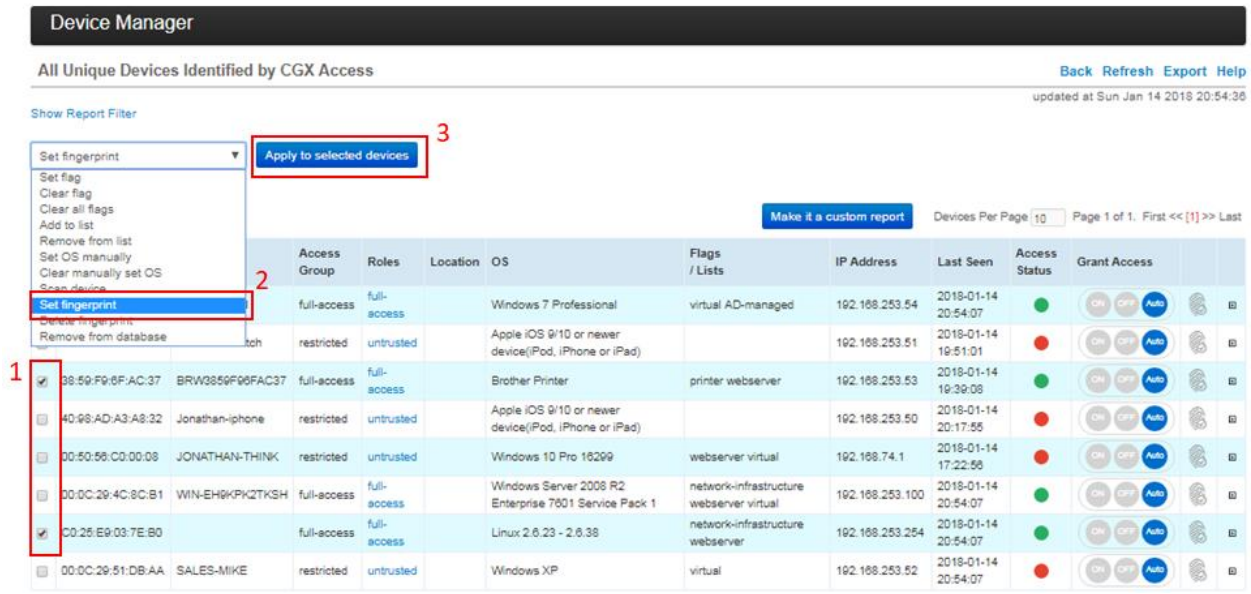
# Anti-spoofing Protection

When using MAC-based authentication on the network, MAC address spoofing can be a concern, as it is easy to change a MAC address. 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, and Hostname). 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 and printer as its OS type. If a Windows, Apple or Linux 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



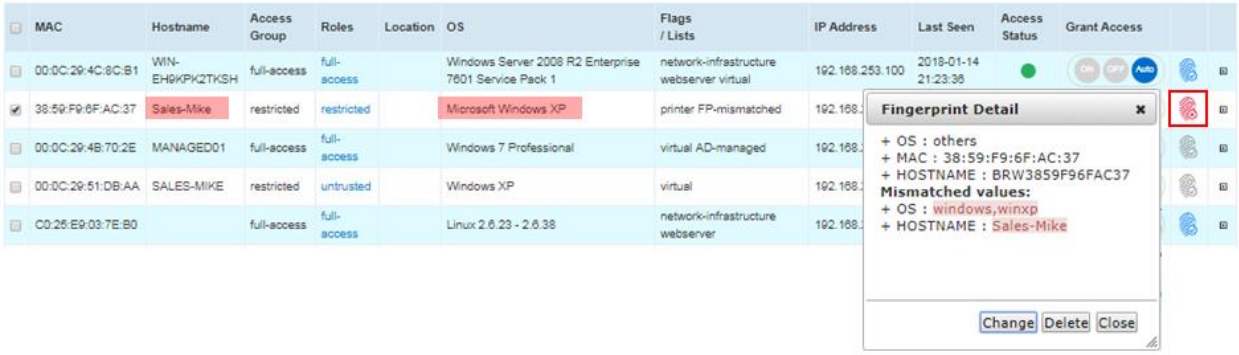

- 4. Confirm details to be included in the fingerprint → Save


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

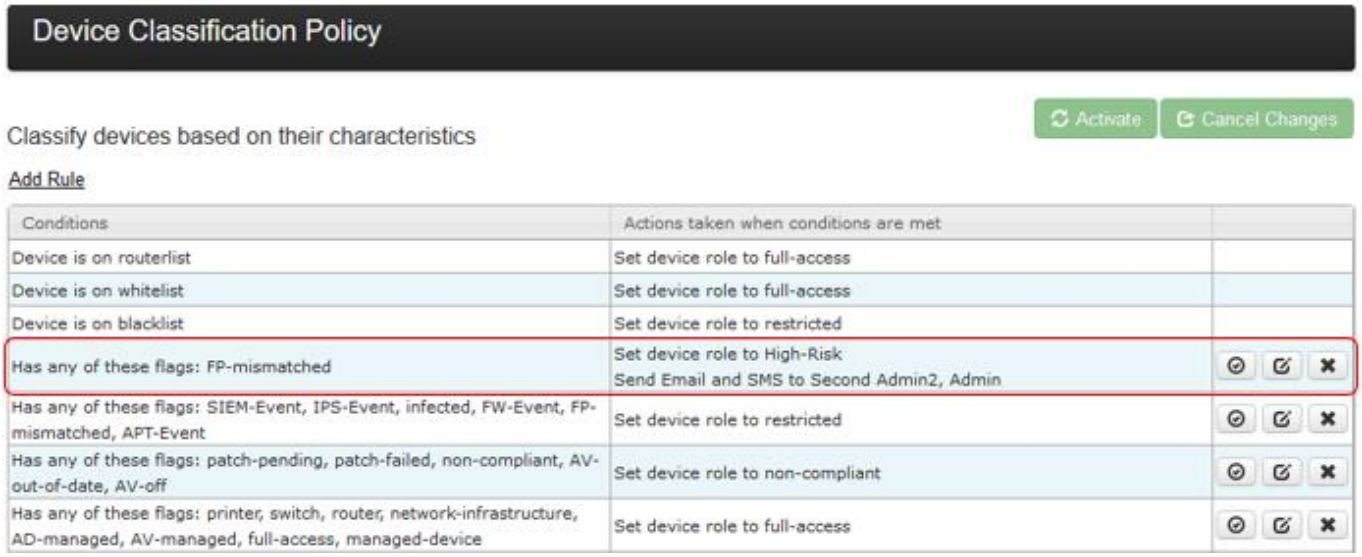

**Tip:** The gray fingerprint icon can be clicked to set quickly set a fingerprint.

## MAC Spoofing Detection

Once a fingerprint has been set, any changes in the fingerprint details will causes 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 host name didn't match the fingerprint. The fingerprint icon was changed to red and device was assigned a FP- mismatched flag so actions can be taken.




Using Policies → Device & Role Classification rules, actions can be taken when a FP-mismatched is detected. The policy below shows the device will be assigned a restricted role and alerts will be sent to the network administrators.

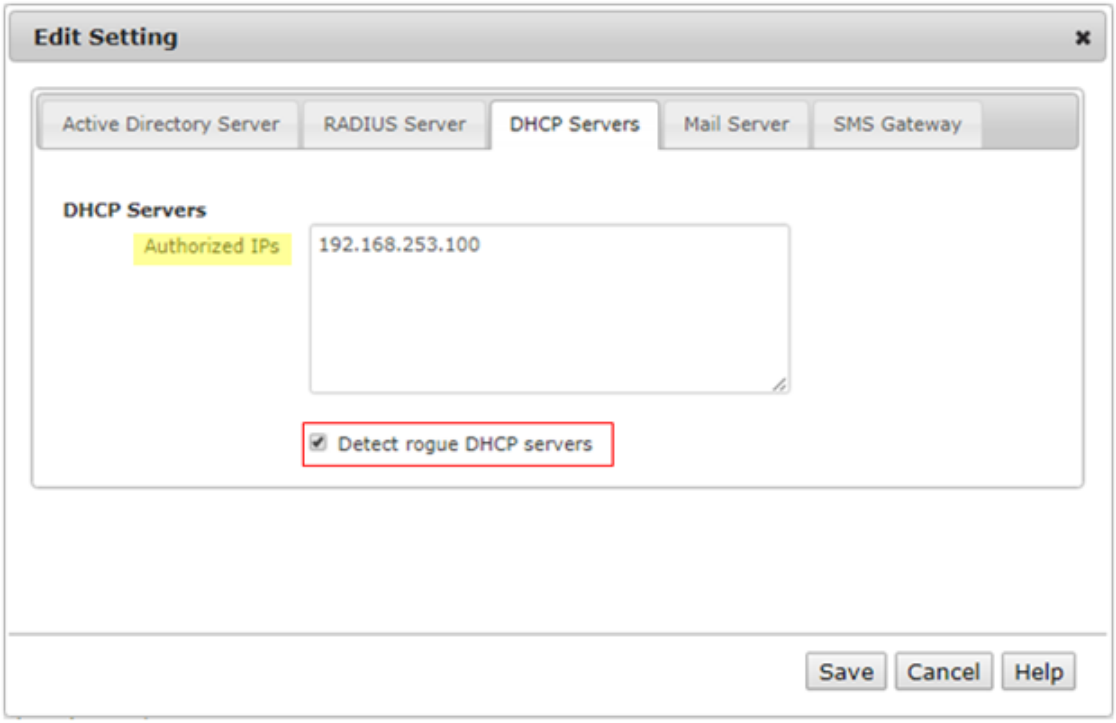



**Tip:** The Fingerprint feature can be used in static IP environments to lock the IP \ MAC combinations to quickly detect and alleviate IP conflicts.

## 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.

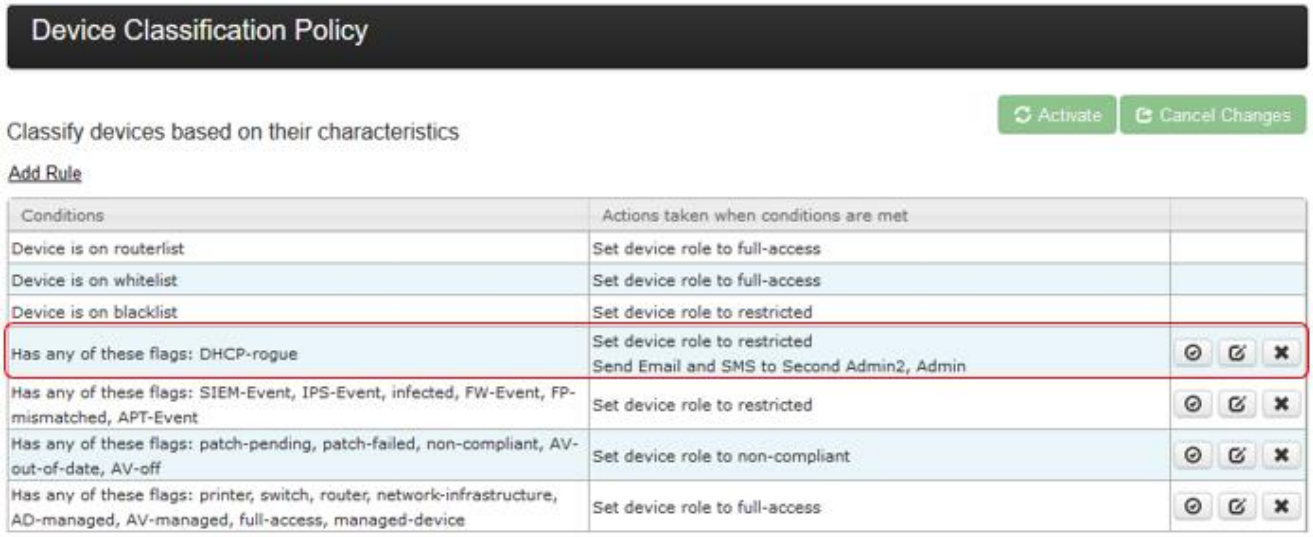
- Go to Configuration → General Settings.
- Click on Servers:




- Under DHCP Servers, input the IP addresses of all the authorized DHCP servers on the network.
- Select "Detect rogue DHCP servers"

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

Using Policies → Device & Role Classification rules, 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.

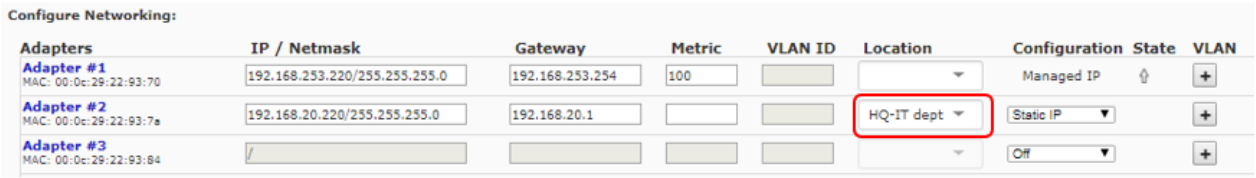


# Time \ Location \ List Policies

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.

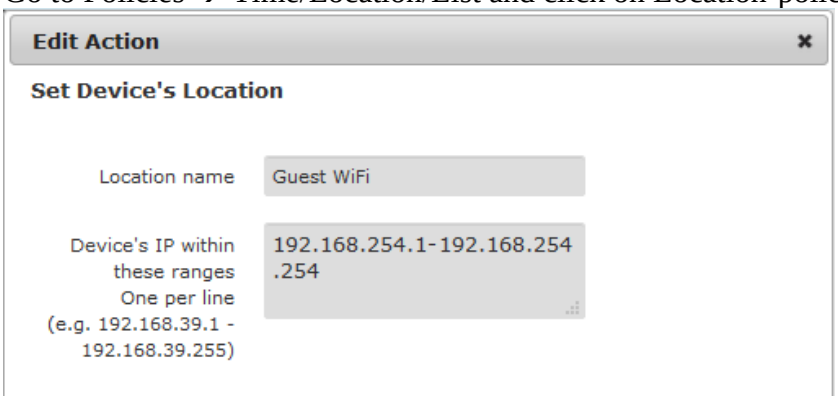
## Location Policy

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



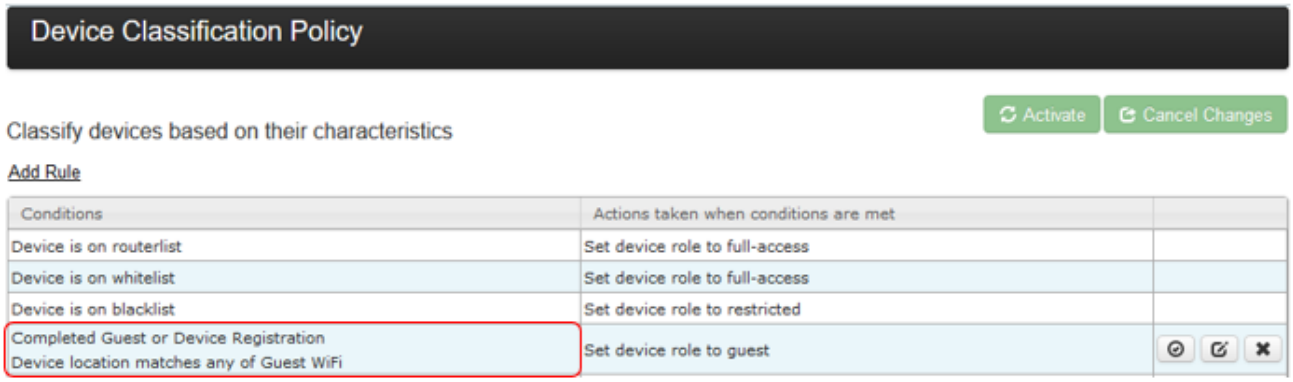

**Option 2:** Define location names by IP range.

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




Location definitions can be based on IP addresses. Once the Location name has been saved, it can now be added as a condition for Guest Access in the Device & Role Classification Policy.

- Go to Policies → Device & Role Classifications

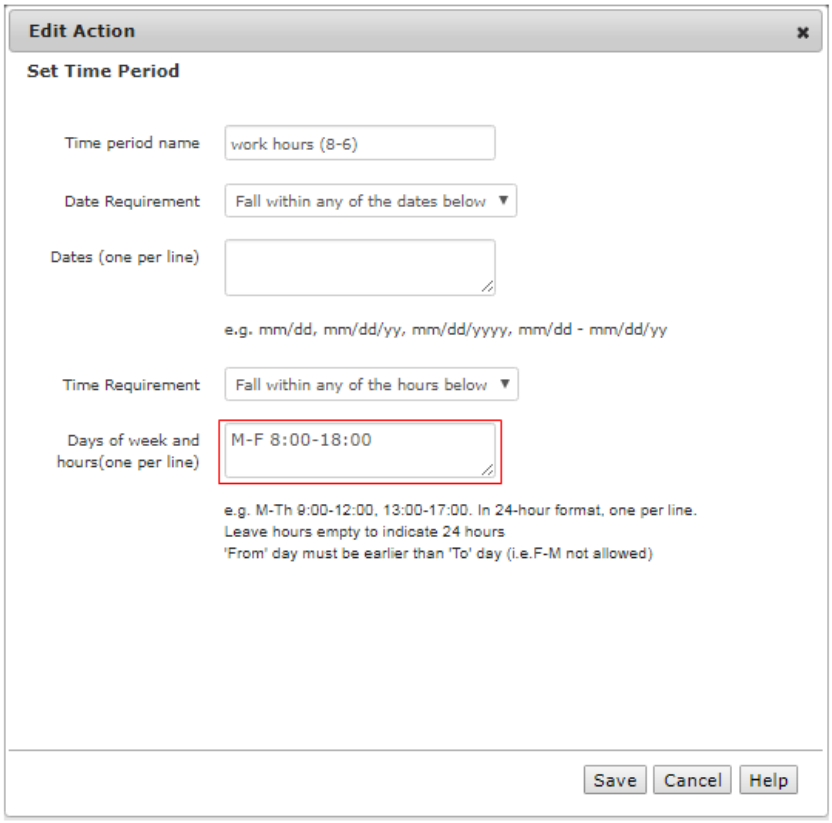



The above Device Classification Policy now has two conditions for guest access to be granted. If we wanted to limited access to office hours, we could set a third condition based on time.

## Time Policy

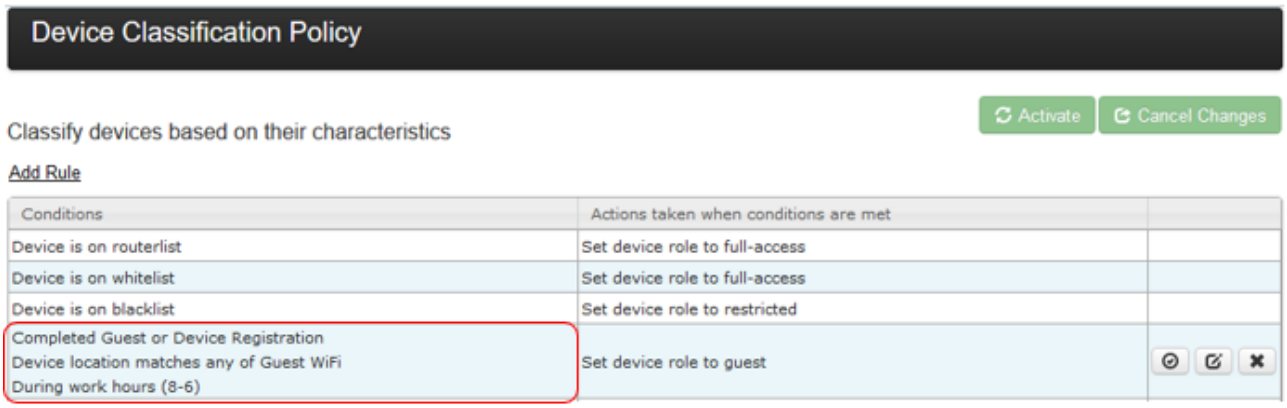
- Go to Policies → Time/Location/List and click on Time-policy.

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 a Device & Roles Classification Policy.

- Go to Policies → Device & Role Classifications



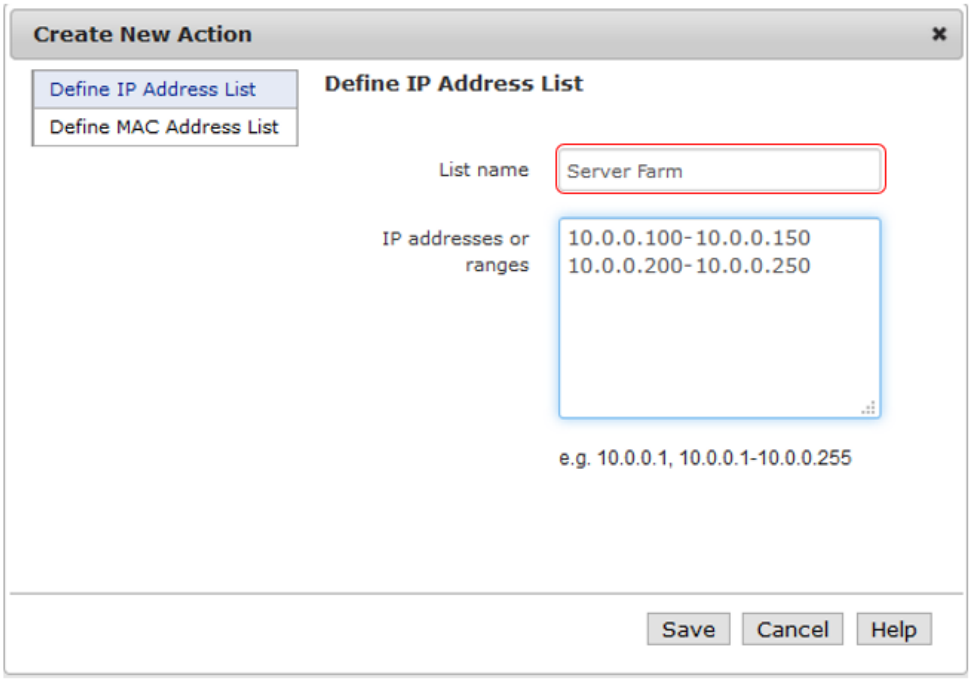

The above Device & Role Classification Policy now has three conditions for guest access to be granted.

## 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 whitelisted.

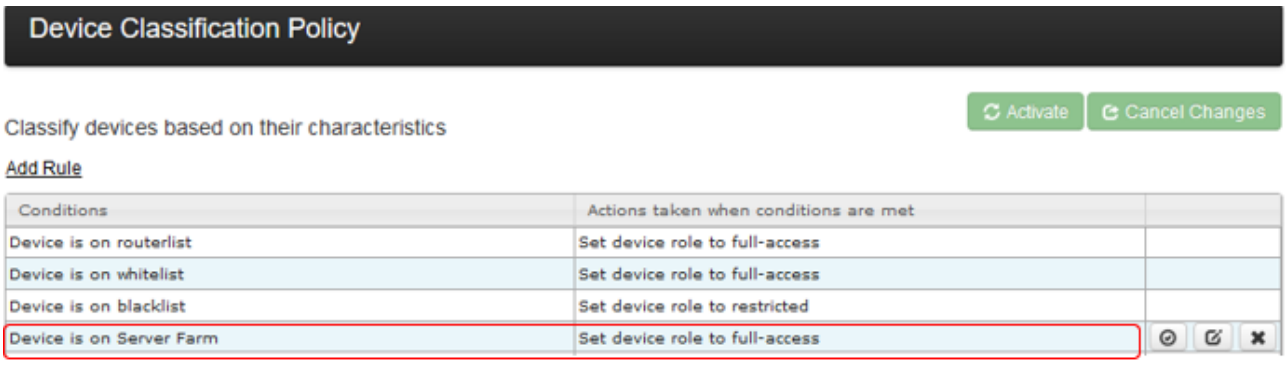
- Go to Policies → Time/Location/List and click on Device-lists.

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:




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

- Go to Policies → Device & Role Classifications




The above Device & Role Classification Policy will assign the Server Farm to have full-access.

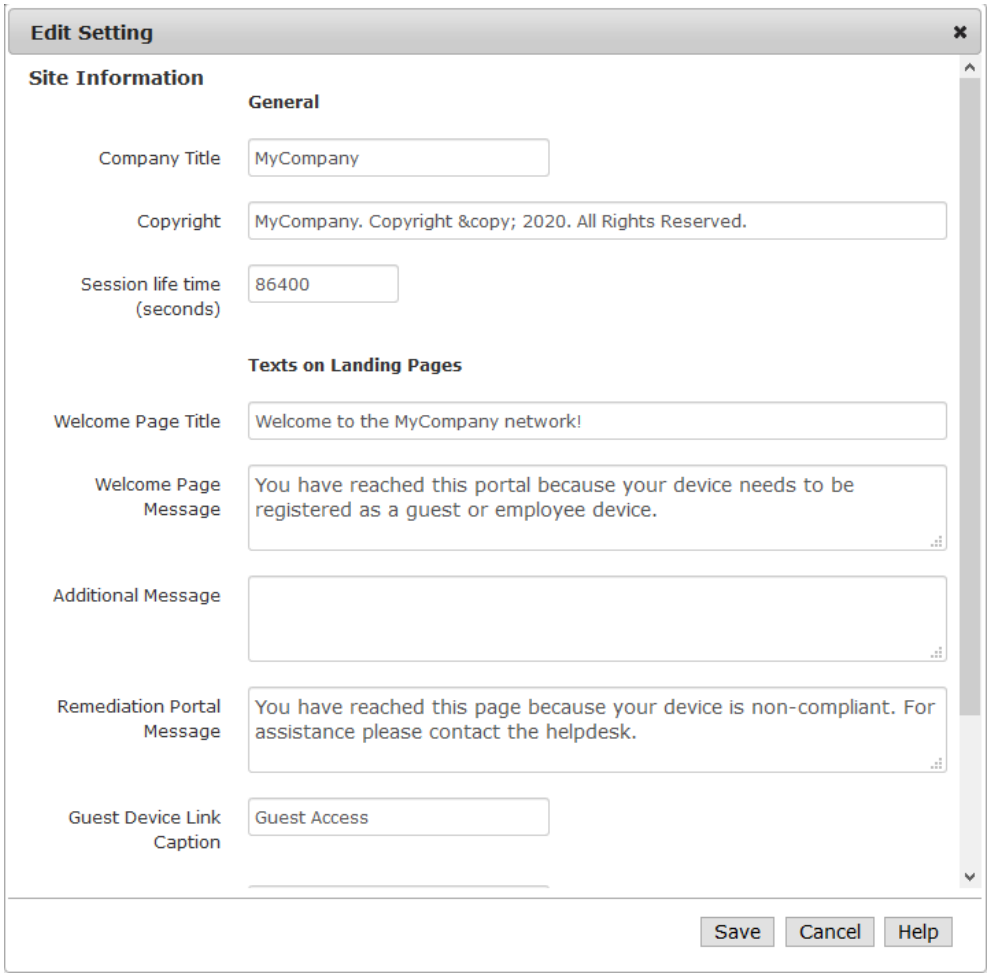
# Configuring Guest Access

CGX Access supports multiple login methods for guest registration. Typical options include self-service registration, sponsor registration, or self-service registration with sponsor approval. Registration with Facebook credentials is also supported. 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 desired.

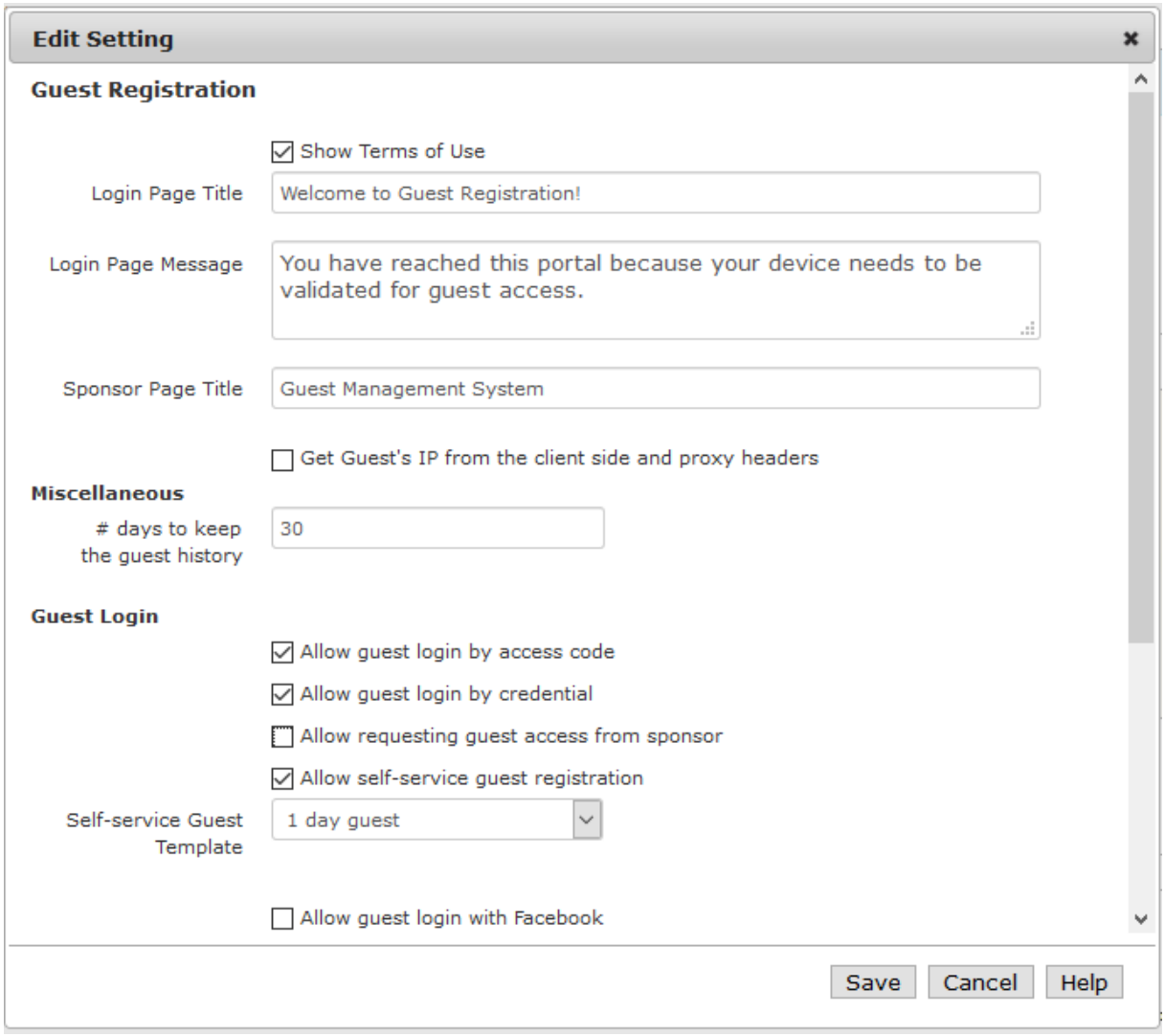



## Customize Guest Portal

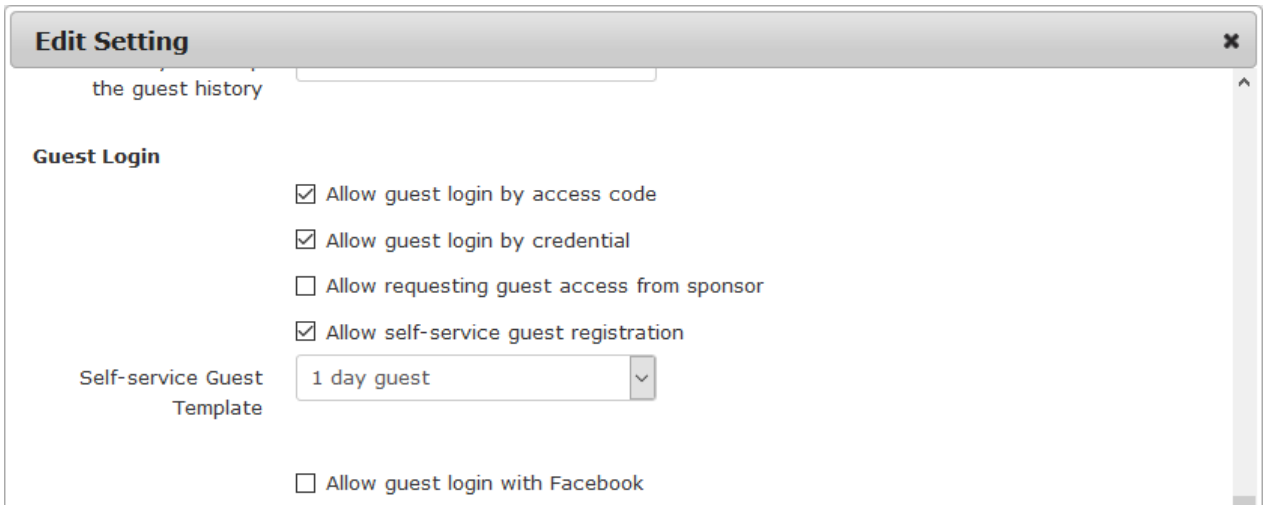
Go to Configuration → General Settings and click on "Guest Registration":

- Edit the title and message boxes as desired.

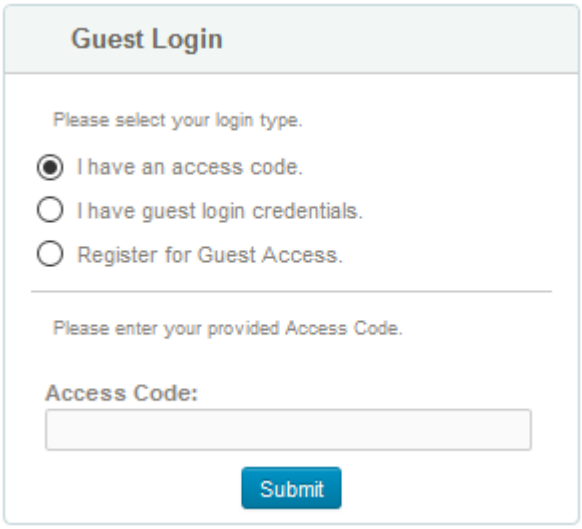
- Enable or disable terms and conditions
- Set the number of days to keep guest history details



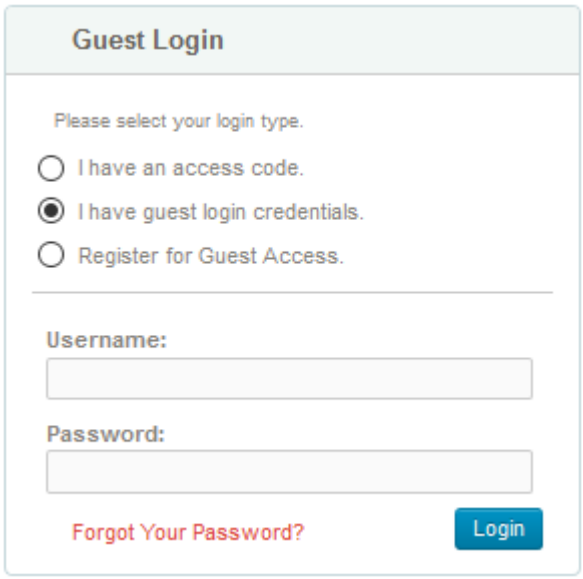

- Scroll down to enable your organizations preferred login methods



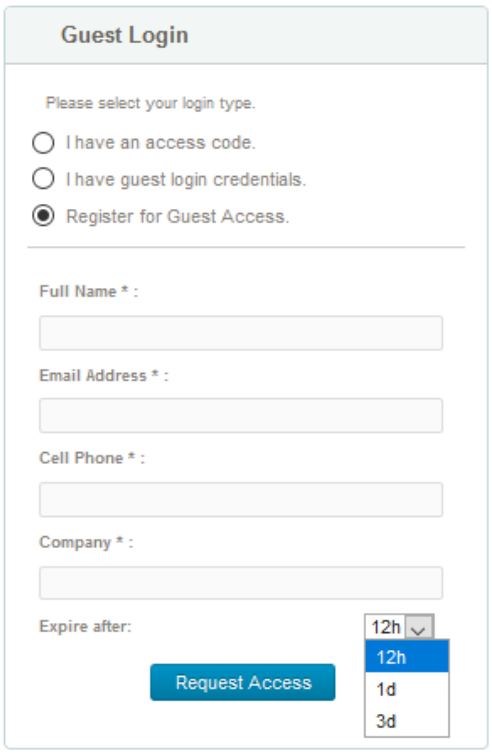
**Allow guest login by access code** – Enabled by default, this option allows for a guest to use a sponsor-provided access code to self-register a guest account. Based on Guest Templates, different access codes can require different registration information or grant different access to the guest \ consultant.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



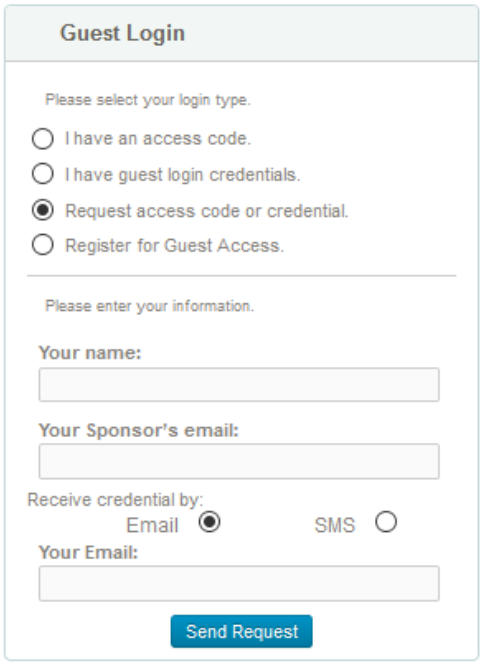

**Allow guest login by credential** – Enabled by default, this option allows for a guest to use their guest credentials to login. Guest Credentials can be created and provided by a sponsor or created by the guest as part of an earlier self-registration process.



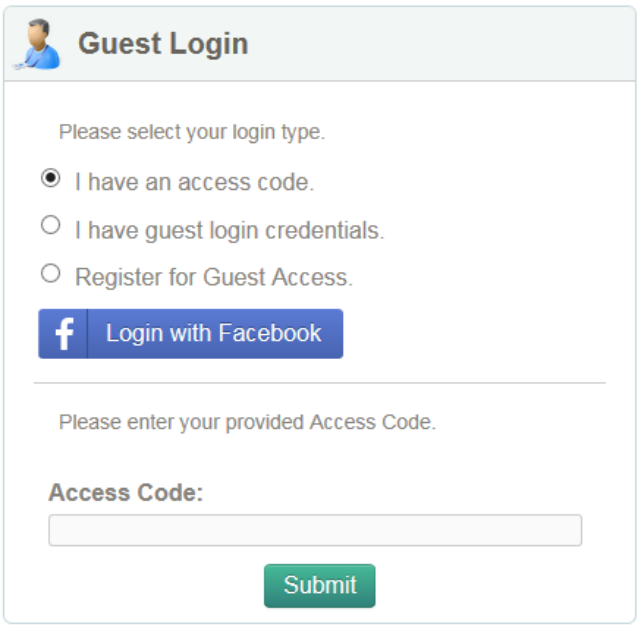

**Allow self-service guest registration** – Enabled by default, this option allows a guest to provide their contact information required and get immediate guest access without requiring an access code. Based on the guest template used, approval can be required, and the information they must provide can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




**Allow requesting guest access from sponsor** – Disabled by default. If enabled, this option allows a guest to provide their sponsor's e-mail address. Sponsor will be notified, and if sponsor approves, an access code will be sent to the guest, via e-mail or SMS.




**Allow guest login with Facebook** – Disabled by default. If enabled, a Facebook login button will be disabled on the captive portal. The guest can then use their Facebook credentials to authenticate as a guest.




**Note:** to use this feature, the organization must enable an APP on its Facebook account. Please see Appendix A for Facebook setup instructions.

**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, CGX Access 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 CGX Access. These templates can be modified, and new templates can be created. The default templates include:

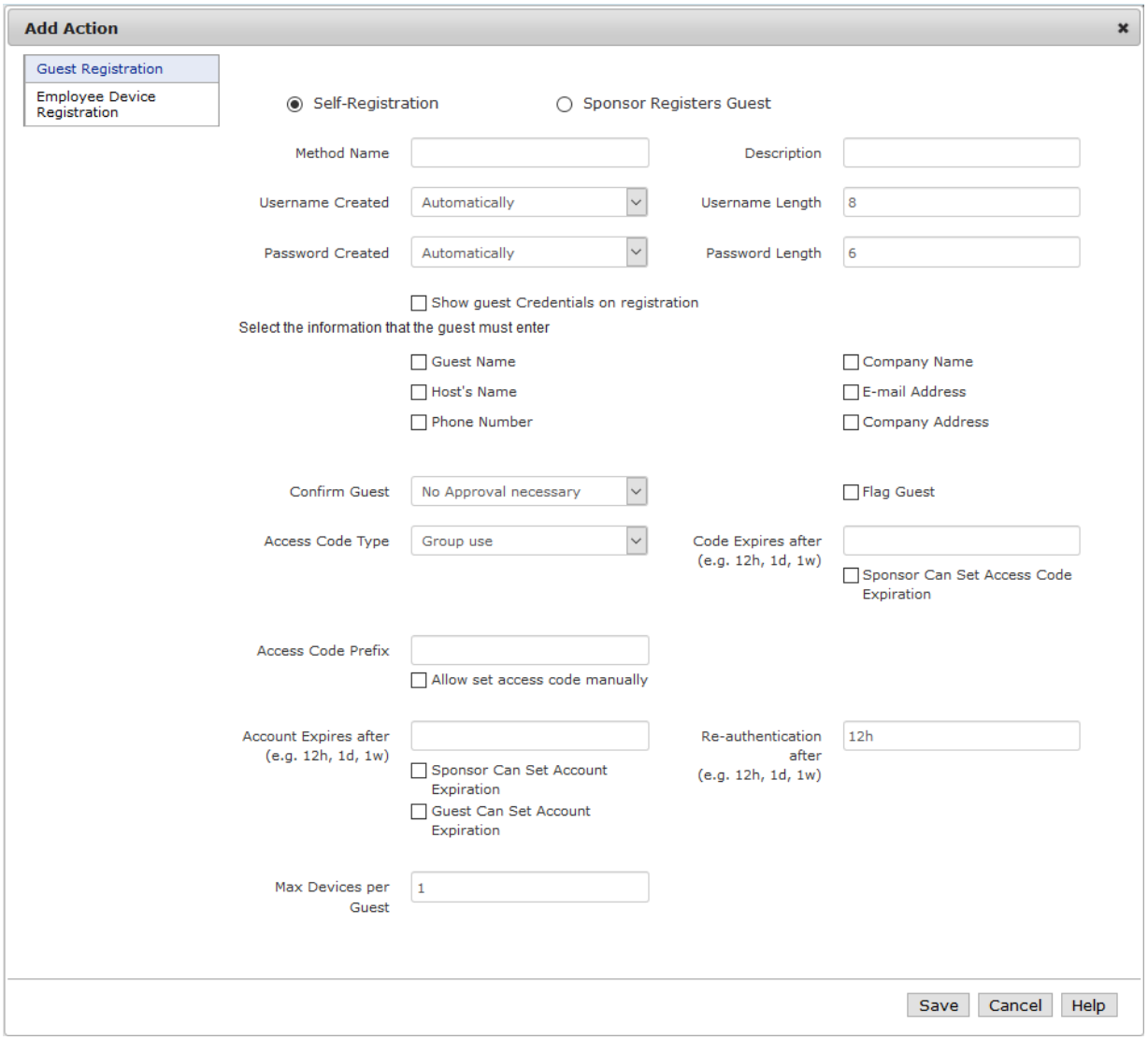
- **Consultant Registers Themselves**
  - Consultant register themselves using an access code
  - Account expiration set for 1 week, with authentication every 12 hours
  - A consultant flag is assigned, so that the guest would be given consultant access
  - Approval is not required, but can be enabled
  - 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

- **Facebook Guest Registration**
  - Used only when user uses Facebook to sign-in for guest access
  - Controls the length of time a user is allowed guest access and how often they must re-authenticate
- **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.


## 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 Create**d - 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 with 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.

**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.

**Flag Guest –** When checked, a Flag can be selected and assigned to the guest's device. This flag is useful for assigning a specific type of access to this guest. For example, if assigned a consultant flag, they will be assigned consultant access. For more details on flags, see the section titled Flagging Devices and Whitelisting.

**Access Code Type –** Access codes are useful when using different templates for different types of guests. This 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.

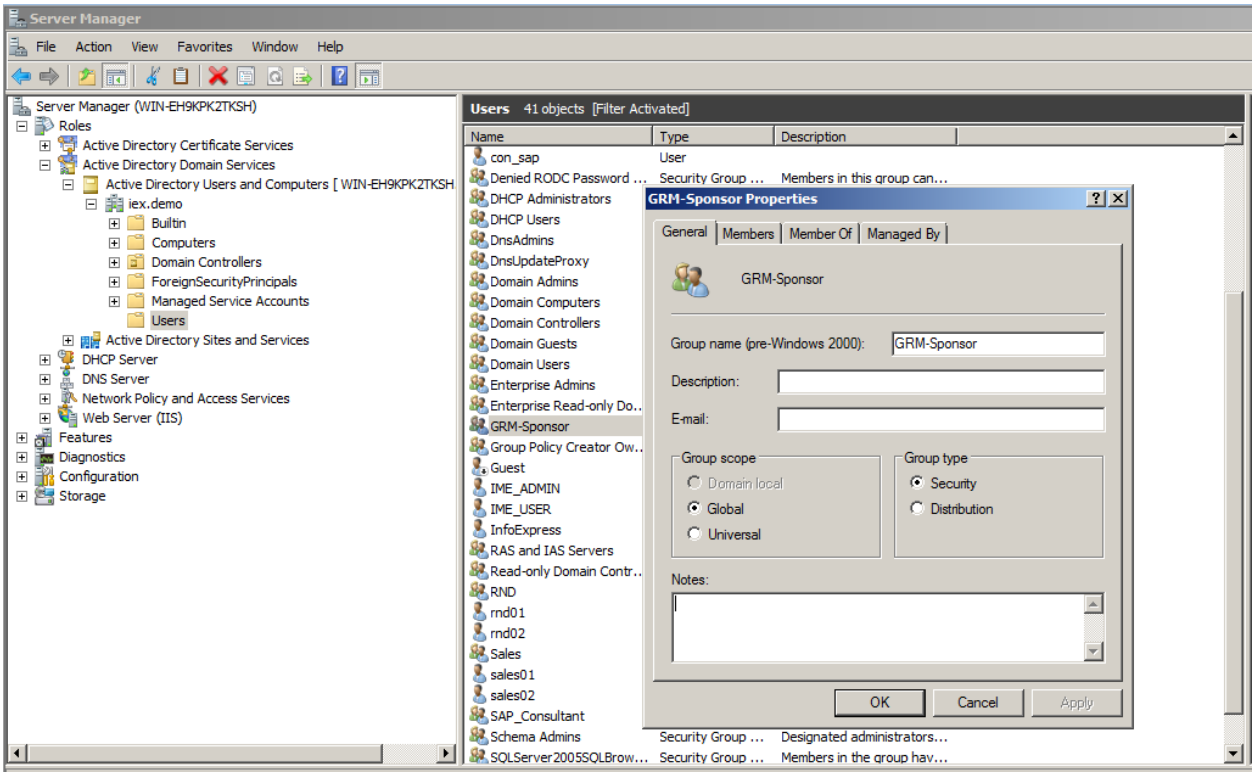
# Setting up Sponsors

CGX Access 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”

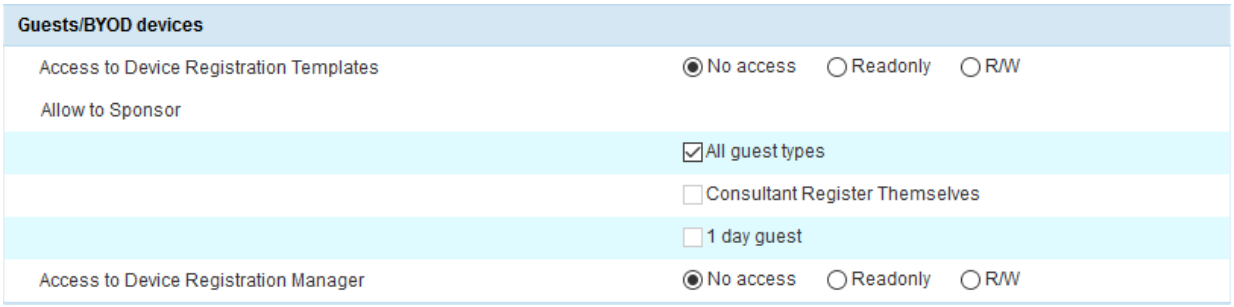
**Note:** upper/lower case is significant when creating AD groups.




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:

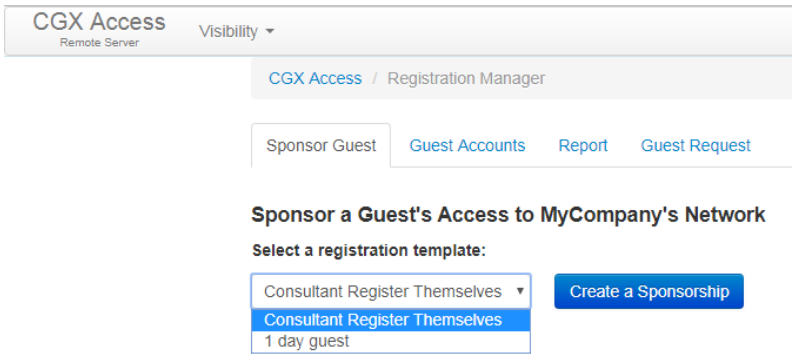
- Go to Configuration → Device Registration Methods
- Verify the types you want the sponsor to be able to administer
- Go to Configuration → Permission Manager and select the GRM-Sponsor Role (or another role you may have created)
- Select the appropriate Registration Methods the sponsor should be allowed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



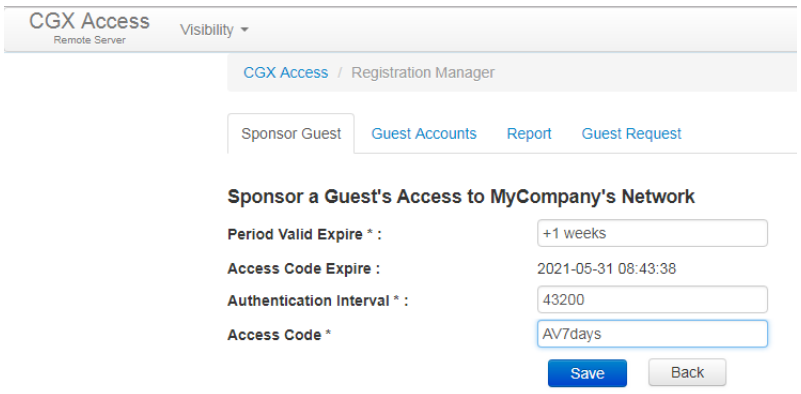

# Sponsoring Users

### 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":




- Complete the fields as desired and click "Save":




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

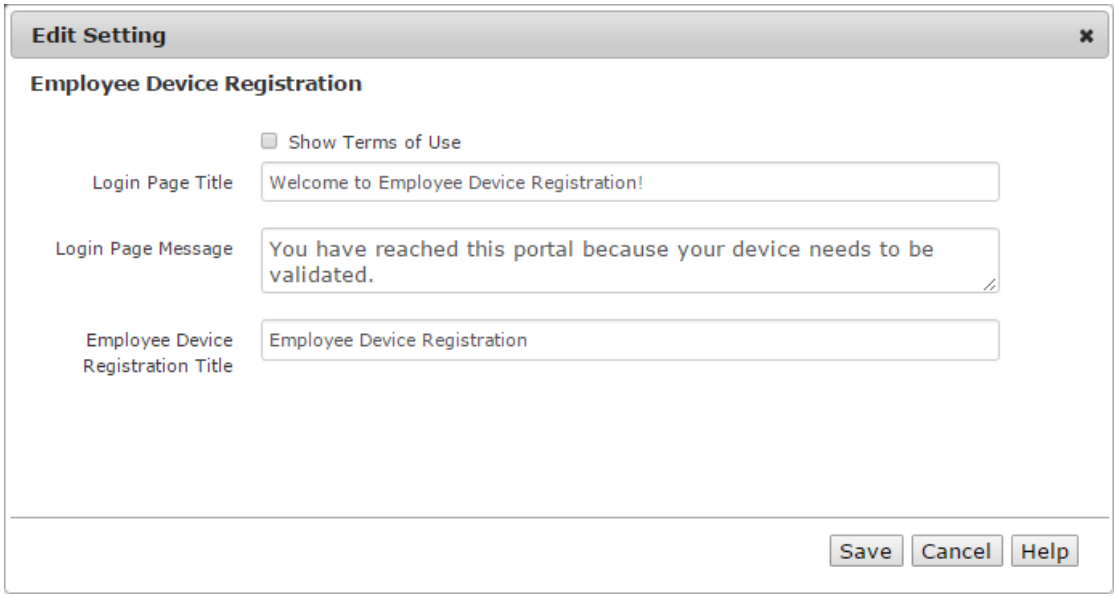
# Configuring Device Registration

CGX Access 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 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 devices
- Quantity of BYOD devices allowed per user (by group)
- Type of BYOD devices allowed
- Network access granted

## Customizing the Device Registration portal

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

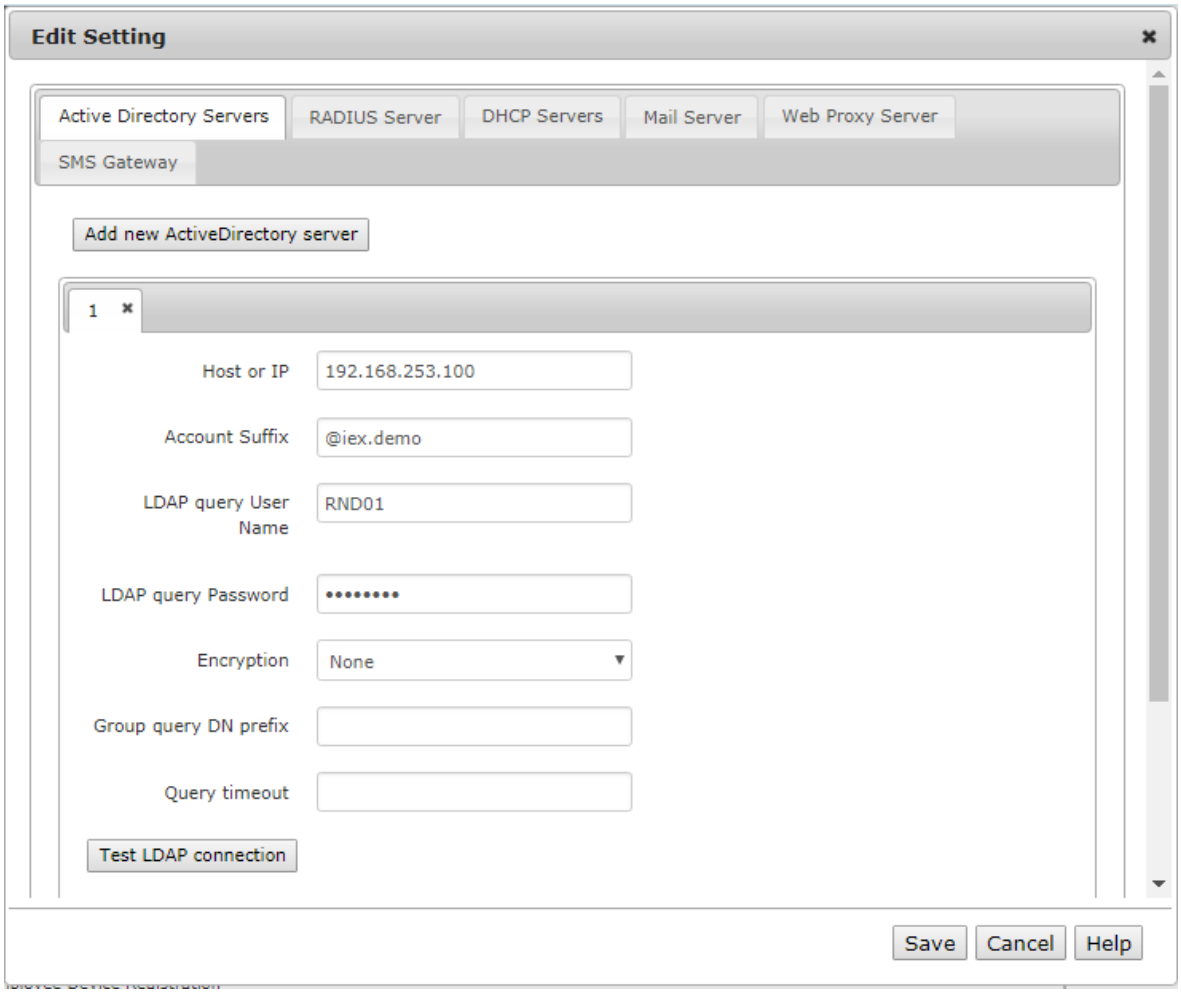



- Edit the title and message boxes as desired.
- Opt-in or Opt-out to show Terms of Use
- Click on save to accept any changes to the configuration.

## Confirm Active Directory settings

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

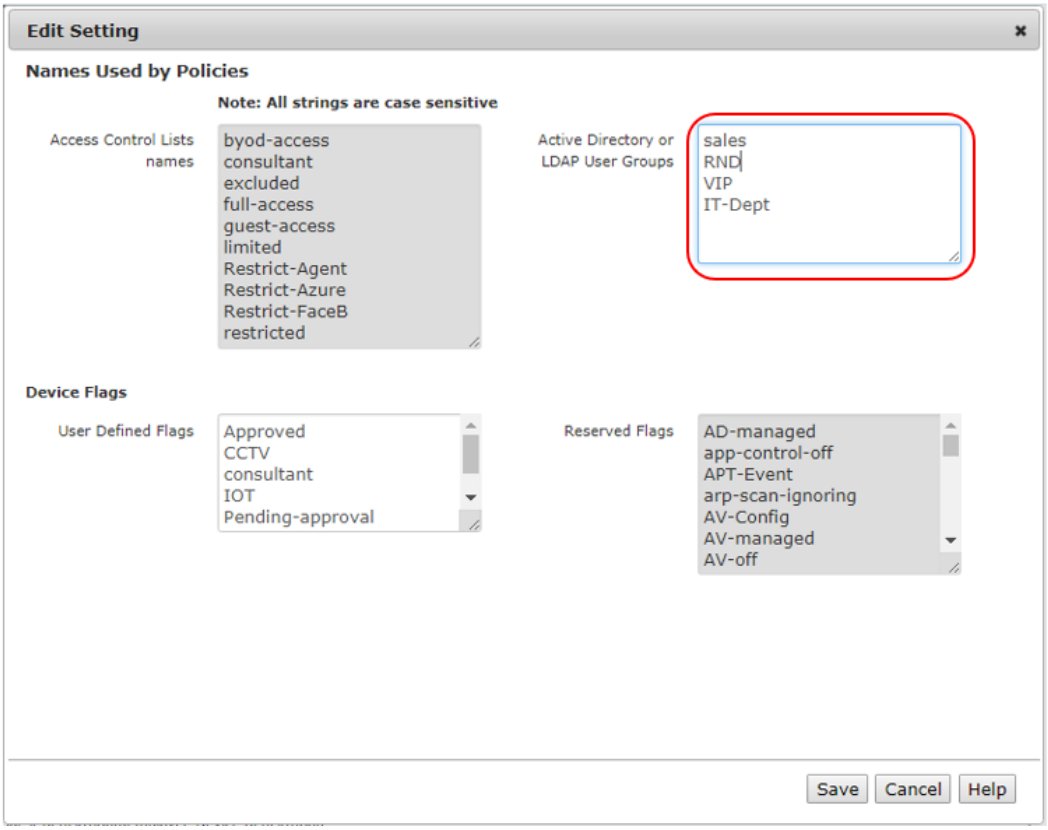
- Go to Configuration → General Settings.
- Click on Servers:




- 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”:



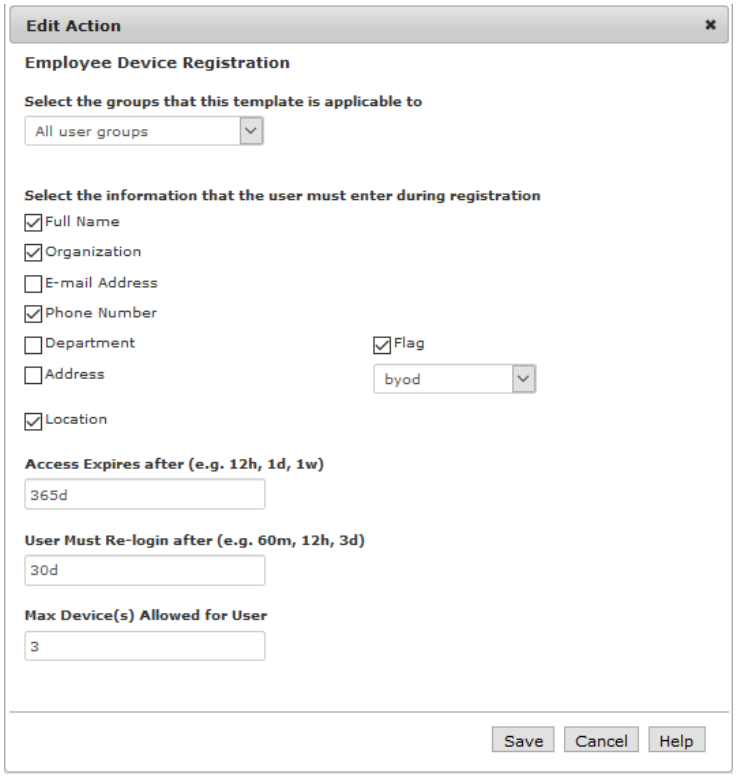

Add the Active Directory groups that would need to register their devices. Groups that are added will be shown as a configurable option when customizing Device Registration methods.

# Customizing Device Registration Methods

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


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

- Click on the "**Employee Registers Personal Device"** registration type:

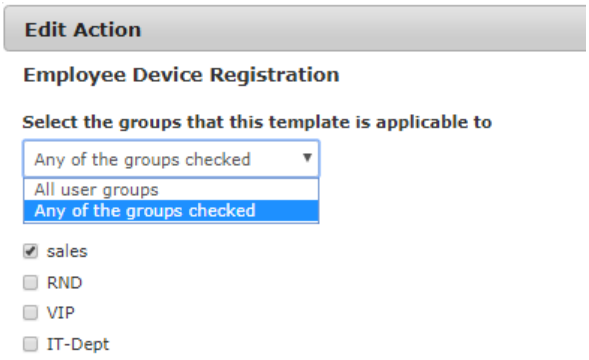



The above defines various parameters that can be customized for the device registration method. The default method is configured to apply to all users with valid credentials.

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:

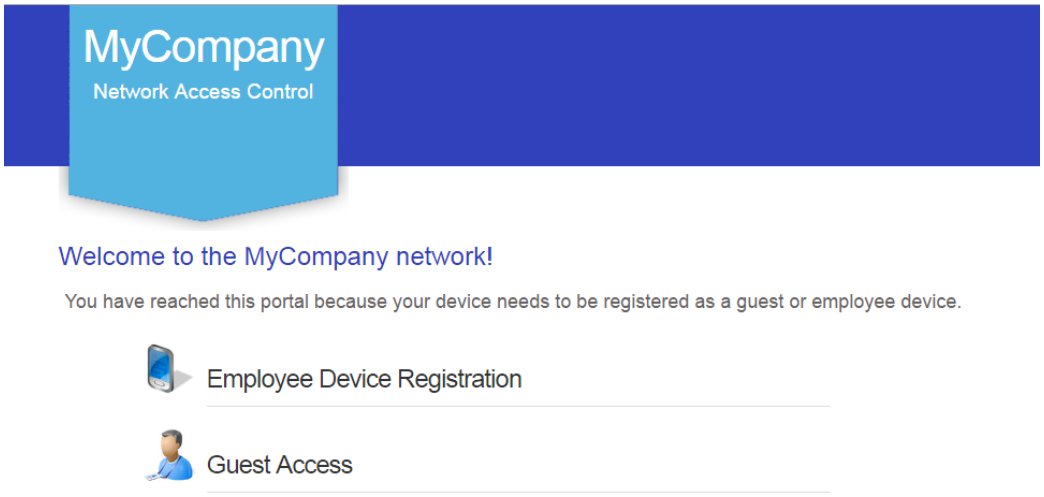



- Change the parameters for information gathered, access expiration, etc.
- Click 'Save' and Activate changes.

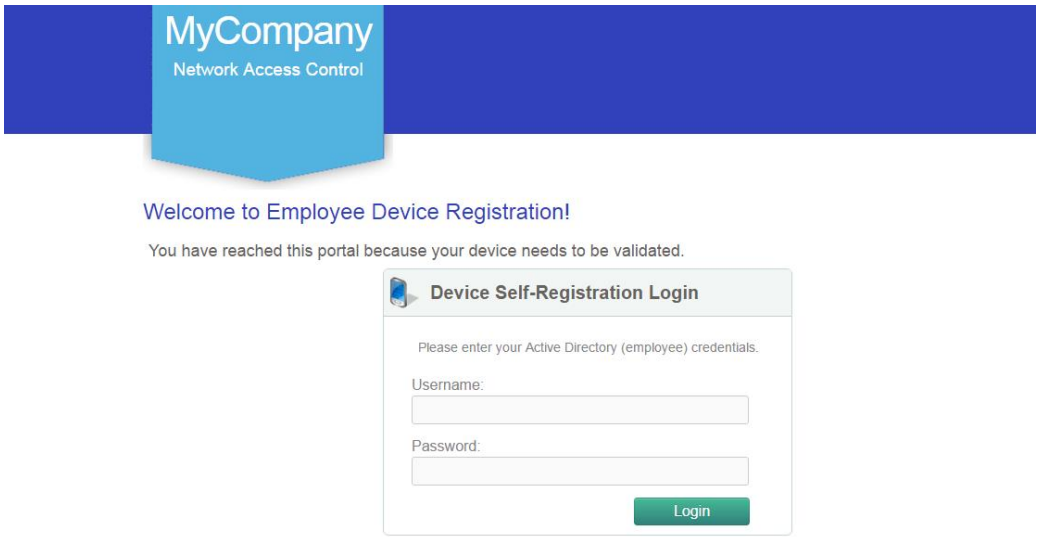
**Note:** When you have multiple Device Registration Methods, they are evaluated in order from top down. Methods can be re-arranged by dragging and dropping them in order they should be evaluated.

# User Experience

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




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




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.

# Integration: Anti-Virus \ Endpoint Management

CGX Access supports integration with enterprise AV and endpoint management vendors. By leveraging the integration at 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:

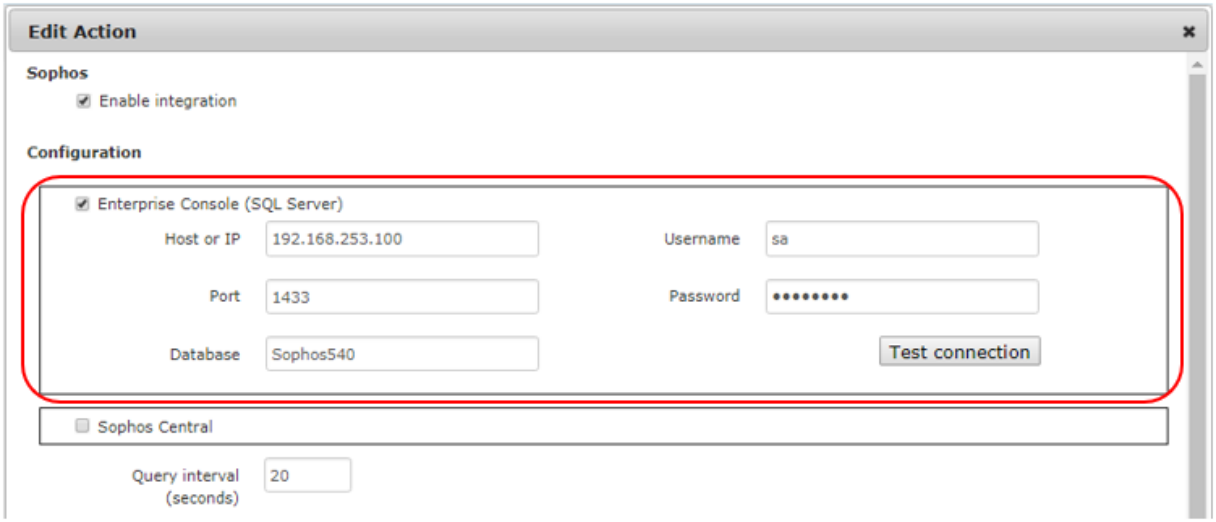
- Sophos Enterprise Console - 5.x +
- Sophos Central (cloud)
- Symantec Endpoint Protection Manager - 12.x and 14.x
- Symantec Endpoint Protection Cloud
- McAfee ePO - 5.x +
- Trend Micro OfficeScan - XG+
- Trend Micro Apex Central (cloud)
- Kaspersky Antivirus - 10.x+
- ESET Antivirus - 6.5+
- Microsoft SCCM \ WSUS – 4.x +
- Microsoft Intune
- Microsoft Windows Management Instrumentation (WMI)
- IBM BigFix - 9.x +
- Kasaya VSA
- Managed Engine Patch Manager
- Moscii StarCat 2013 and StarCat 10
- Carbon Black Cb Response – 6.x +
- InfoExpress CyberGatekeeper 9.x +

# Sophos Integration

Easy NAC support 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)”




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

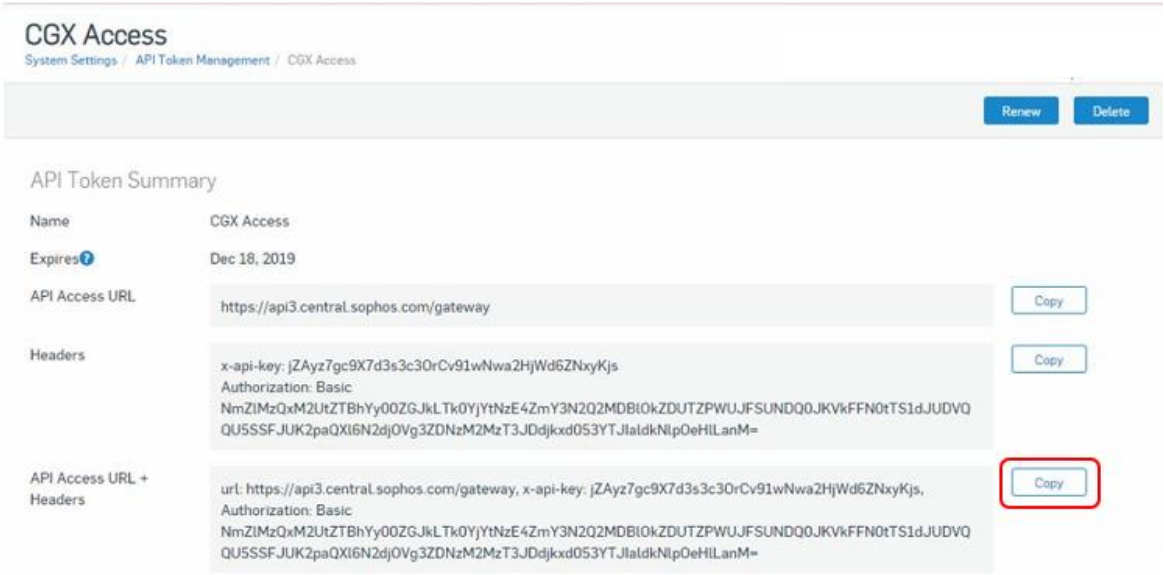
**Sophos SQL Prerequisites:**

- 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

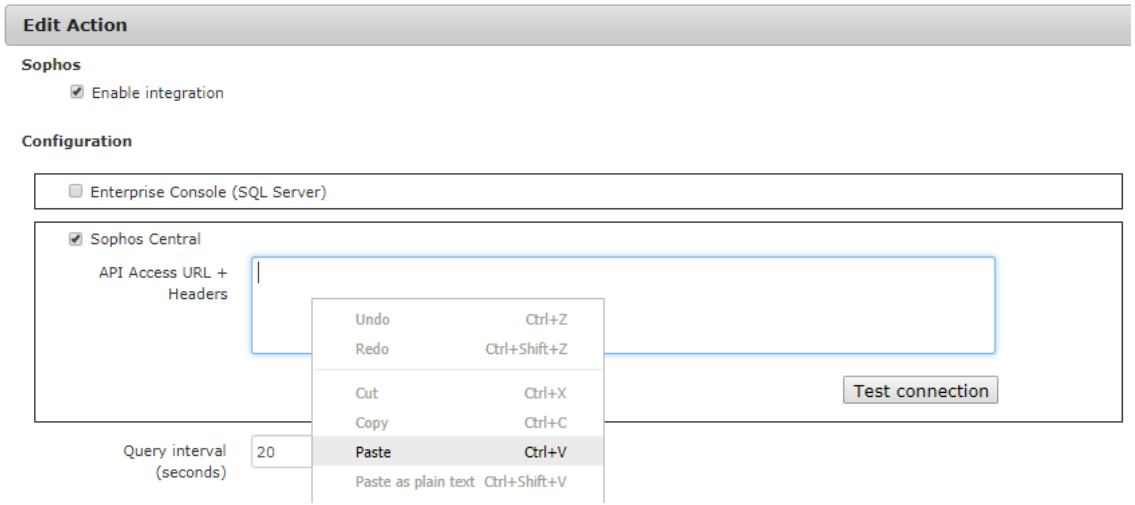
**Tip:** It may be helpful to search, “how to enable remote connections on SQL version…” referencing the specific version used by your Sophos Server.

**Configuring Sophos Central:**

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




- 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

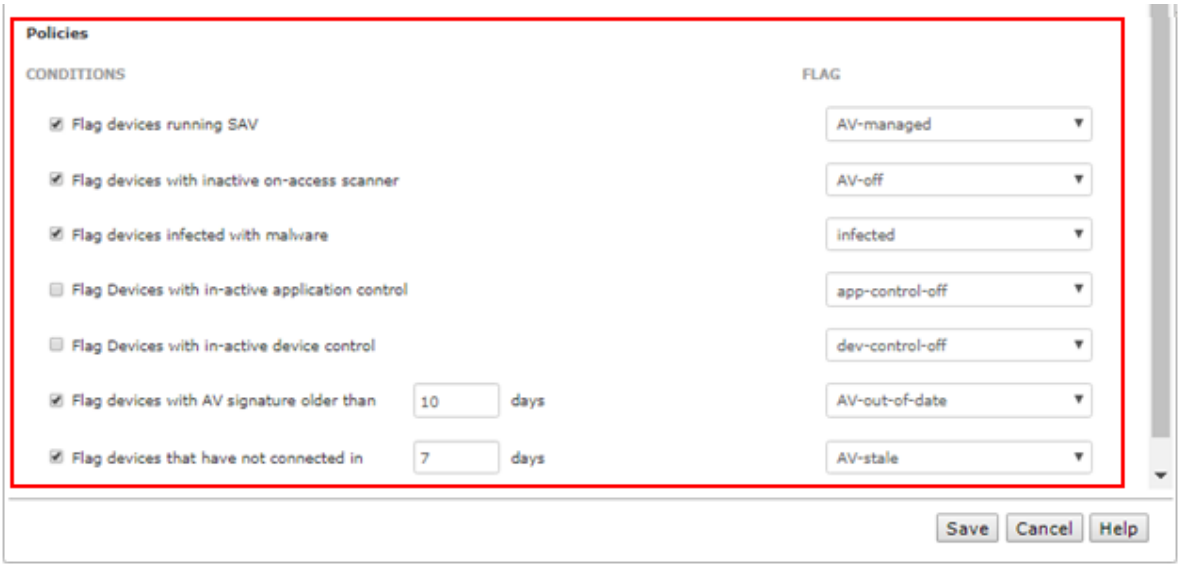



- Test the Connection
- If test is successful Save changes
- If test is unsuccessful, check that the CGX Access appliance has access to the Sophos Cloud.

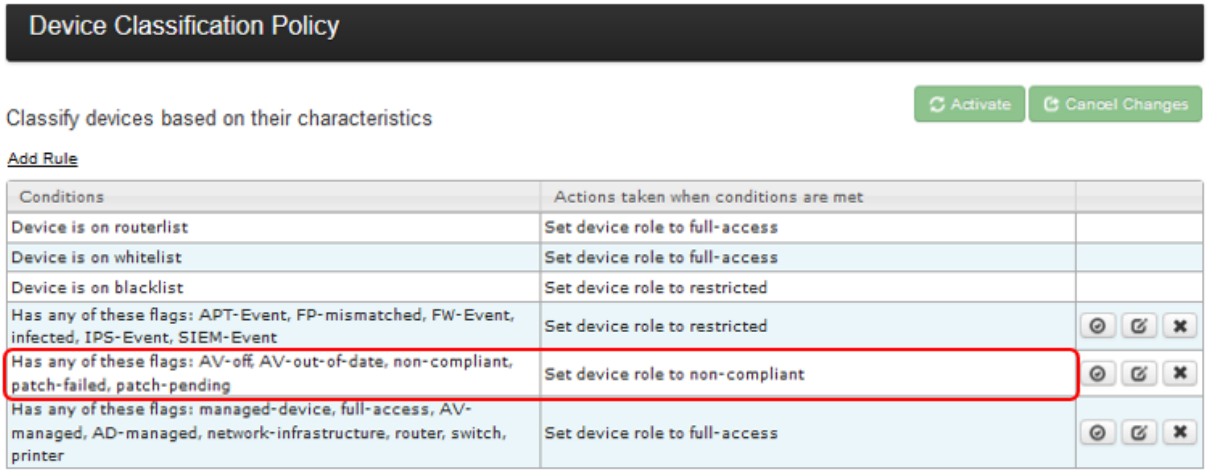
## Setting and Enforcing Anti-Virus Compliance Policies

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 flags 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 flags on specific devices that meet or fail the conditions. Using Device & Role Classification policies, devices with specific flags can be assigned different roles.

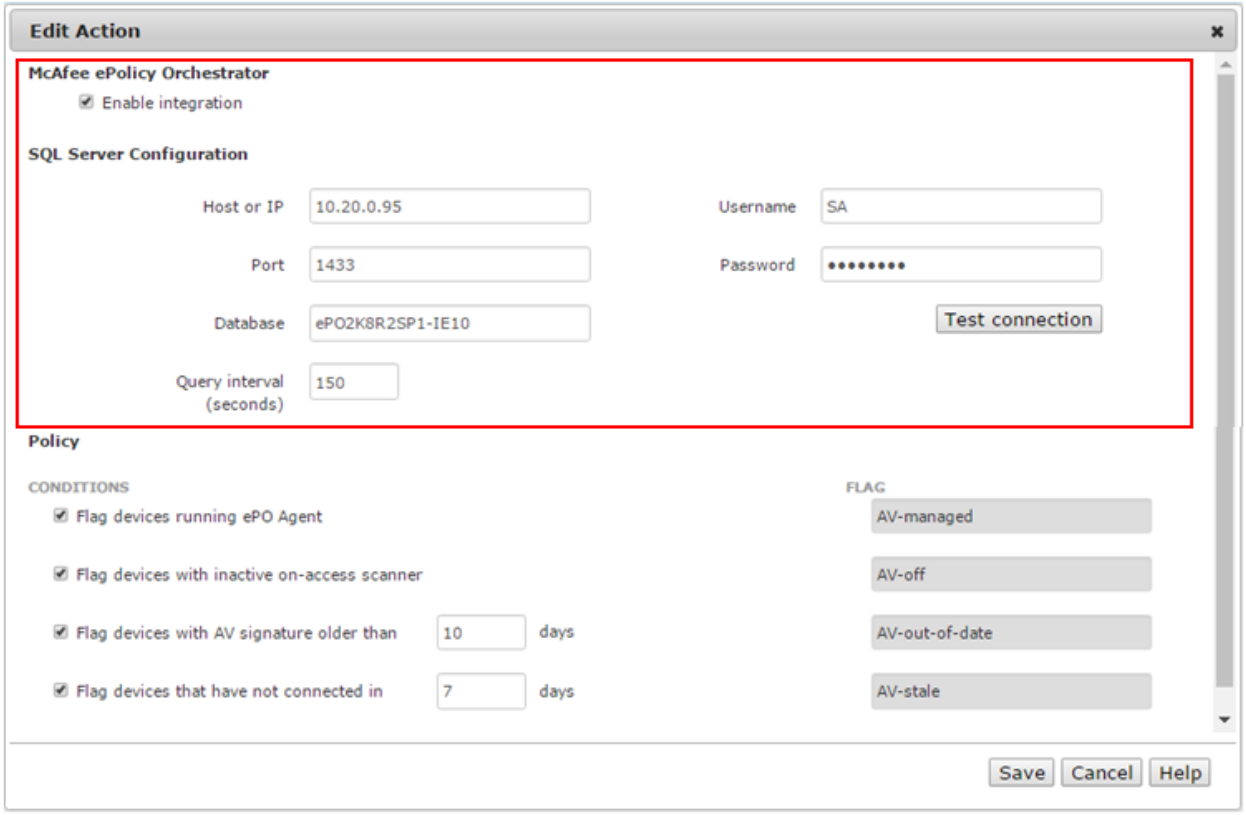



The example above shows a device will be assigned a non-compliant role if it has been flagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies, take precedence.

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

# McAfee ePolicy Orchestrator Integration

- In CGX Access GUI go to Configuration → Integration
- Select the "McAfee ePolicy Orchestrator"




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:**

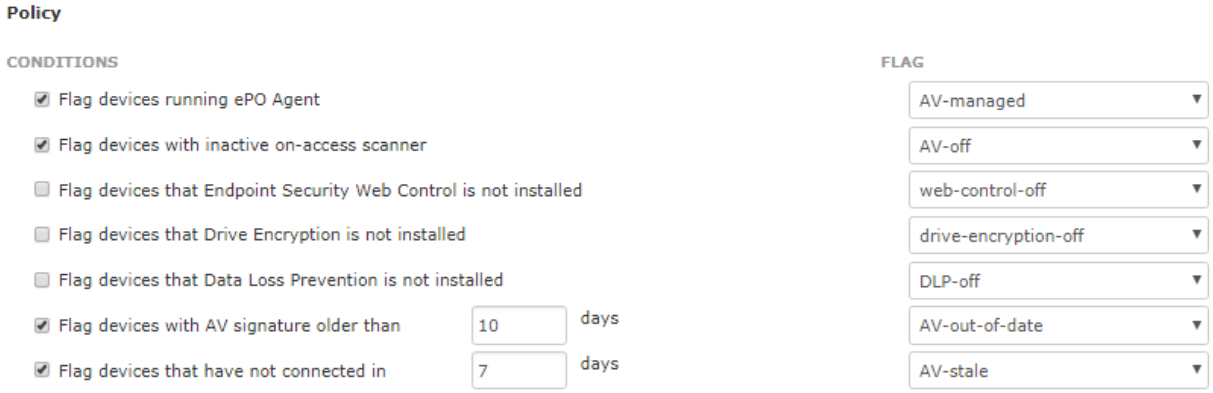
- Configure the MS SQL Server on the ePO server to enable TCP/IP and specify a port such as 1433
- Configure the firewall on the ePO server to allow CGX Access to communicate with the MS SQL Server port: 1433

**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

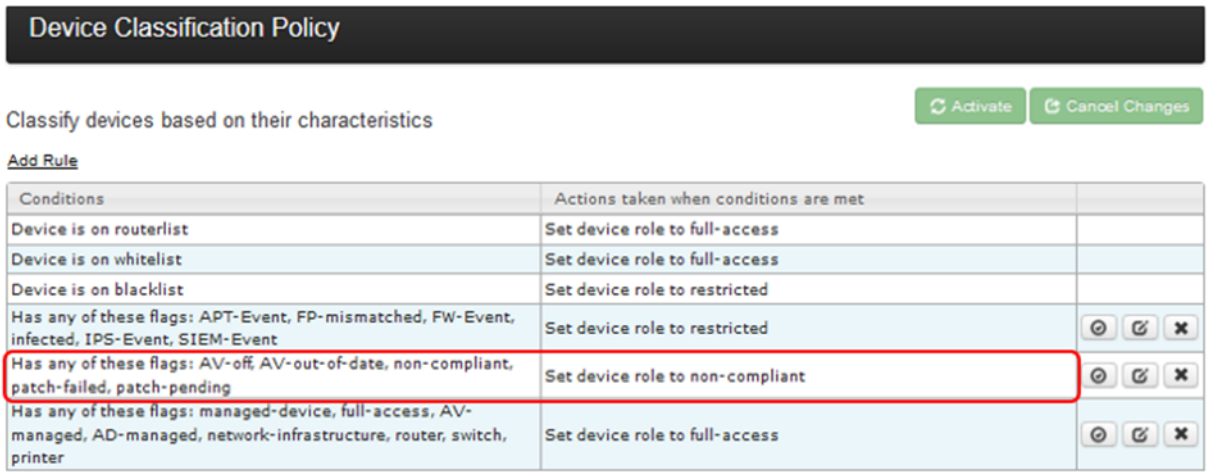
Once the communications between the CGX Access appliance and ePO SQL server have been successfully tested, policies can be set to enforce compliance with AV policies.

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




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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.

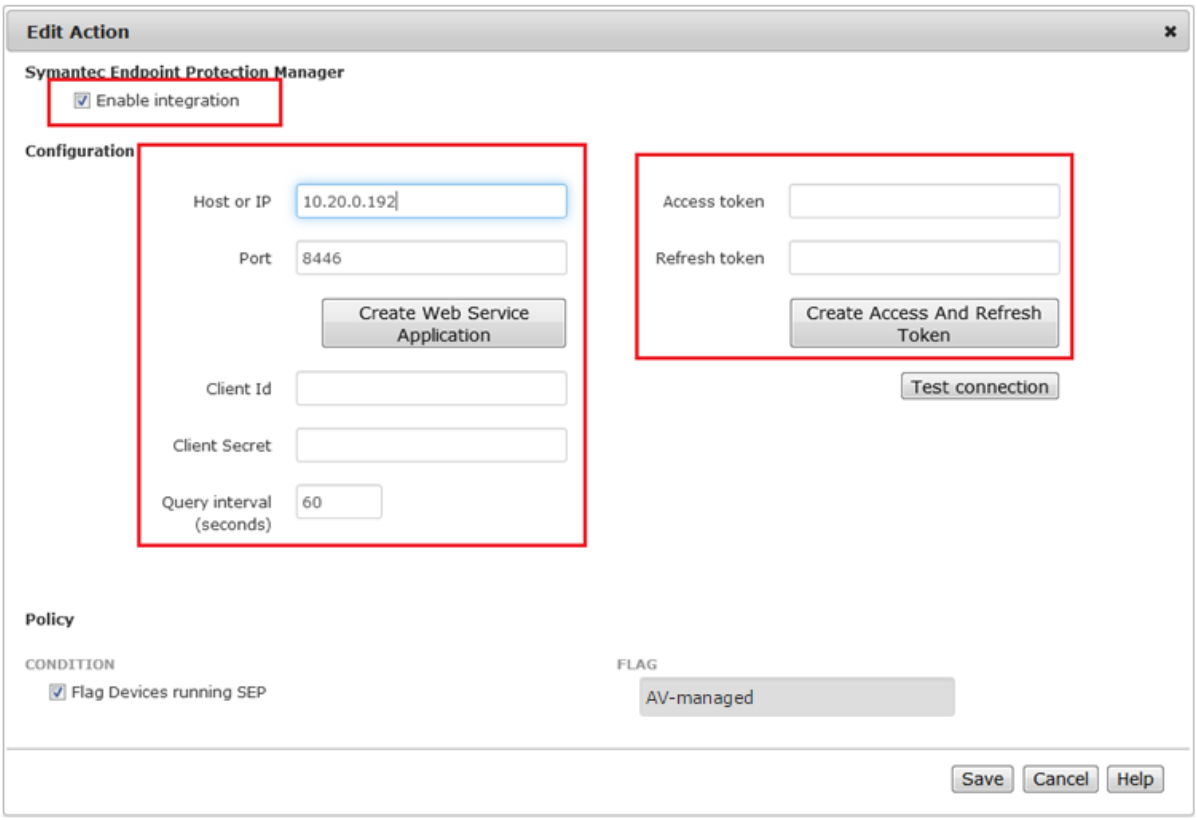



The example above shows a device will be assigned a non-compliant role if it has been flagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies, take precedence.

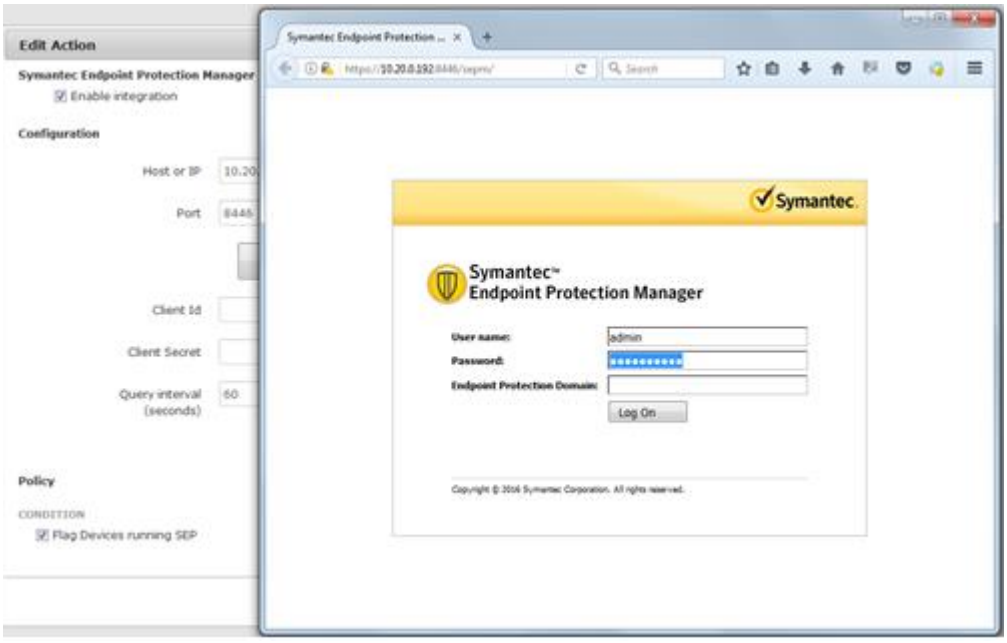
**Tip:** The AV-managed flag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

# Symantec Endpoint Protection Manager - 12.x

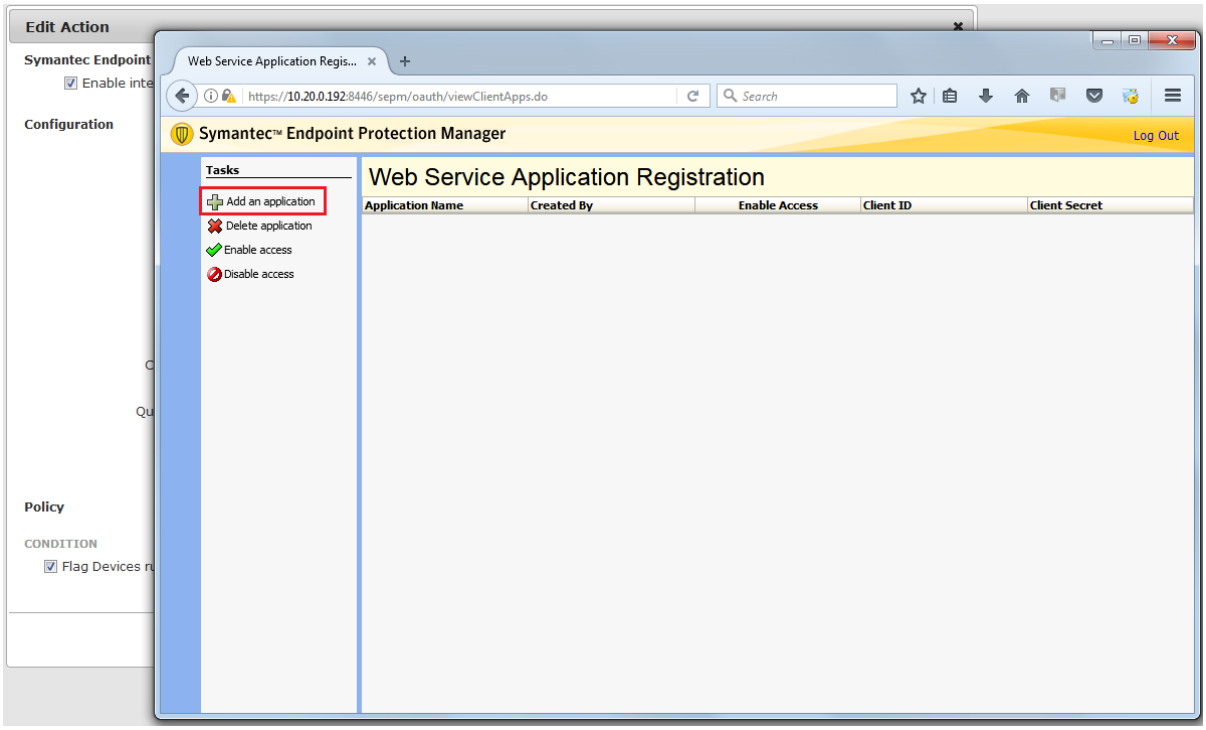
- In CGX Access GUI go to Configuration → Integration
- Click on "Symantec Endpoint Protection Manager"



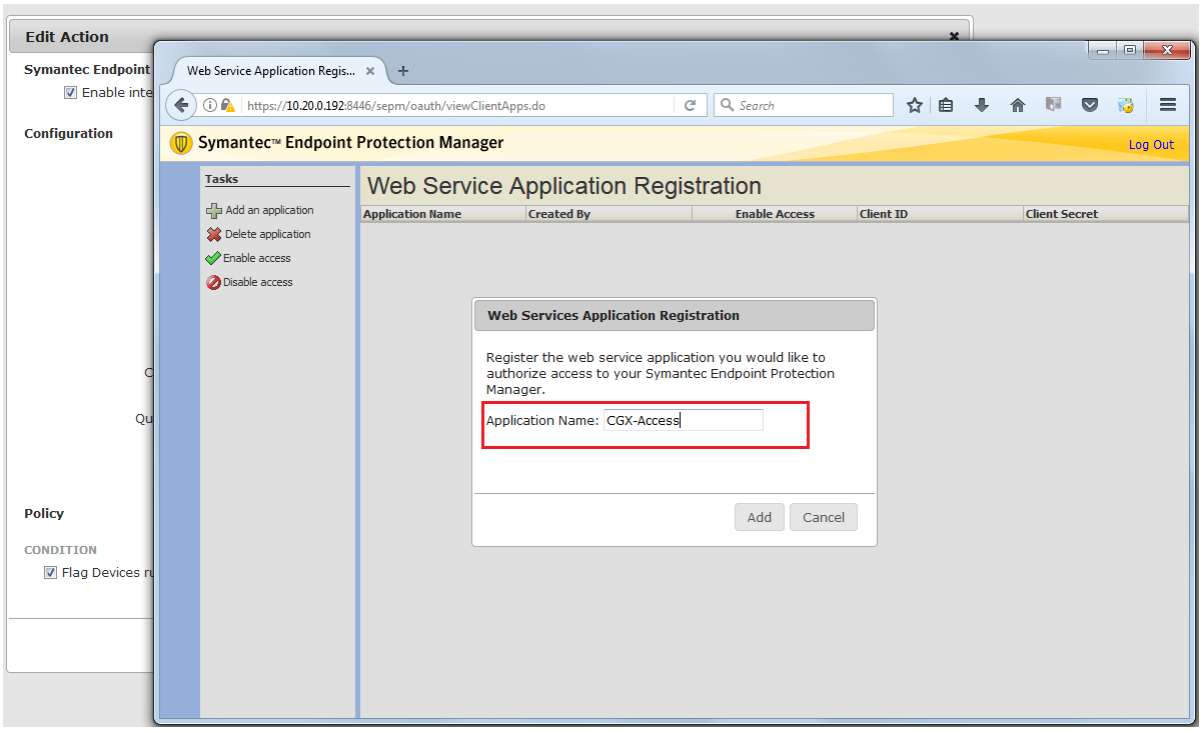

- Check “Enable Integration”
- Enter Hostname or IP / port
- Click on "Create Web Service Application" button (a new web-browser window will open)



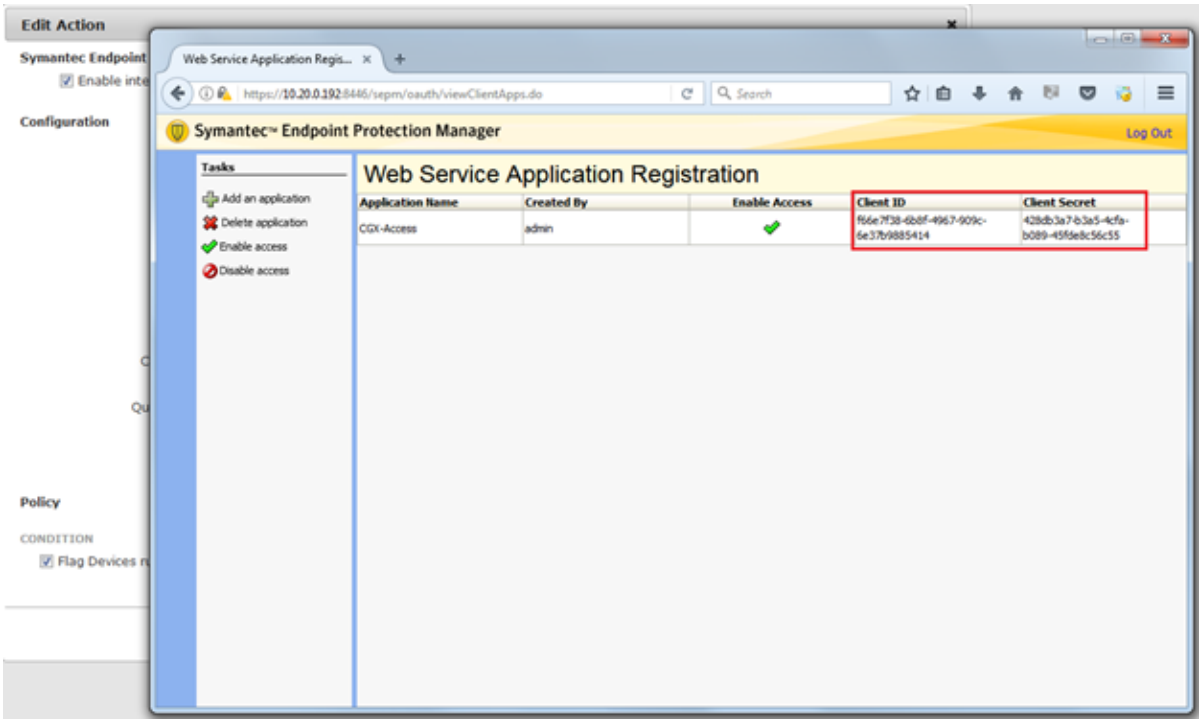
- Enter Username / Password to login to SEPM



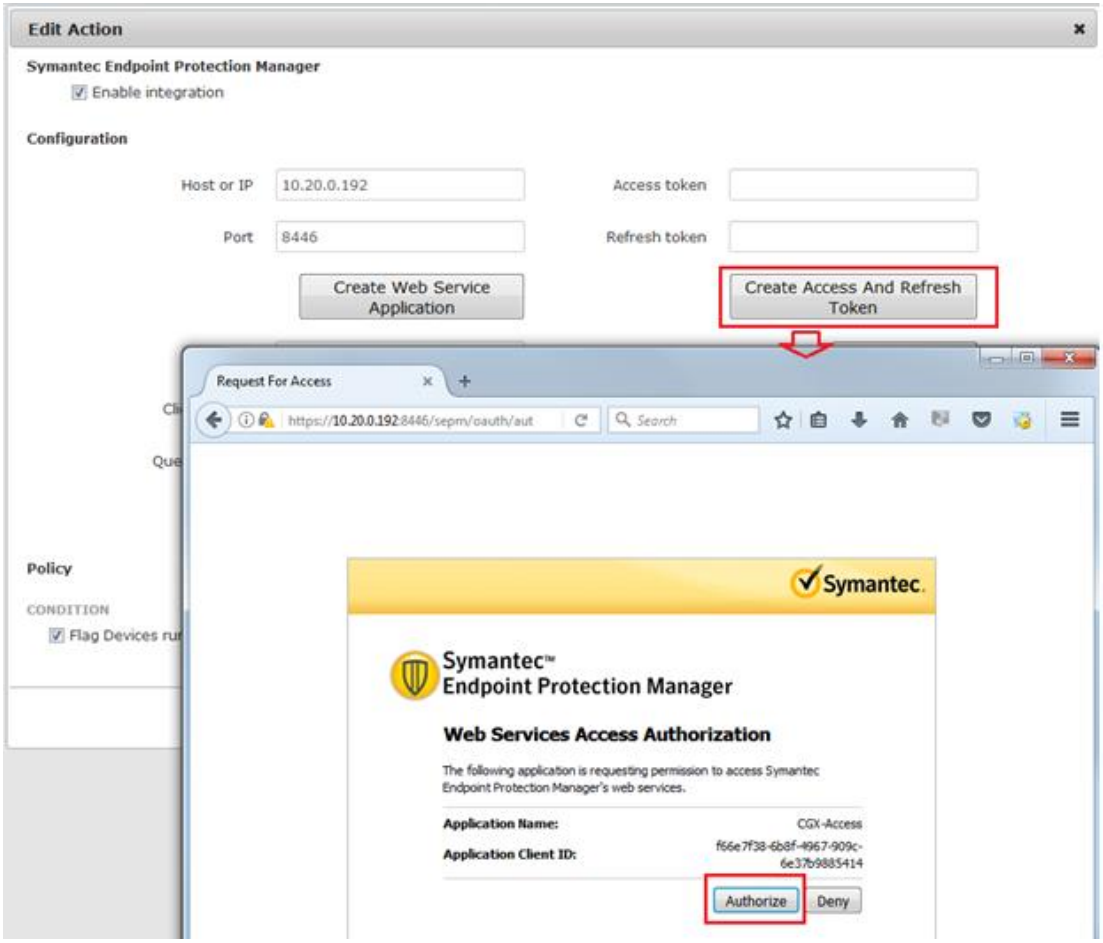

- In left hand pane click on "Add an application"



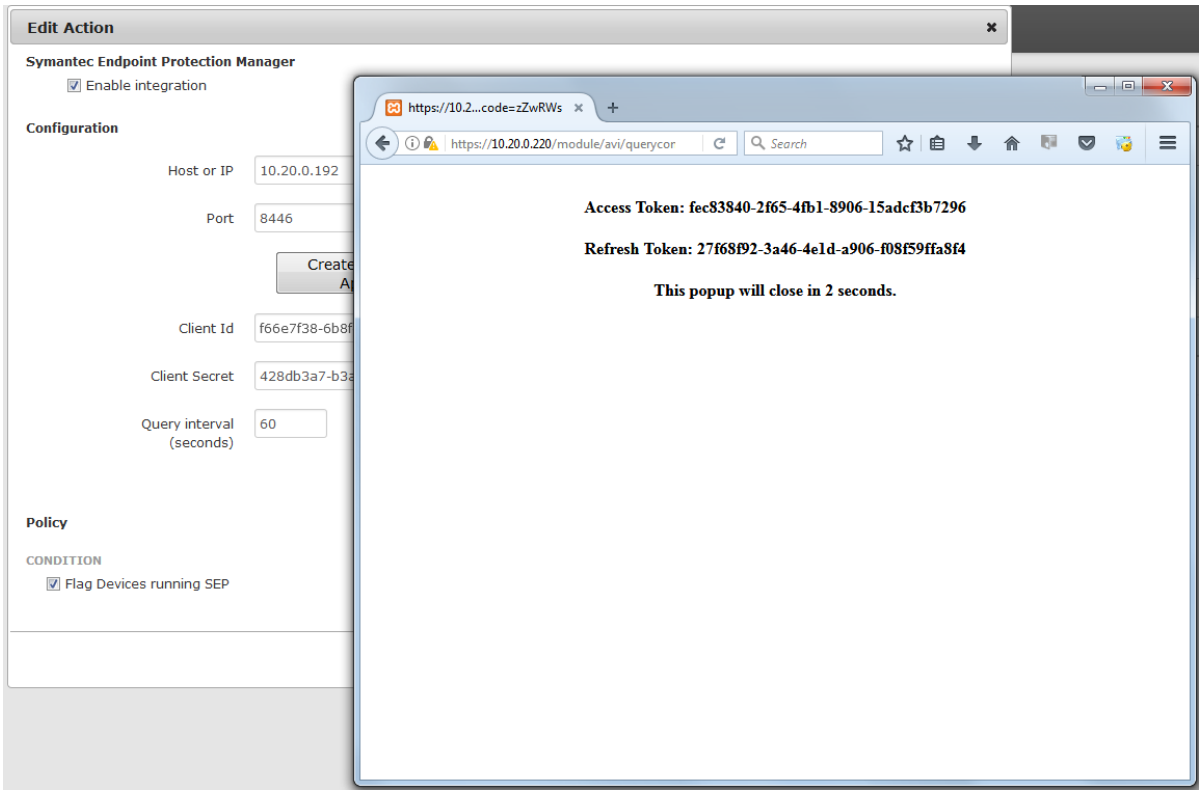

- Enter Name of application and click on “Add” button (this will generate client-id and client-secret)



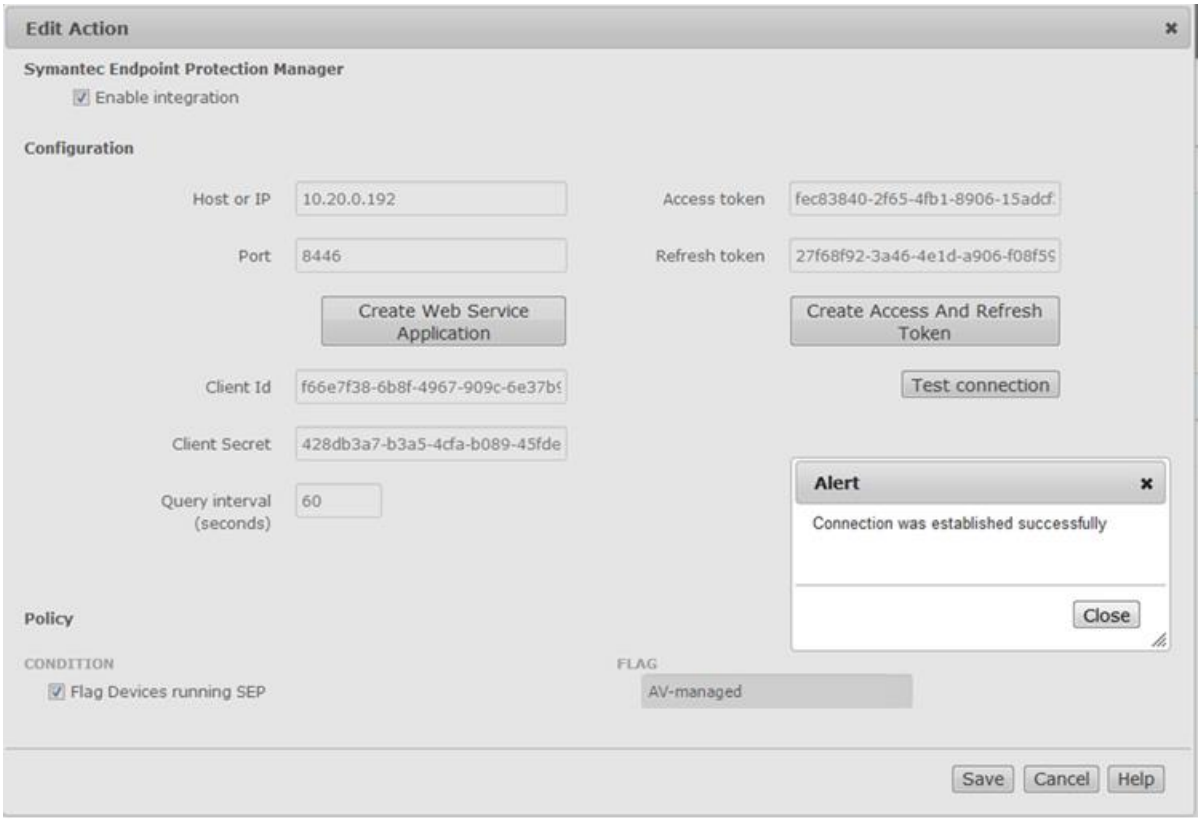

- Enter these credentials in CGX configuration page and click on "Create Access and Refresh Token" button.



- Click on "Authorize" button to authorize this application and generate tokens.




- These values will automatically get populated in CGX Access configuration page.

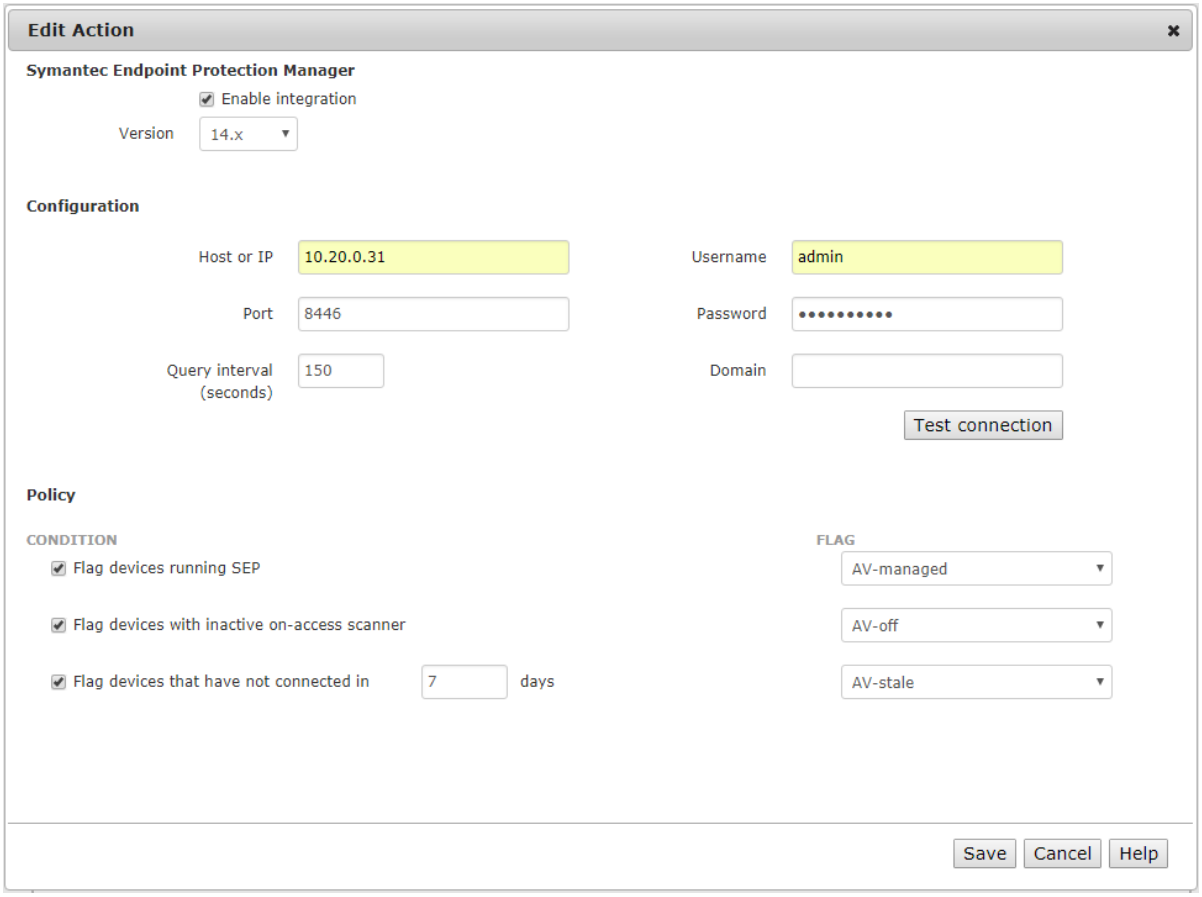


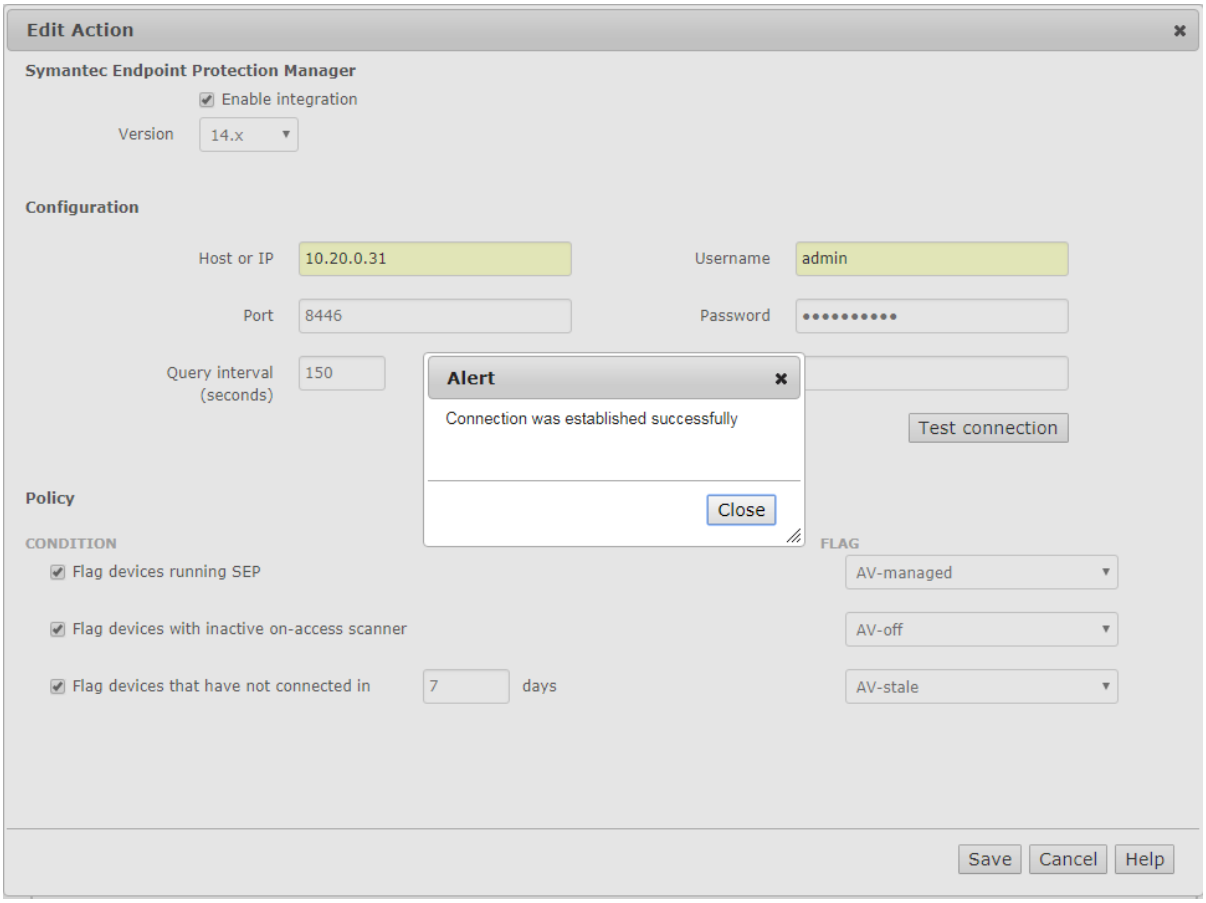

- Use "Test connection" button to validate settings
- You may leave Query interval and flagging conditions as default or modify as required
- Save this configuration

**Tip:** The AV-managed flag 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






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

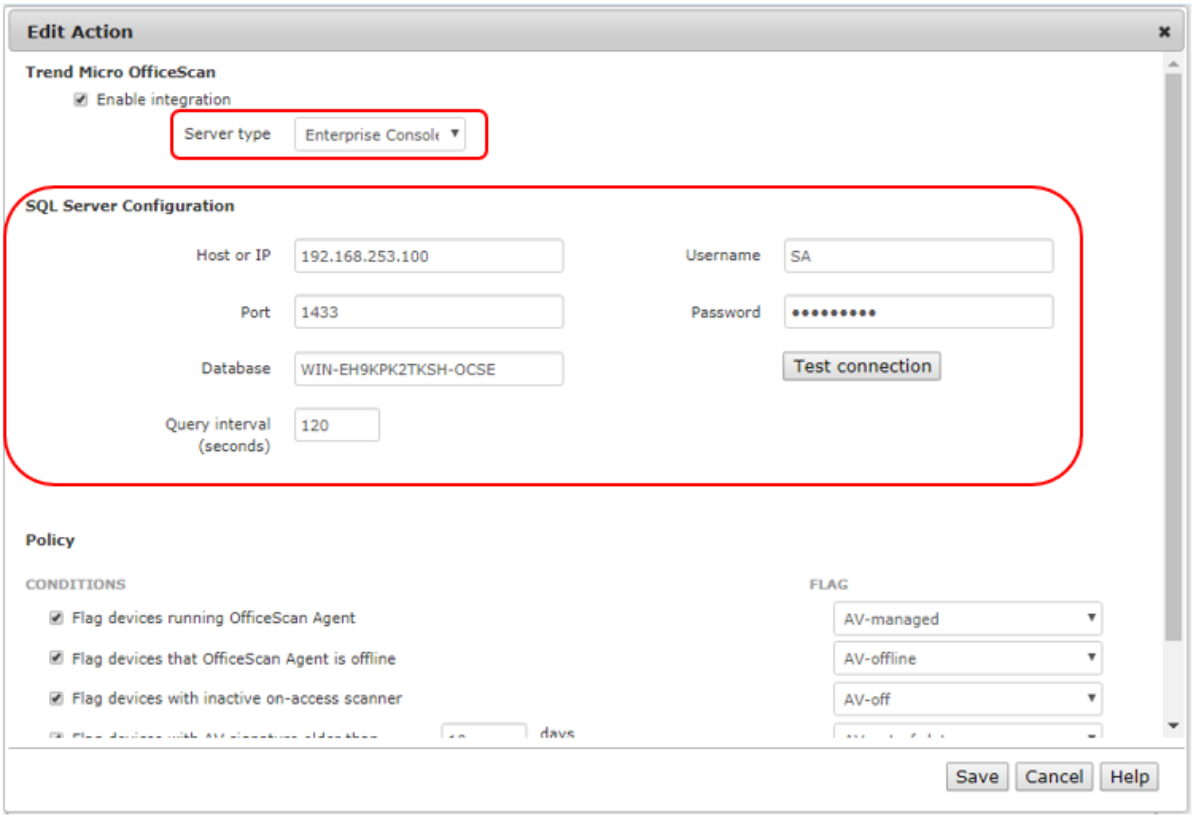
**Tip:** The AV-managed flag is helpful in expediting deployments. Any device that is being managed by the corporate AV server can automatically be granted access to the network.

# Trend Micro OfficeScan Integration

Easy NAC support 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 OfficeScan"
- Check "Enable integration" and select the "Enterprise Console" server type




CGX Access communicates with the Trend Micro Office Scan by querying the SQL database used by OSCE.

- Setup the SQL Server used by OCSE 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

**OCSE SQL Prerequisites:**

- By default, OCSE uses an internal database, called Codebase. For integration with CGX Access, it is required to use an SQL database. Trend Micro provides a migration tool to make this easy:

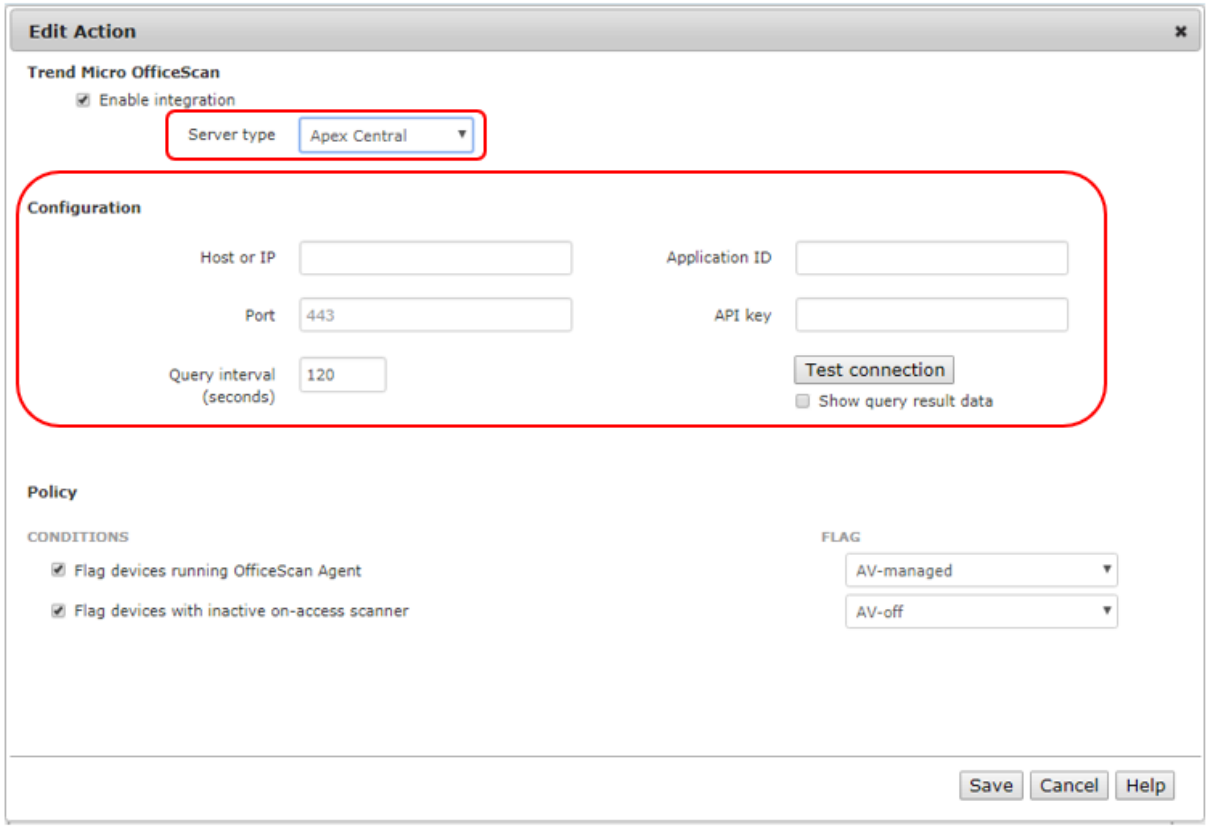
https://success.trendmicro.com/solution/1059973-migrating-officescan-osce-server-database-to-an-sql-server

- 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 OCSE 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 OCSE Server.

**Configuring APEX Central:**

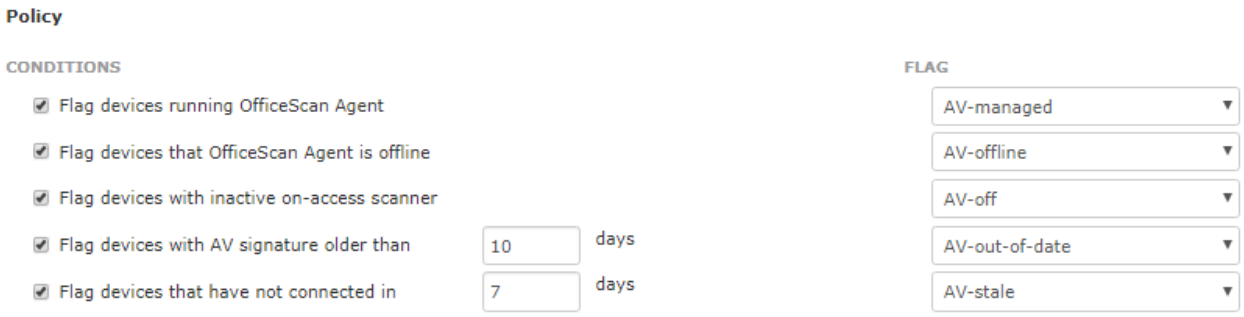
- In Apex Central, use Automation API Access Settings to generate an Application ID and API Key
- In CGX Access GUI go to Configuration → Integration
- Select Trend Micro
- Check "Enable integration" and select the "APEX Central"
- Add Host or IP address
- Copy the Application ID and API Key to CGX Access



## Setting and Enforcing Anti-Virus Compliance Policies

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

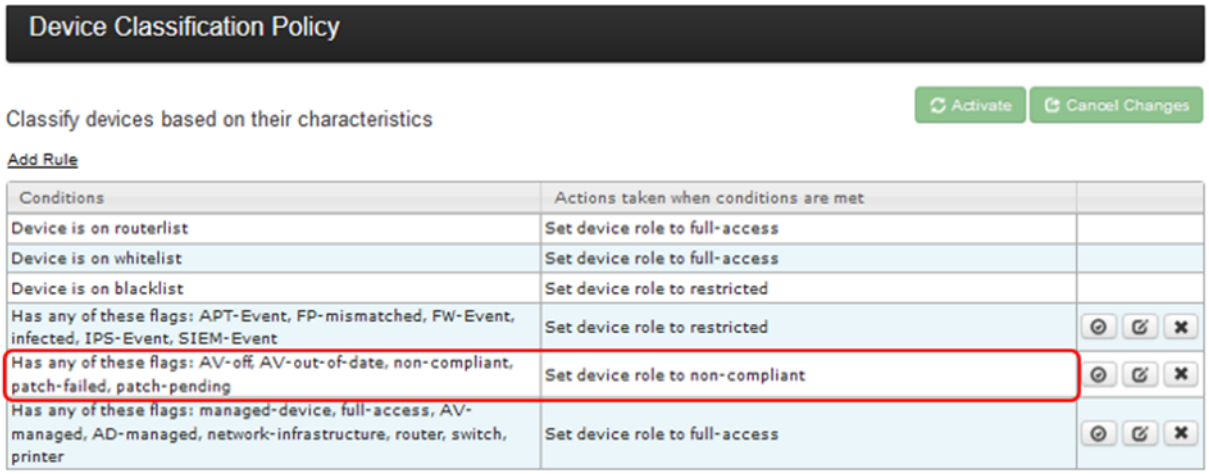
Select the flags that should be assigned to devices that meet or fail the specific conditions.




There are multiple conditions you can select to monitor. When selected CGX Access will set flags 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 Device & Role Classification policies, devices with specific flags can be assigned different roles.

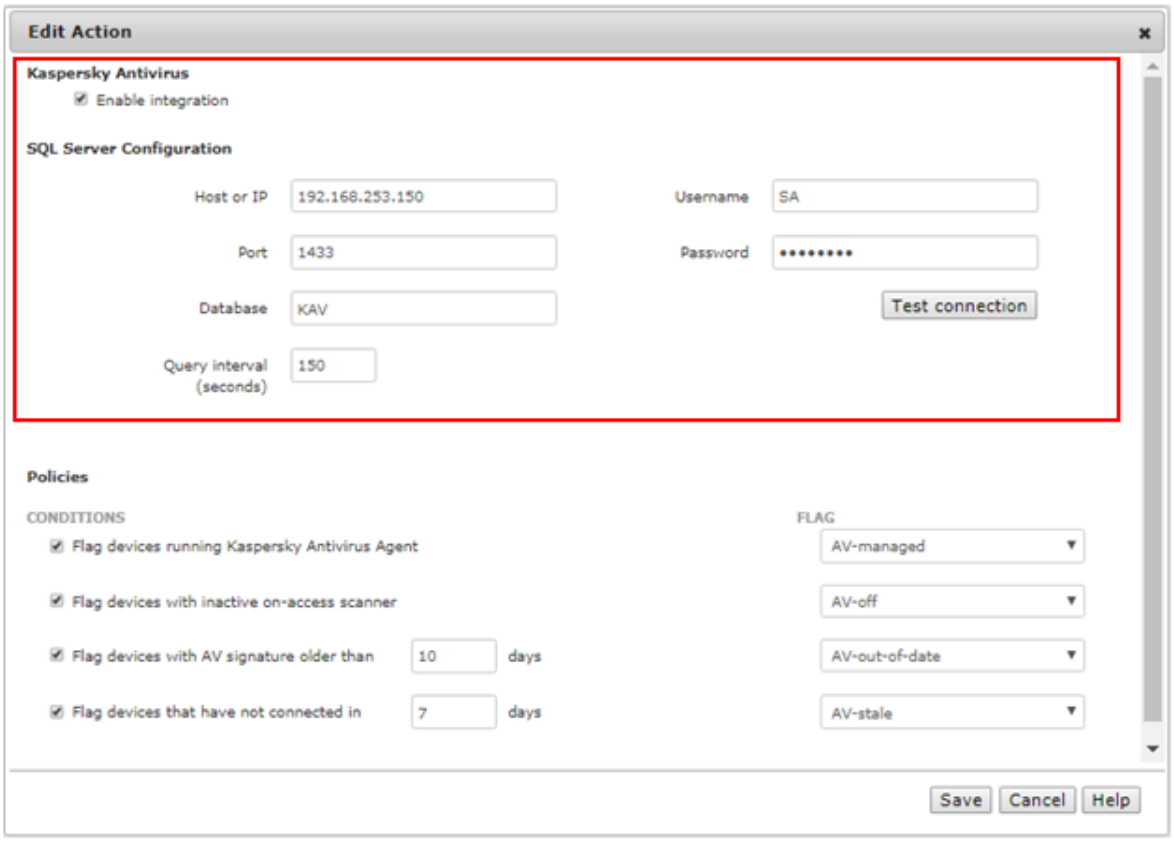



The example above shows a device will be assigned a non-compliant role if it has been flagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies, take precedence.

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

# Kaspersky Antivirus Integration

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




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:**

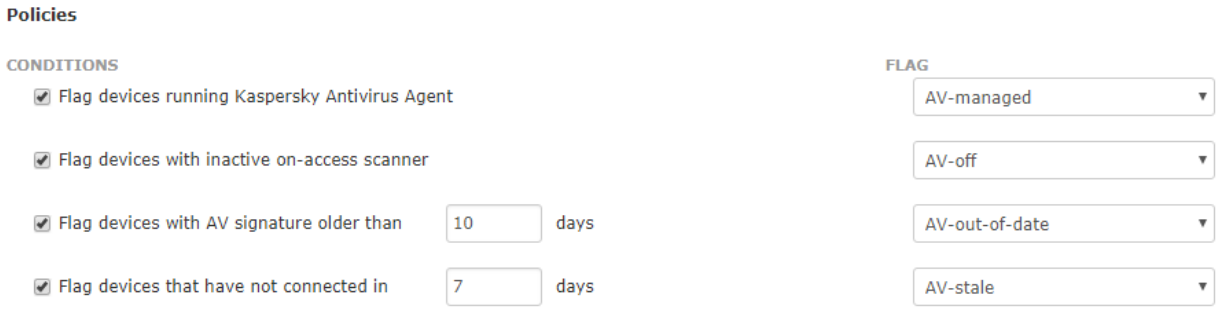
- Configure the MS SQL Server on the Administration Server to enable TCP/IP and specify a port such as 1433
- Use MS SQL Server management studio to create an account with permission to read the KAV database. KAV is the default database name used by Kaspersky.
- Configure the firewall on the Kaspersky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

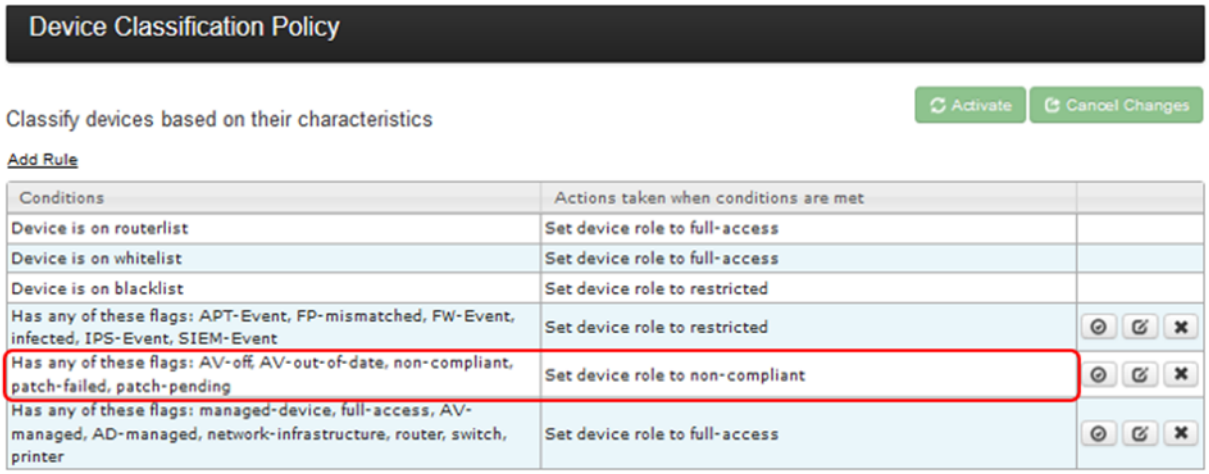
Once the communications between the CGX Access appliance and Kaspersky Administration Server have been successfully tested, policies can be set to enforce compliance with AV policies.

Select the flags 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 flags on specific devices that meet or fail the conditions.

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.

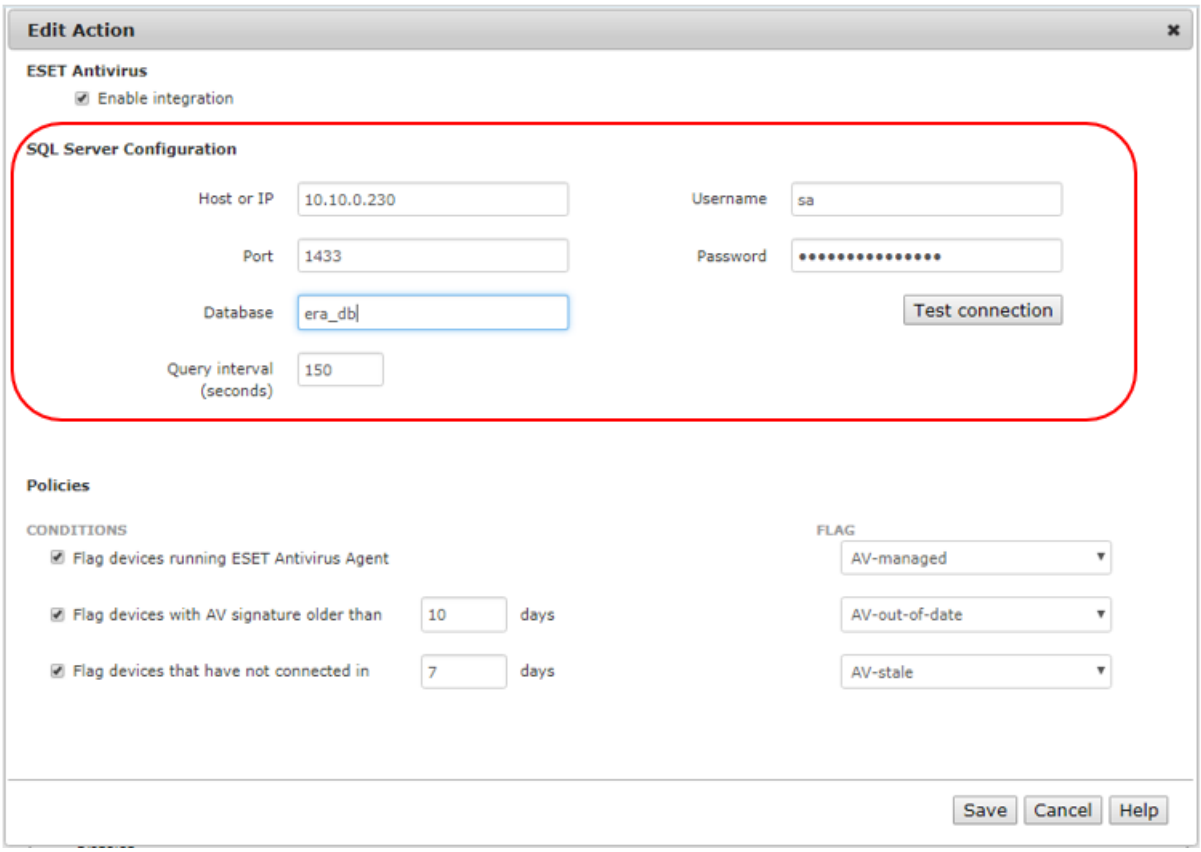



The example above shows a device will be assigned a non-compliant role if it has been flagged as AV-off or AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies, take precedence.

**Tip:** The AV-managed flag 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”




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:**

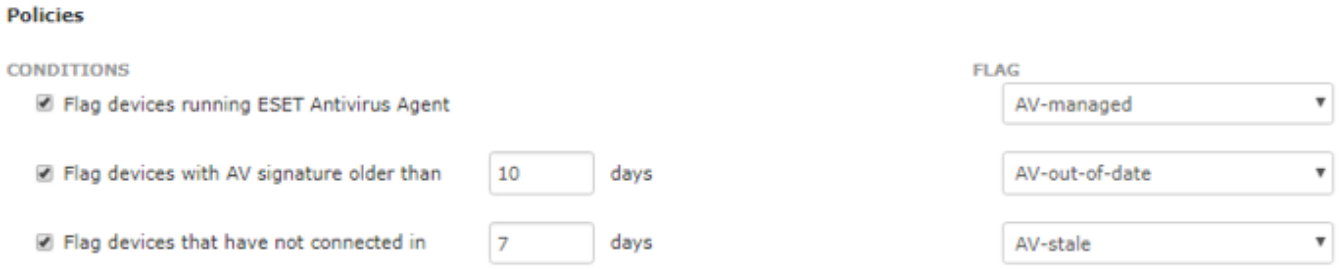
- Configure the MS SQL Server on the Administration Server to enable TCP/IP and specify a port such as 1433
- Use MS SQL Server management studio to create an account with permission to read the era_db database. The default database name use by ESET is era_db.
- Configure the firewall on the ESMC to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

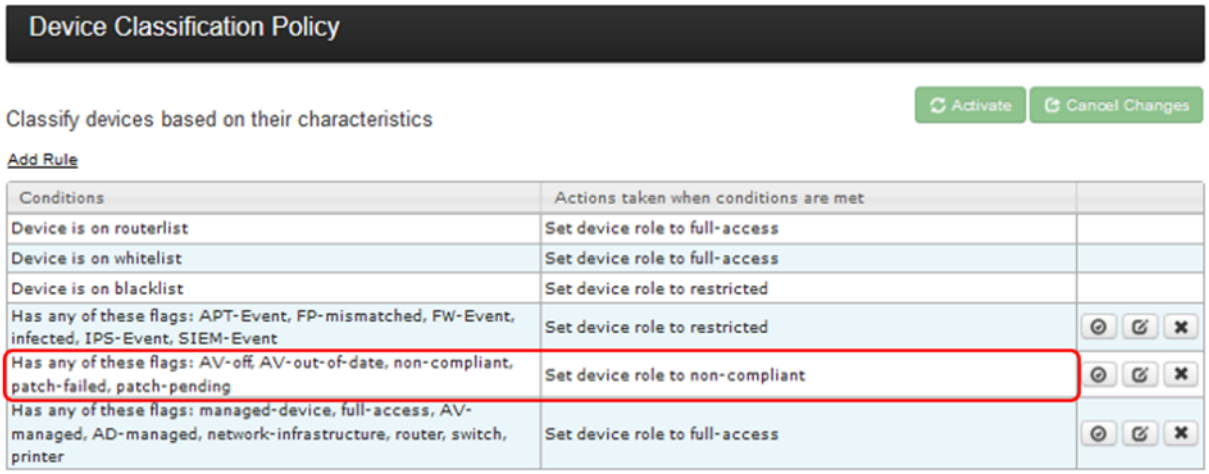
Once the communications between the CGX Access appliance and ESET Security Management Console have been successfully tested, policies can be set to enforce compliance with AV policies.

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




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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.



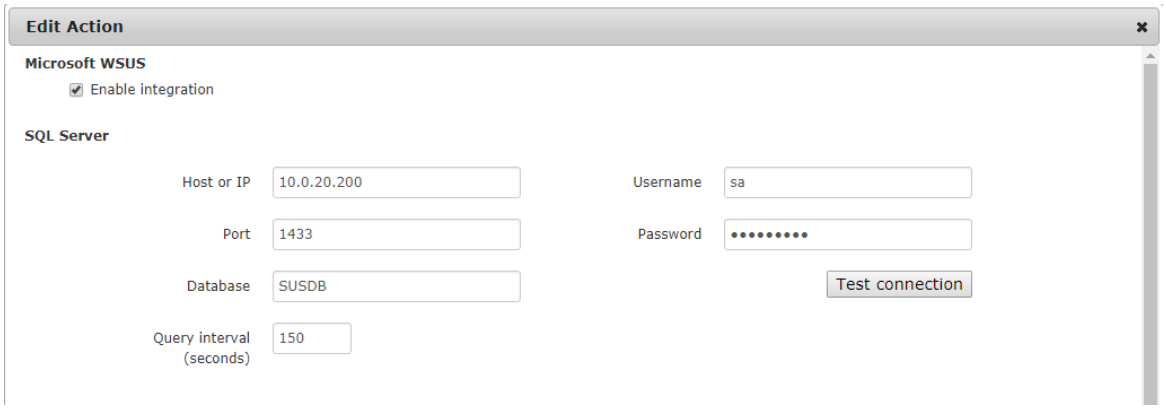

The example above shows a device will be assigned a non-compliant role if it has been flagged as AV-out-of-date. The placements of the rules are important and are evaluated top-down. The first rule that applies takes precedence.

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

# 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:**

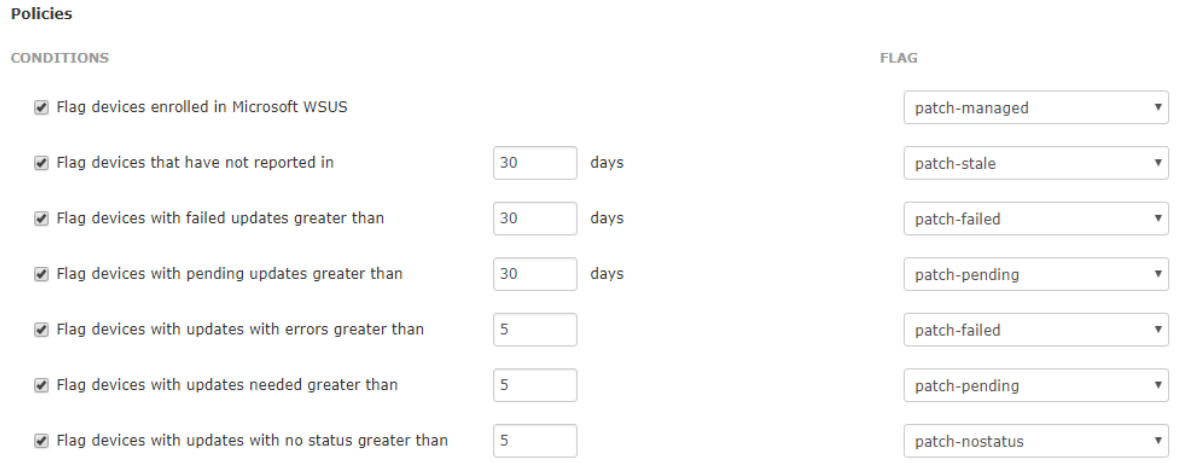
- By default, WSUS uses the Windows Internal Database. For integration with CGX Access, it is required to use an SQL database.
- Verify the MS SQL Server on the WSUS server was enabled for TCP/IP and specify a port such as 1433.
- Configure the firewall on the WSUS server to allow CGX Access to communicate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

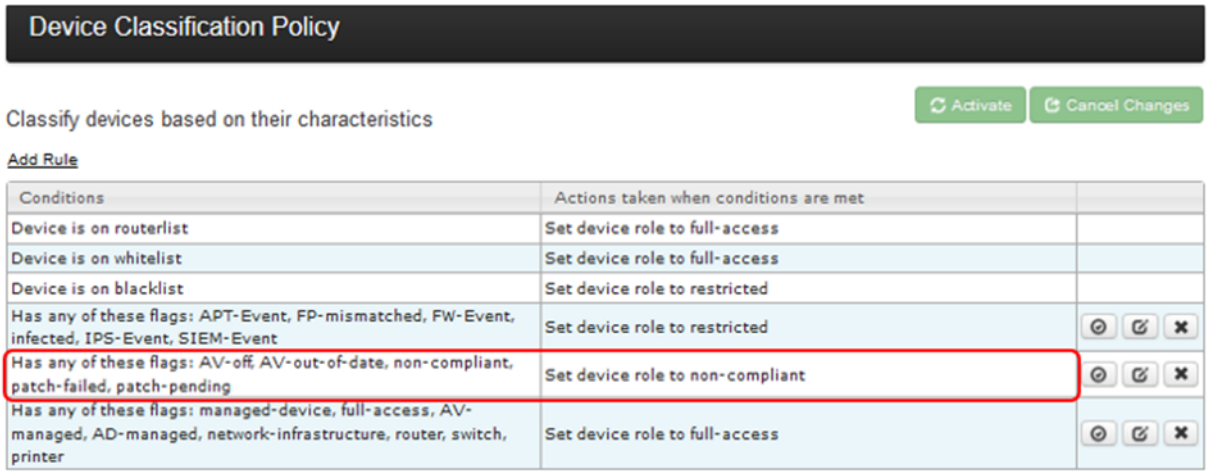
Once the communications between the CGX Access appliance and WSUS server have been successfully tested, policies can be set to enforce compliance with patch policies.

Select the flags 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 flags on specific devices that meet or fail the conditions.

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.



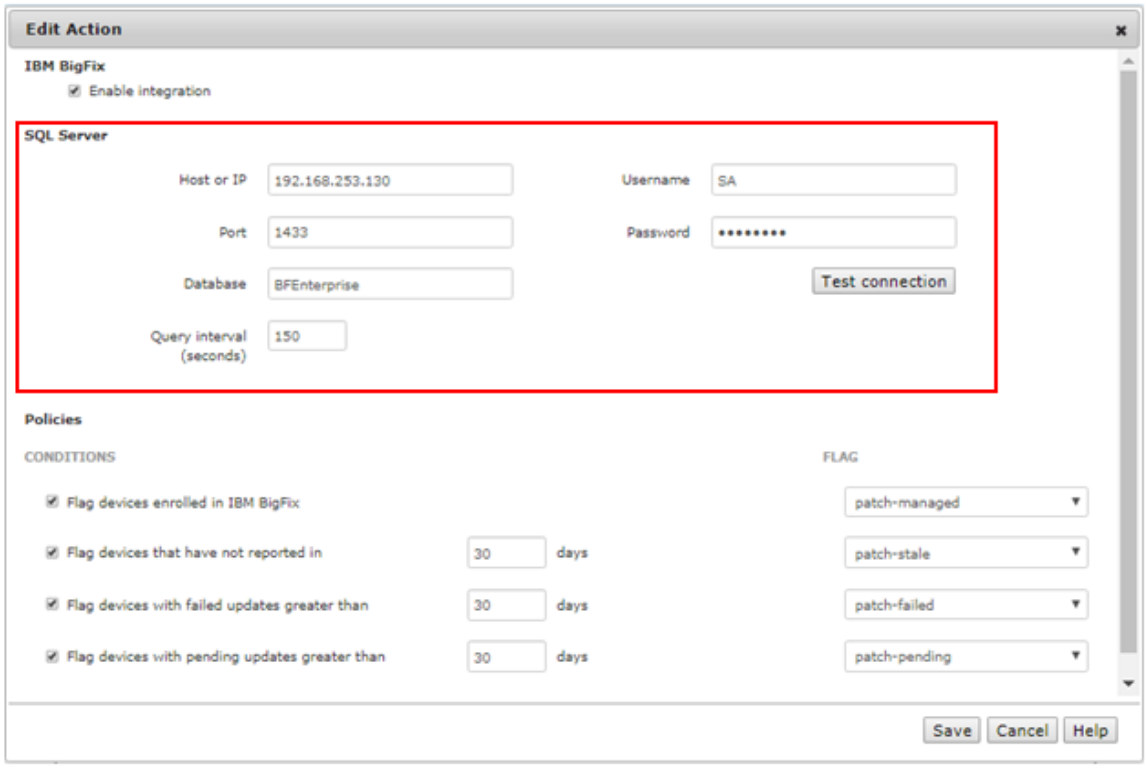

The policy above shows a device will be assigned a non-compliant role if it has been flagged as patch-pending or patch-failed. The order of the rules is important, as they are evaluated is descending order.

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

# IBM BigFix Integration

In CGX Access GUI go to Configuration → Integration

- Select “IBM BigFix”




- 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:**

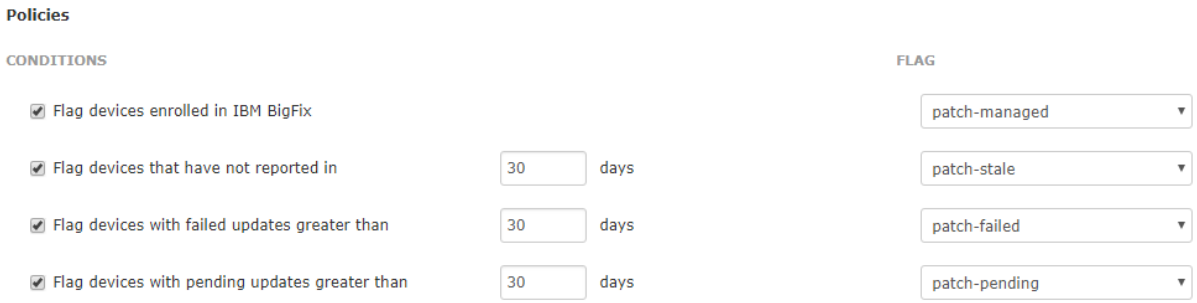
- Verify the MS SQL Server on the BigFix server was enabled for TCP/IP and specify a port such as 1433.
- Use MS SQL Server management studio to create an account with permission to read the BFEnterprise database. BFEnterprise is the default database name used by BigFix.
- Configure the firewall on the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

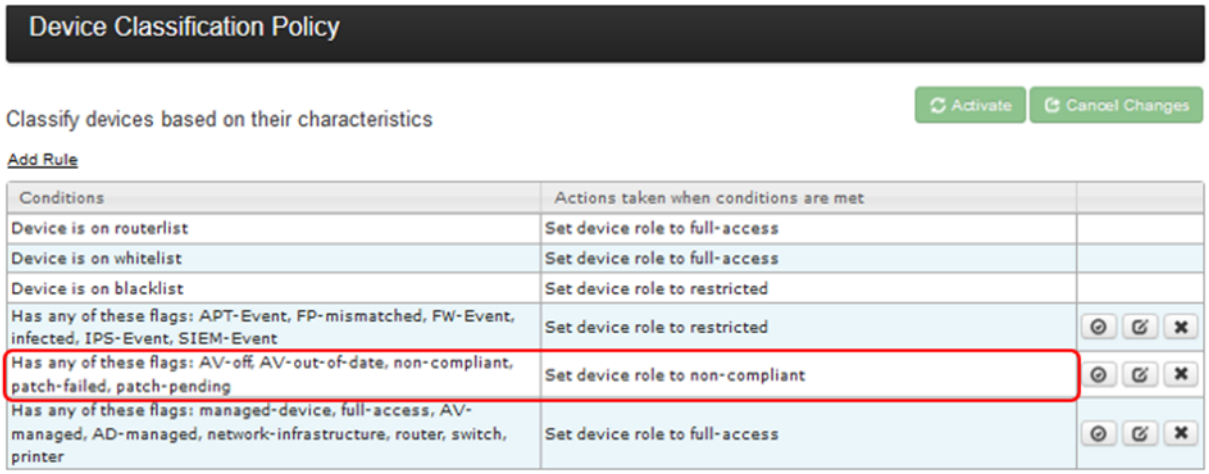
Once the communications between the CGX Access appliance and BigFix server have been successfully tested, policies can be set to enforce compliance with patch policies.

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




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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.

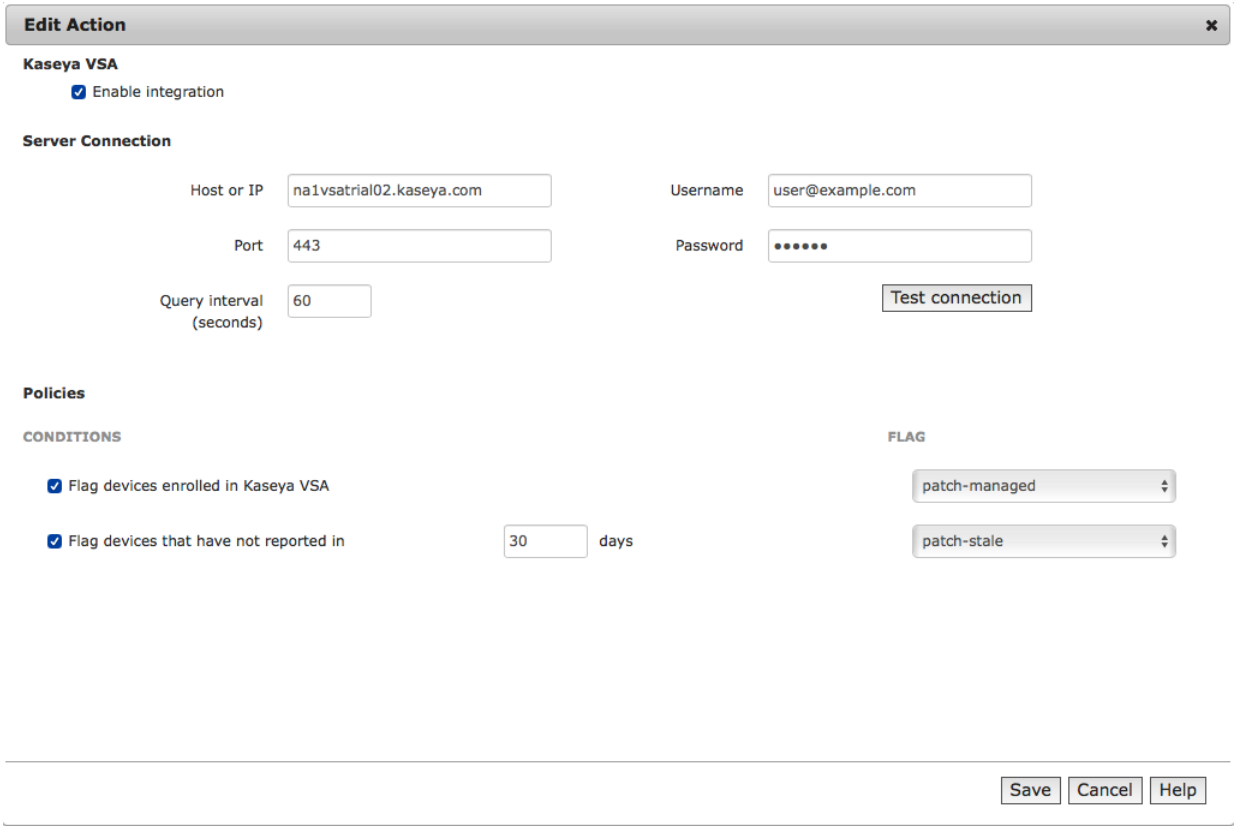



The policy above shows a device will be assigned a non-compliant role if it has been flagged as patch-pending or patch-failed. The order of the rules is important, as they are evaluated is descending order.

**Tip:** The patch-managed flag is helpful in expediting deployments. Any device that is being managed by the BigFix server 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

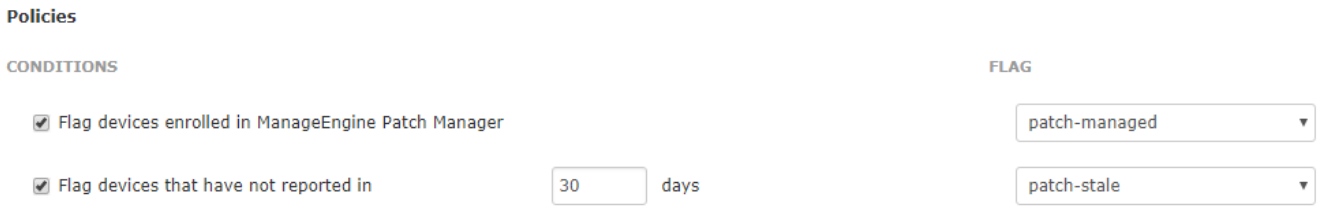



- Use "Test connection" button to validate settings
- You may leave Query interval and flagging conditions as default or modify as required
- Save this configuration

## Setting and Enforcing Patch Compliance Policies

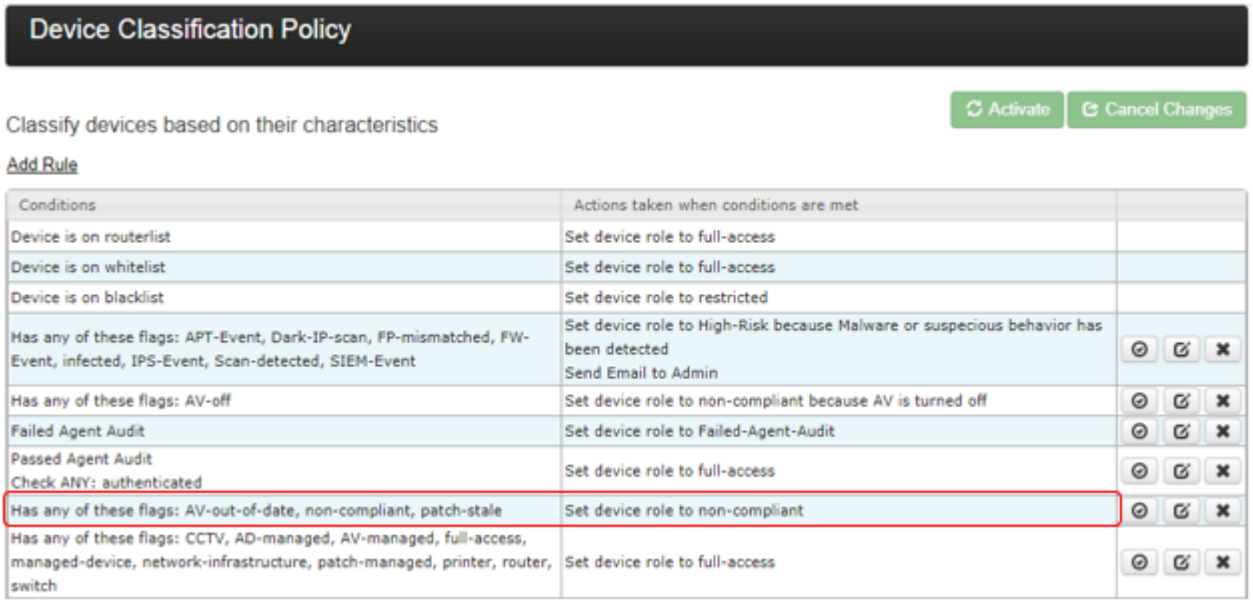
Once the communications between the CGX Access appliance and Kaseya VSA server have been successfully tested, policies can be set to enforce compliance with patch policies.

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




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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.

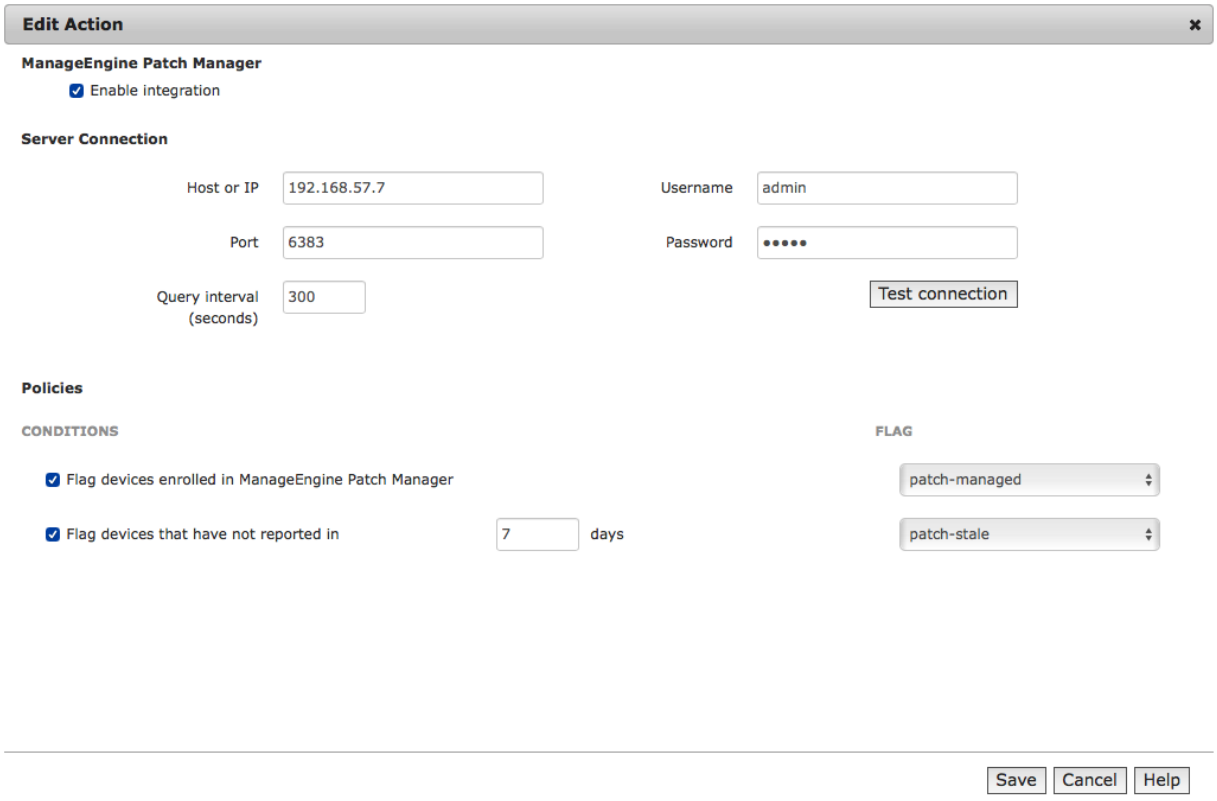



The policy above shows a device will be assigned a non-compliant role if it has been flagged as patch-stale. The order of the rules is important, as they are evaluated is descending order.

**Tip:** The patch-managed flag is helpful in expediting deployments. Any device that is being managed by Kaseya VSA 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”
- Enter Hostname or IP / port
- Enter Username / Password to login to ManageEngine

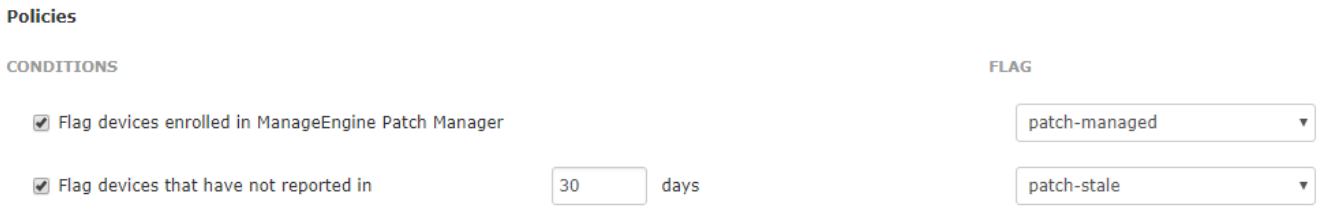



- Use "Test connection" button to validate settings
- You may leave Query interval and flagging conditions as default or modify as required
- Save this configuration

## Setting and Enforcing Patch Compliance Policies

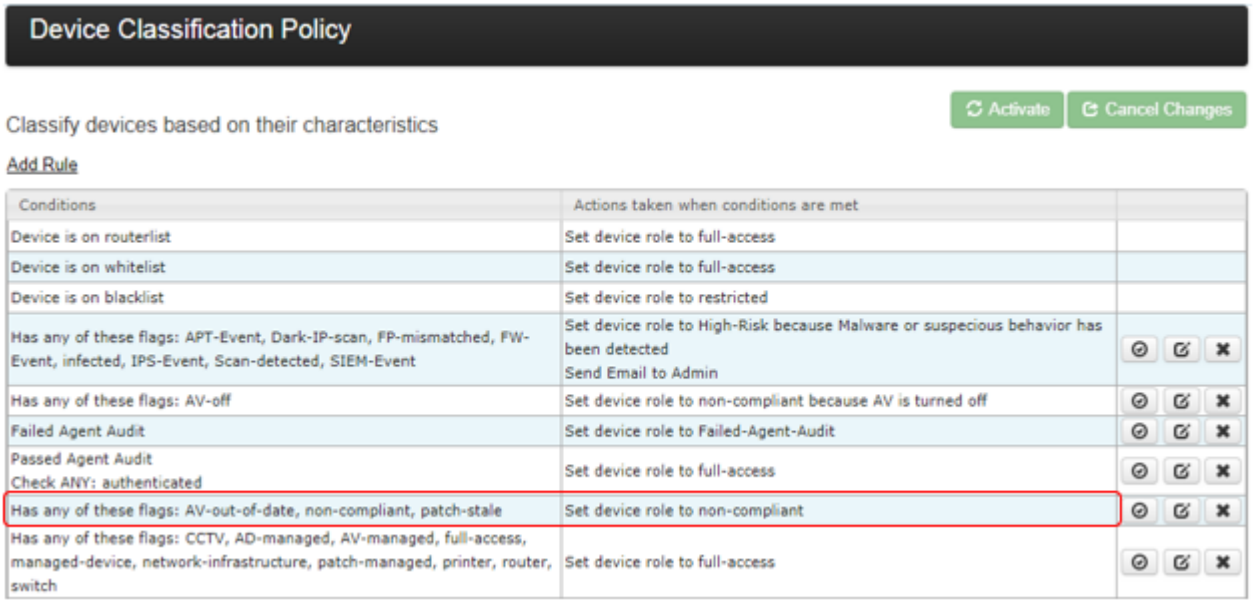
Once the communications between the CGX Access appliance and ManageEngine server have been successfully tested, policies can be set to enforce compliance with patch policies.

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




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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.



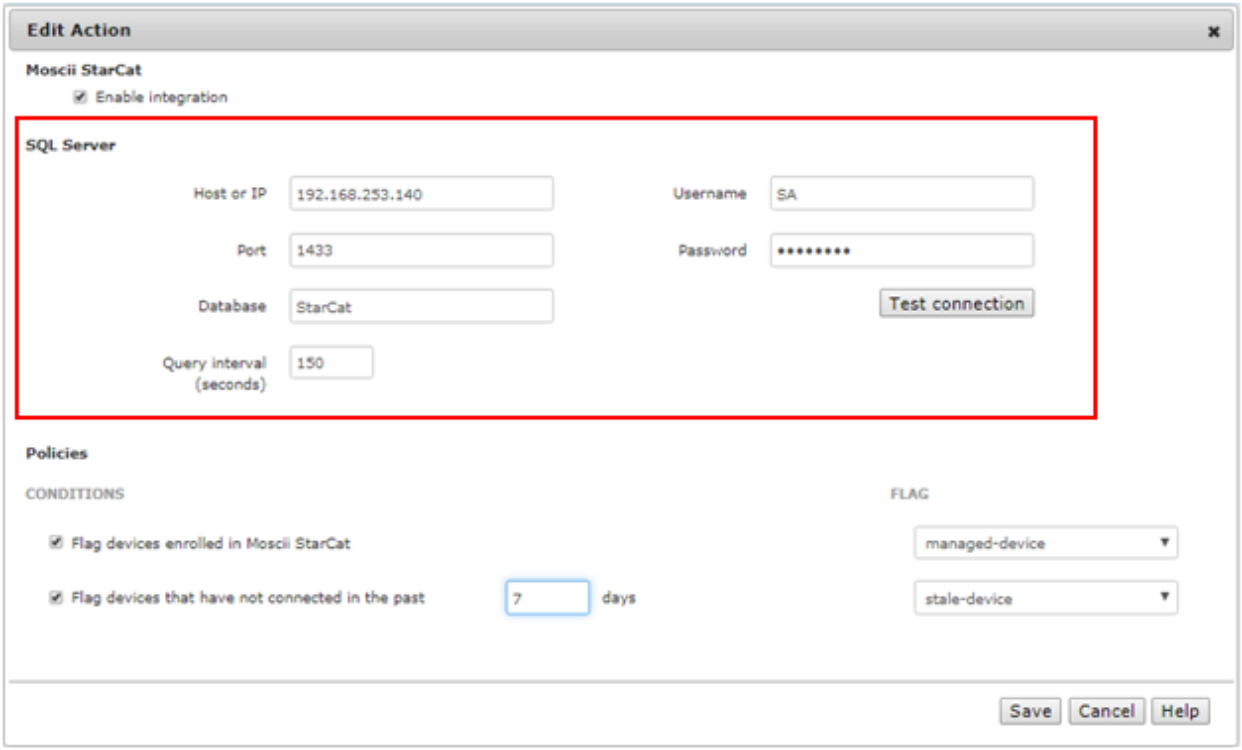

The policy above shows a device will be assigned a non-compliant role if it has been flagged as patch-stale. The order of the rules is important, as they are evaluated is descending order.

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

# Moscii StarCat Integration

In CGX Access GUI go to Configuration → Integration

- Select “Moscii StarCat”




- 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:**

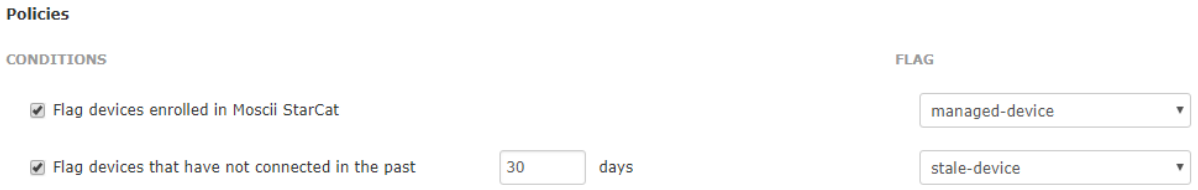
- Verify the MS SQL Server on the StarCat server was enabled for TCP/IP and specify a port such as 1433.
- Use MS SQL Server management studio to create an account with permission to read the StarCat database. StarCat 2013 doesn’t use a default database name, so check the SQL server for the correct name.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

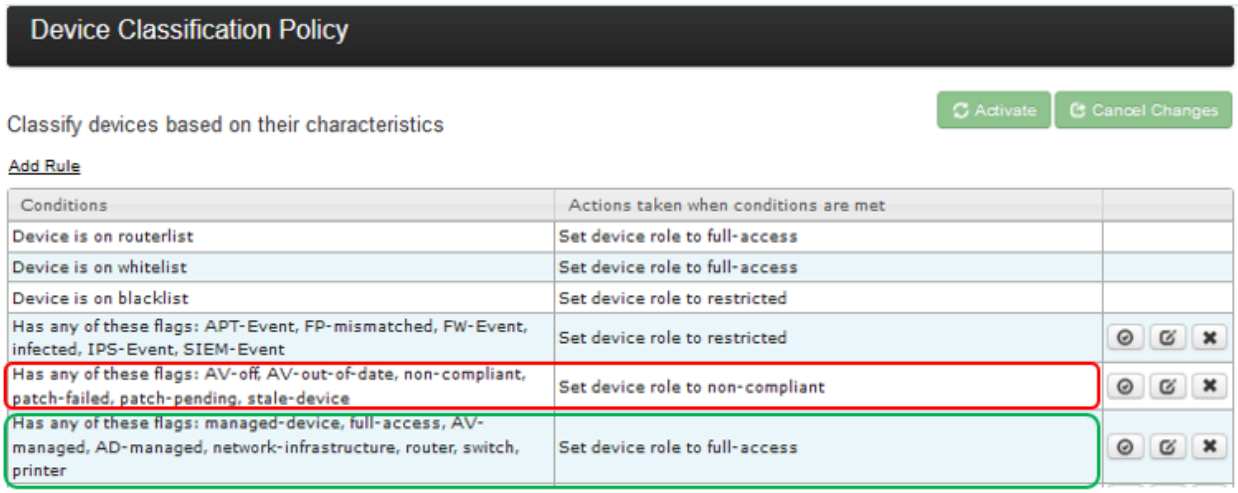
Once the communications between the CGX Access appliance and StarCat server have been successfully tested, policies can be set to enforce all Windows devices have been installed with the StarCat agent and connecting to the server regularly.

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




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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.

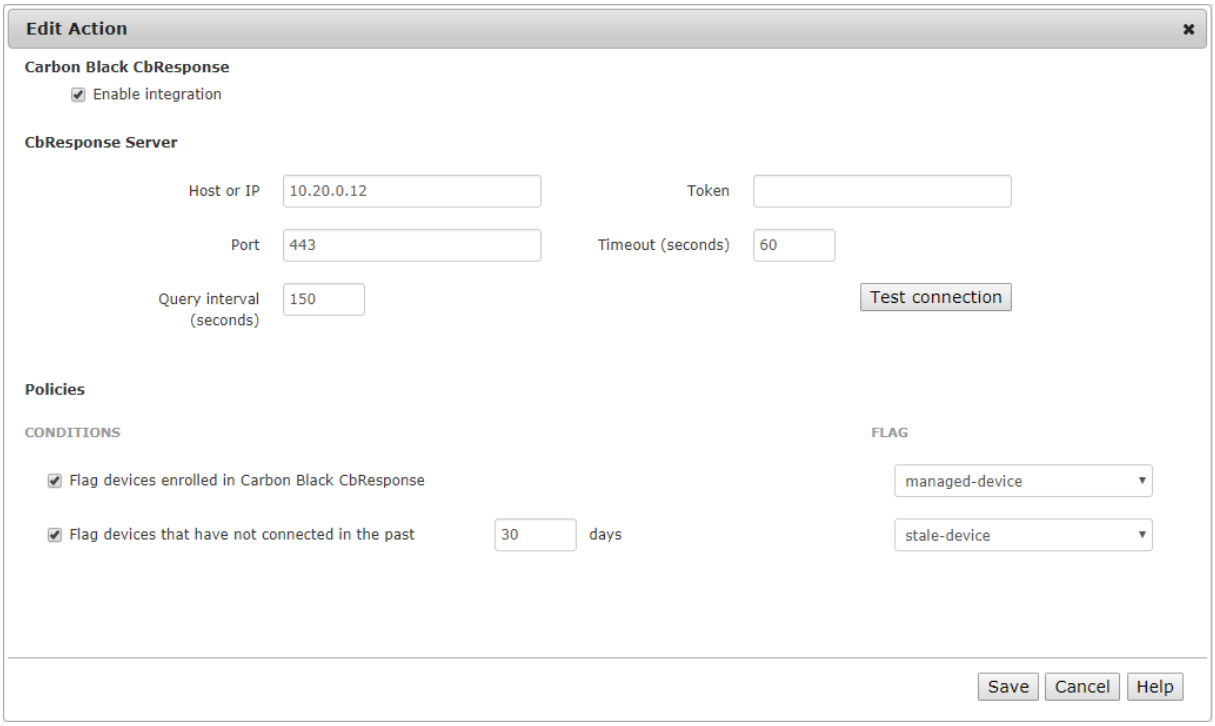



The policy above shows a device will be assigned full-access if flagged as managed-device. However, it would be given a non-compliant role if it has been flagged as a stale-device. The order of the rules is important, as they are evaluated is descending order.

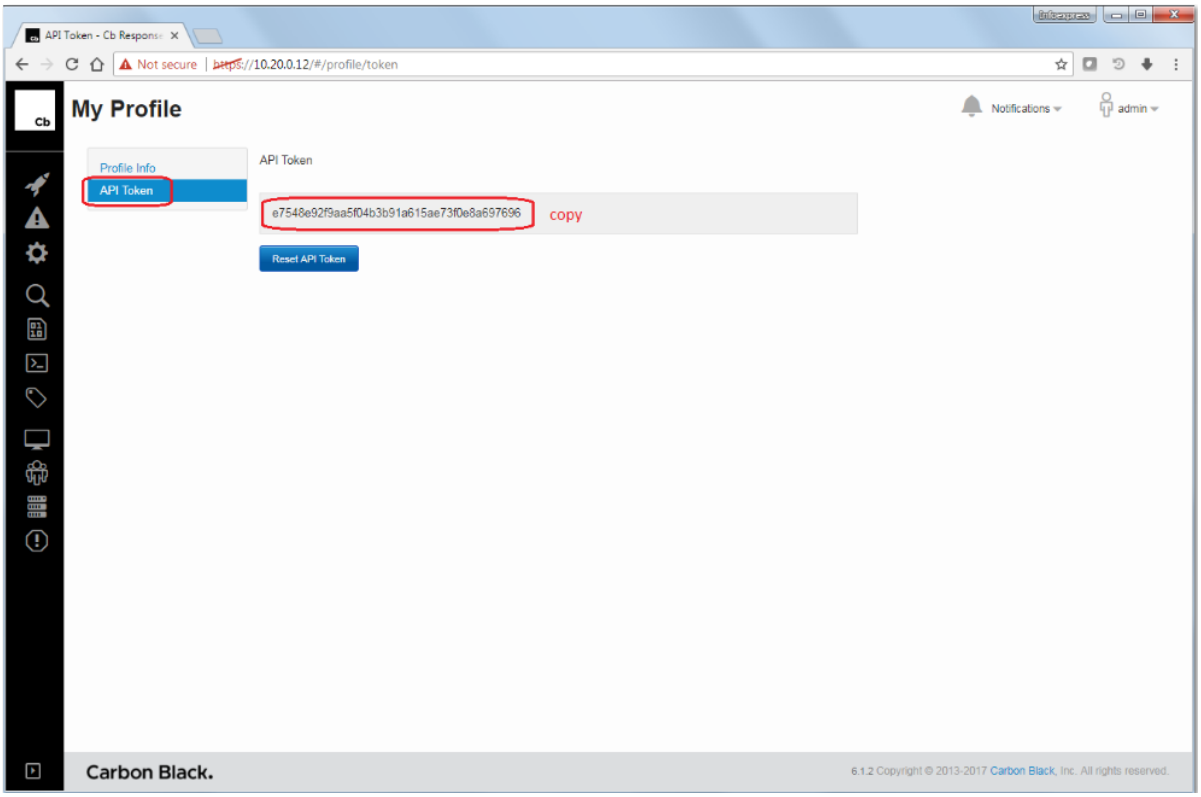
**Tip:** The managed-device flag is helpful in expediting deployments. Any device that is being managed by the StarCat server can automatically be granted access to the network.

# Carbon Black Cb Response Integration

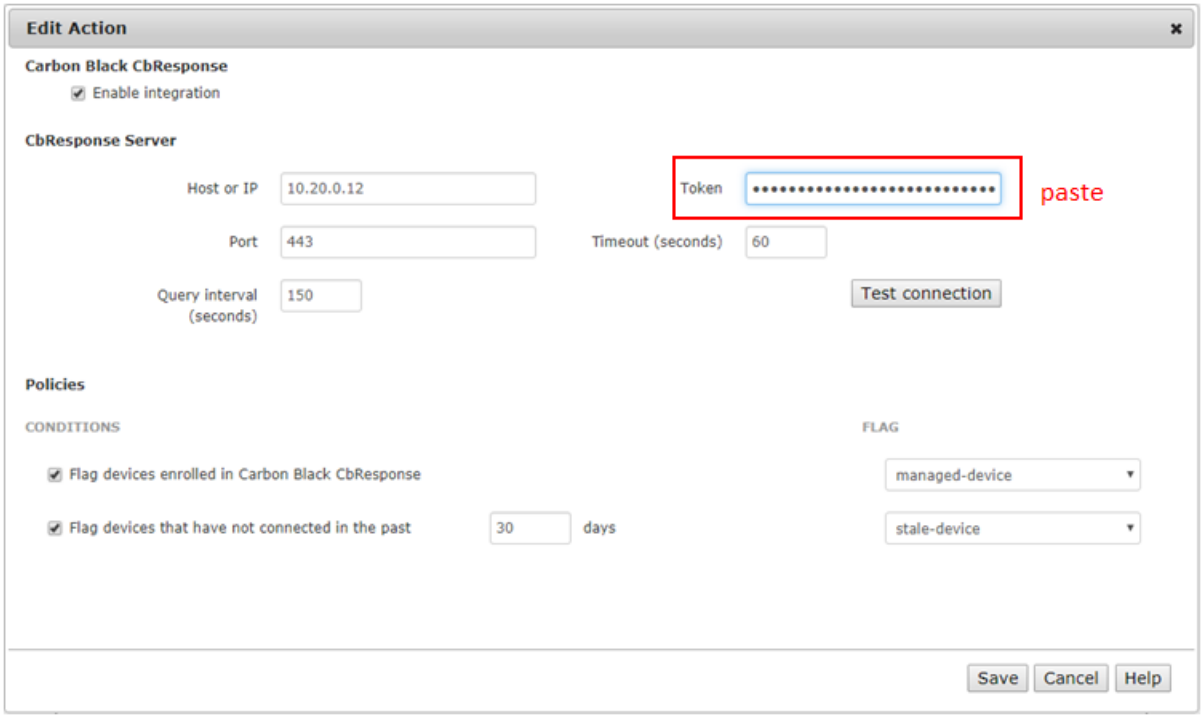
- In CGX Access GUI go to Configuration → Integration
- Click on "Carcon Black Cb Response"




- Check “Enable Integration”
- Enter Hostname or IP / port
- In Cb Response console go to Admin→ My Profile → API Token




- Copy API Token and Paste into Token field

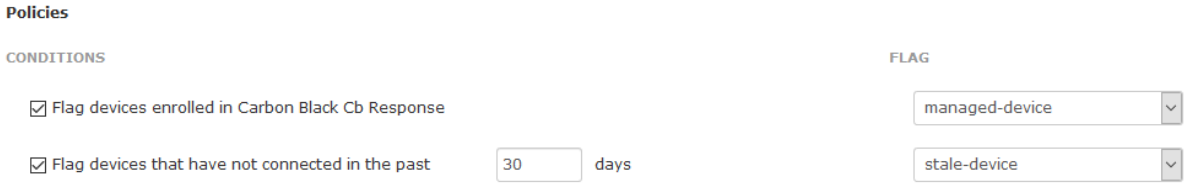



- Use "Test connection" button to validate settings and connectivity

**Setting and Enforcing Compliance Policies**

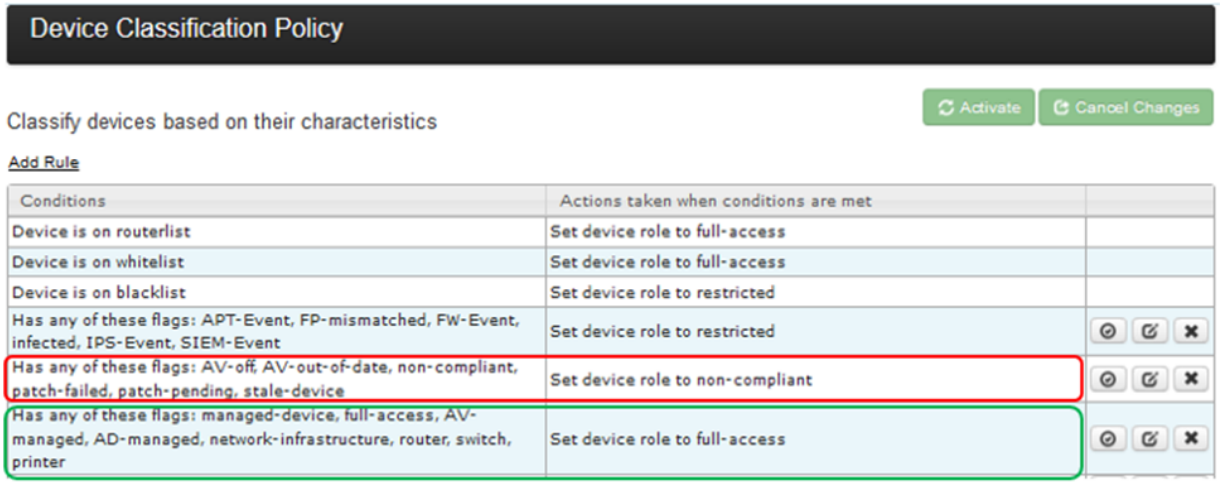
Once the communications between the CGX Access appliance and Cb Response server have been successfully tested, policies can be set to enforce endpoint devices have been installed with the Cb Response agent and connecting to the server regularly.

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




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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.




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

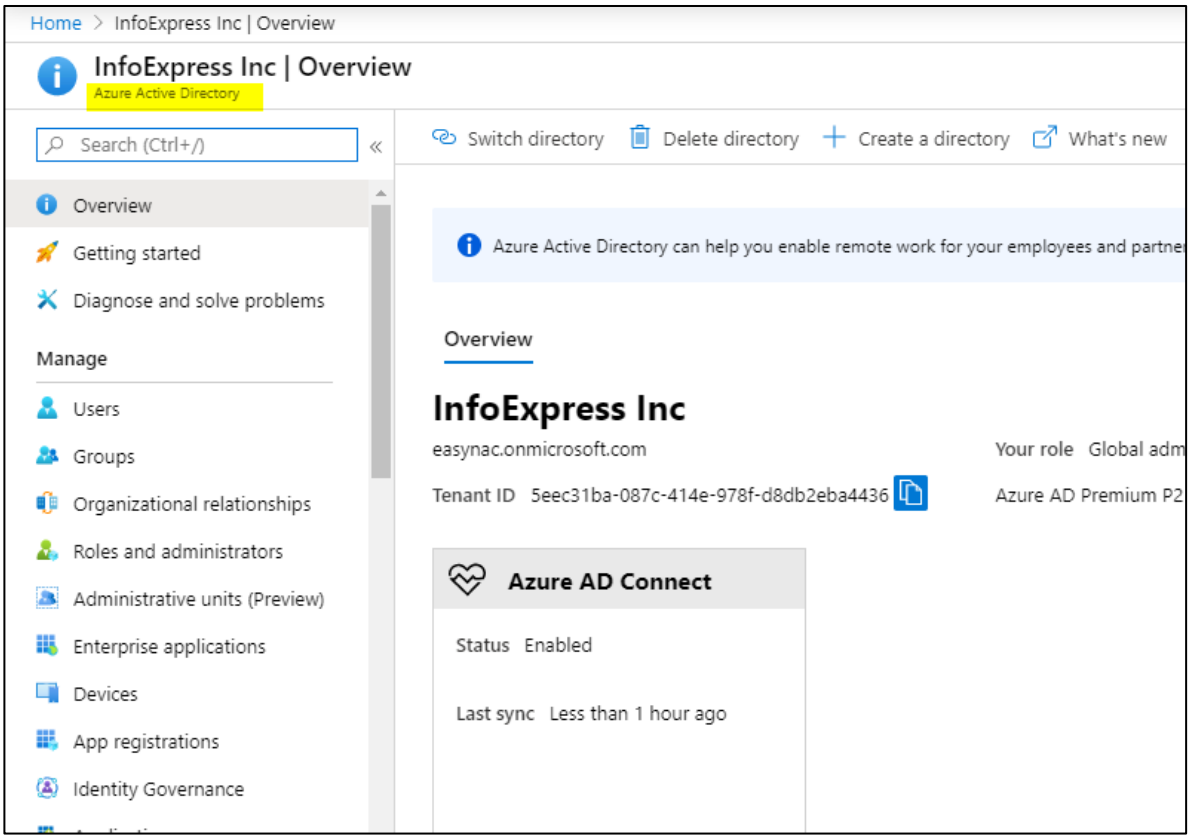
**Tip:** The managed-device flag is helpful in expediting deployments. Any device that is being protected by the Carbon Black will automatically be granted access to the network.

# Microsoft Intune Integration

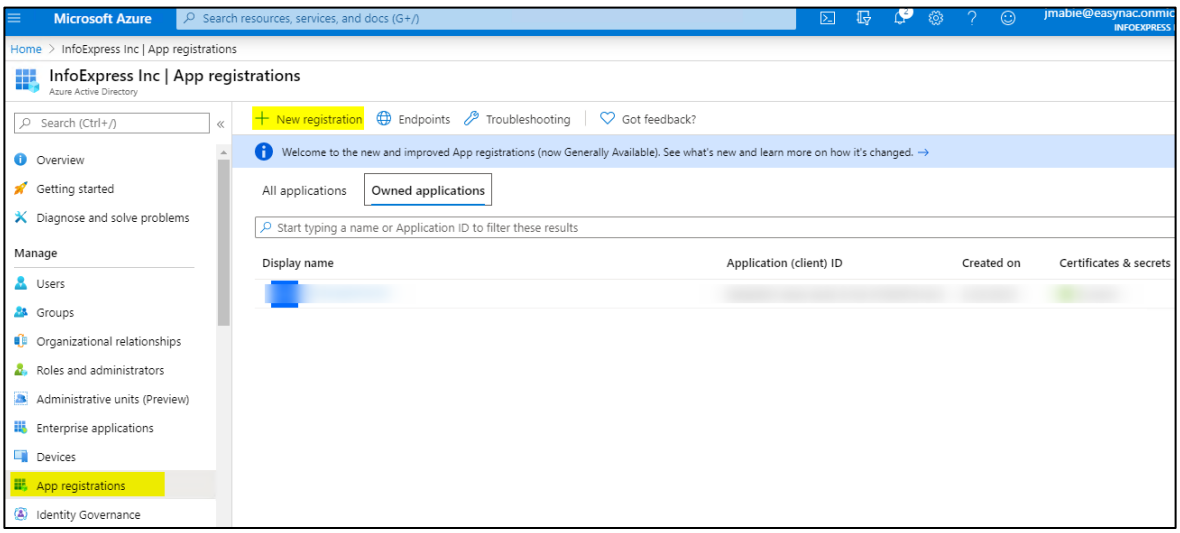
Integration with MS Intune requires an application be registered in MS Azure.

**Step 1: Register a new application in Azure directory**

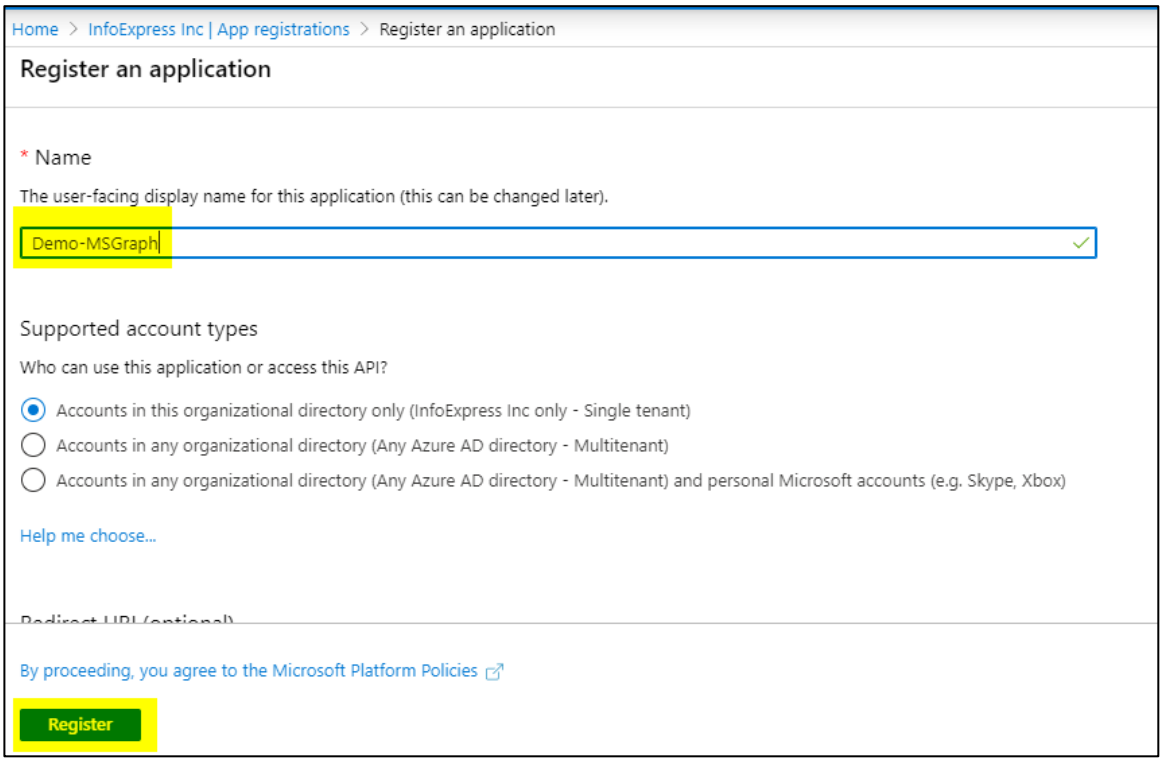
- Go to Azure Directory → App registration → New registration (Screen 1, 2 & 3)



Screen-1

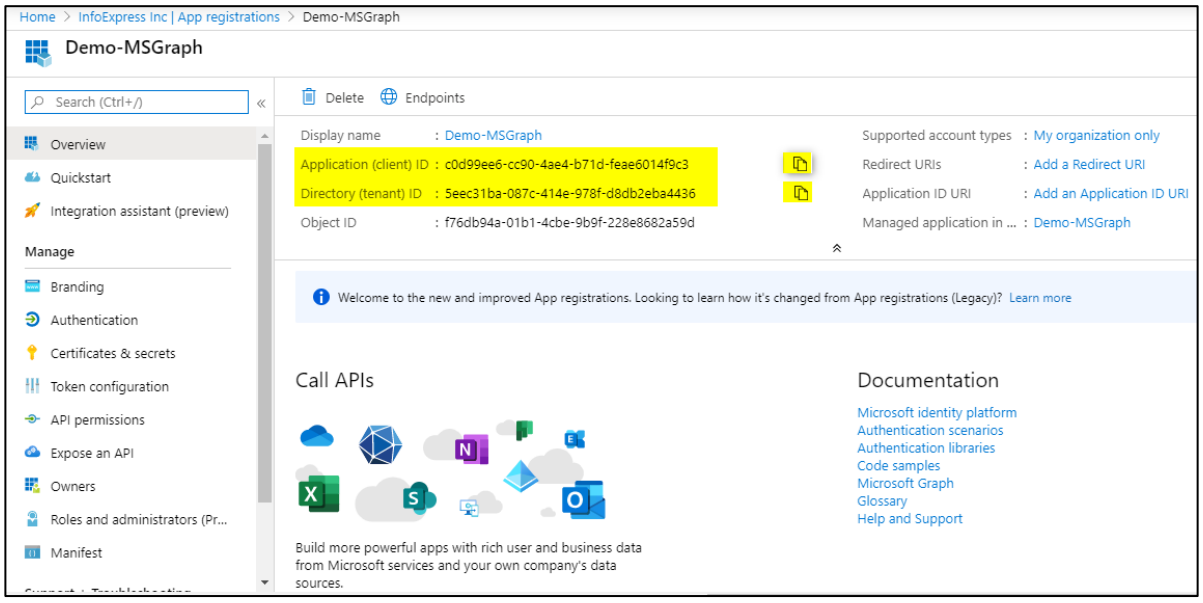


Screen-2

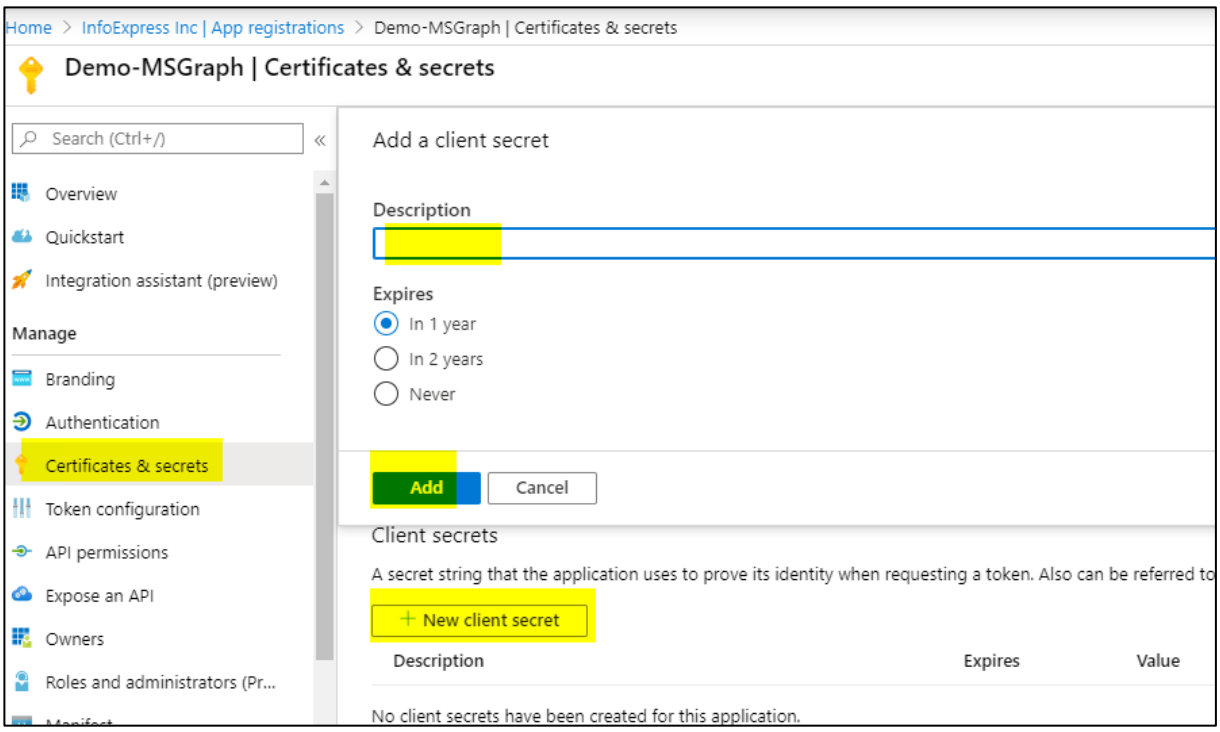



Screen-3

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



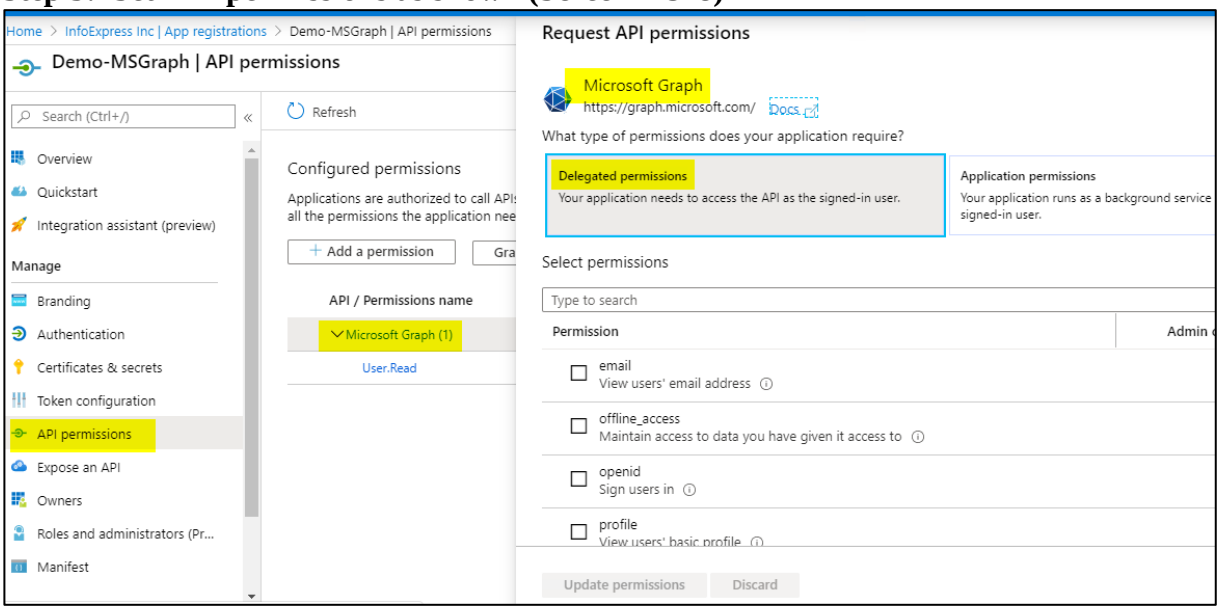

Screen-4




Screen-5

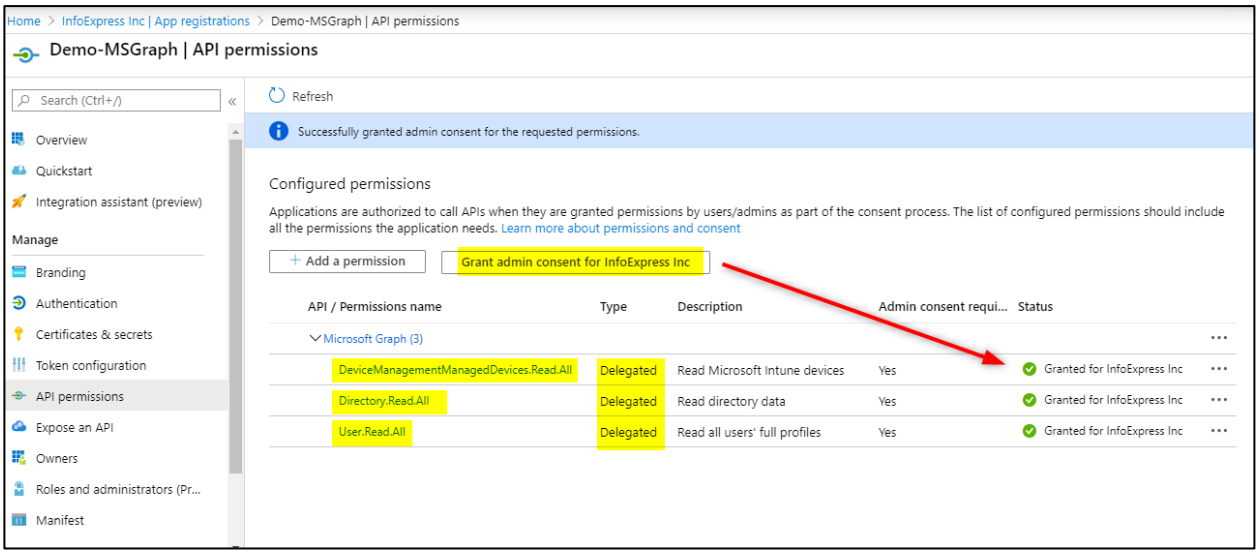

Screen-6

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




Screen-7

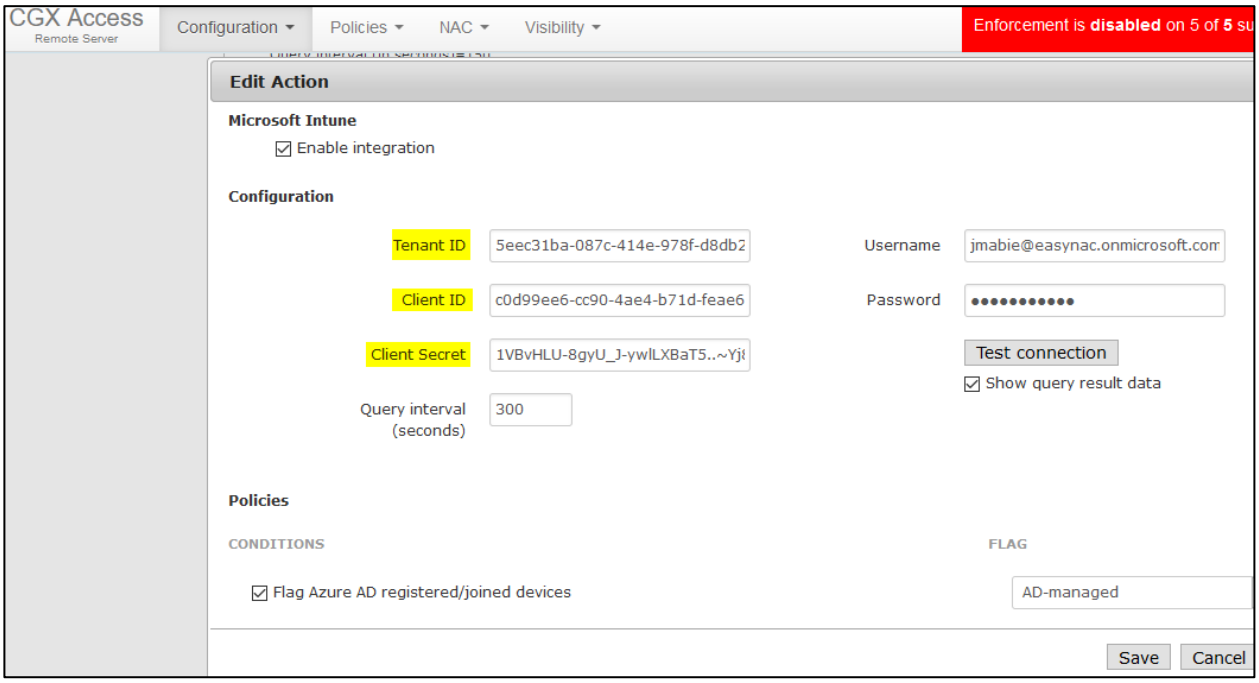
- Ensure permission name, type and Admin consent is granted for each permission



Screen-8

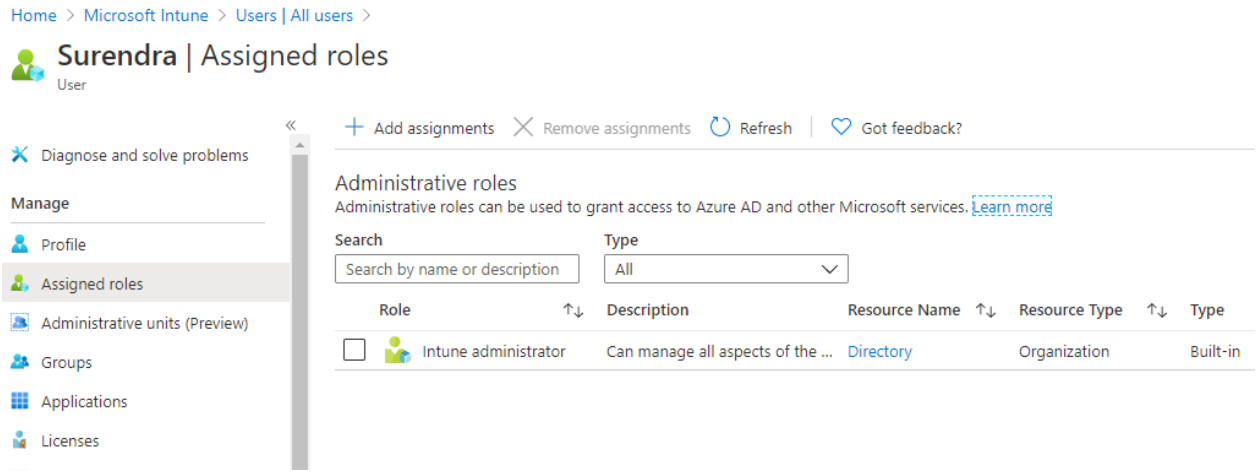
**Step 4: Go to CGX Access → Configuration → Integration →Microsoft Intune.**

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



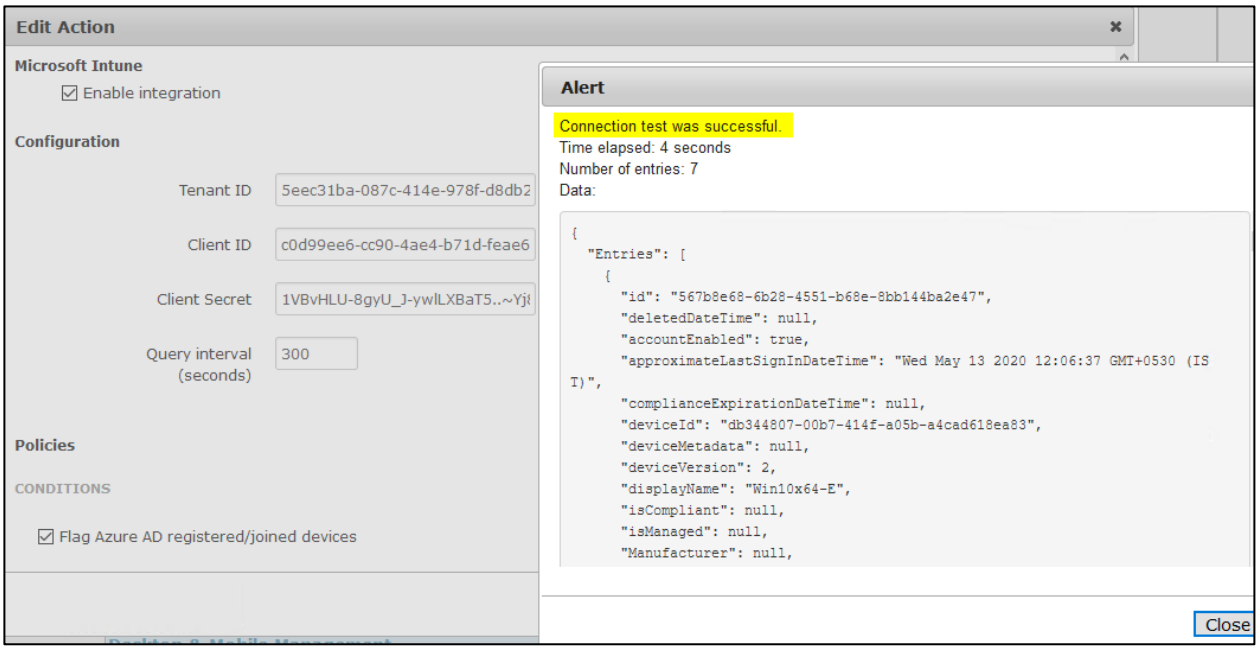
Screen-9

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




Screen-10

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




Screen-11

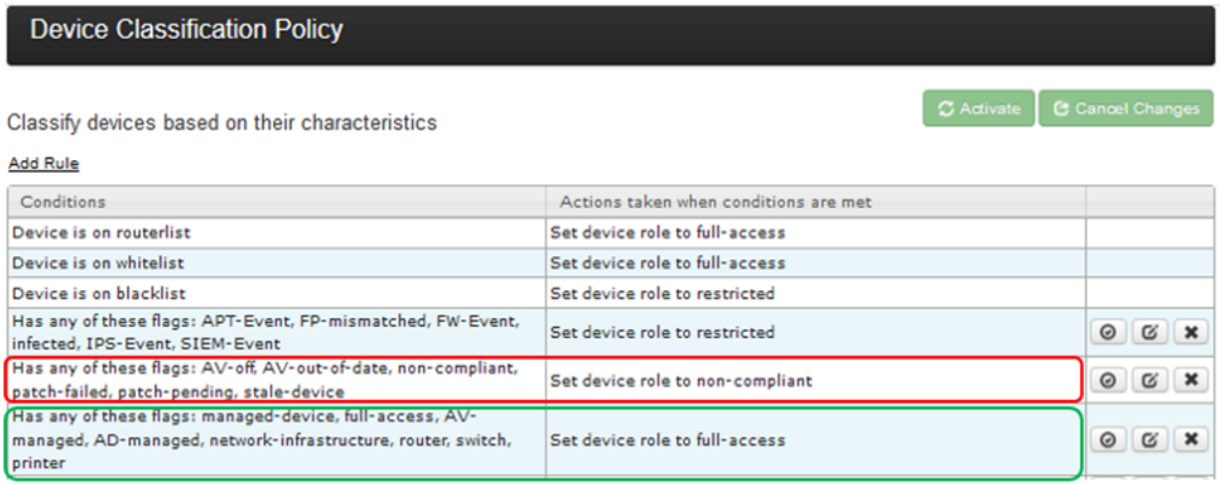
**Setting and Enforcing Compliance Policies**

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


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

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.



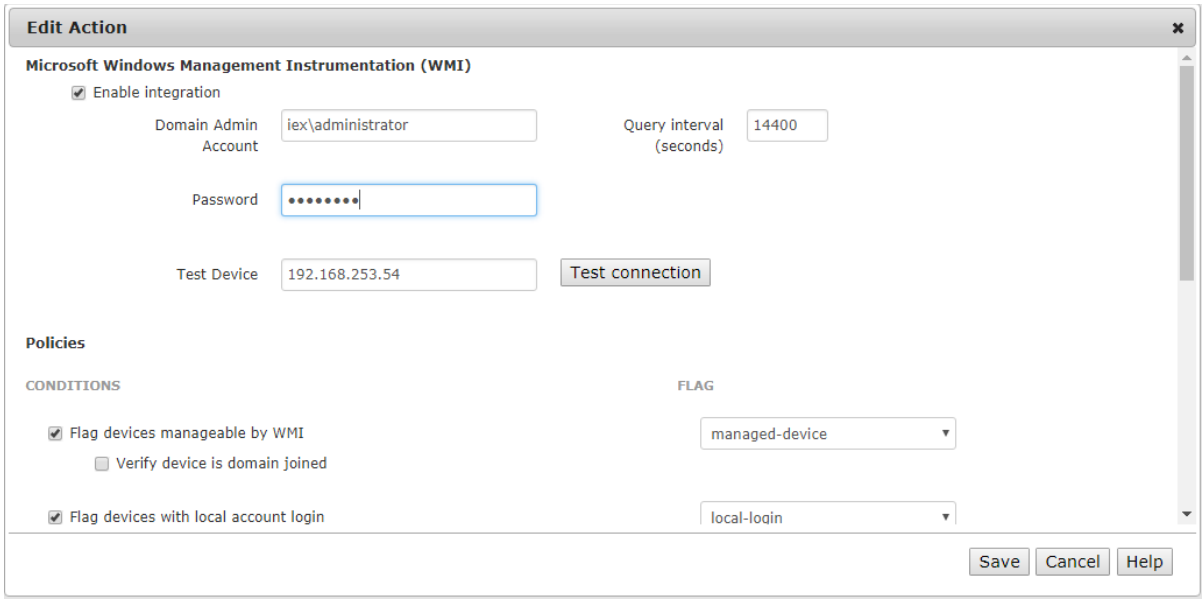

The policy above shows a device will be assigned full-access if flagged as AD-Managed or managed-device. However, it would be given a non-compliant role if it has been flagged as a non-compliant. The order of the rules is important, as they are evaluated is descending order.

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

# 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.

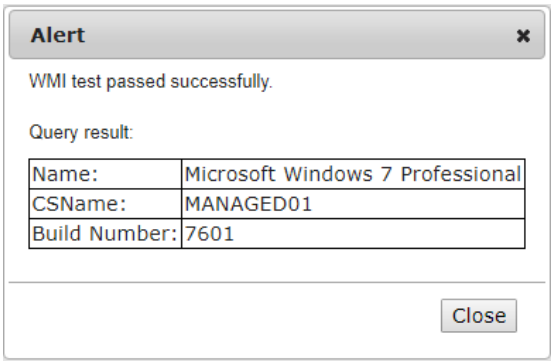
- In CGX Access GUI go to Configuration → Integration
- Select the “Microsoft WMI”




- 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




- Save changes

**WMI Troubleshooting:**

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

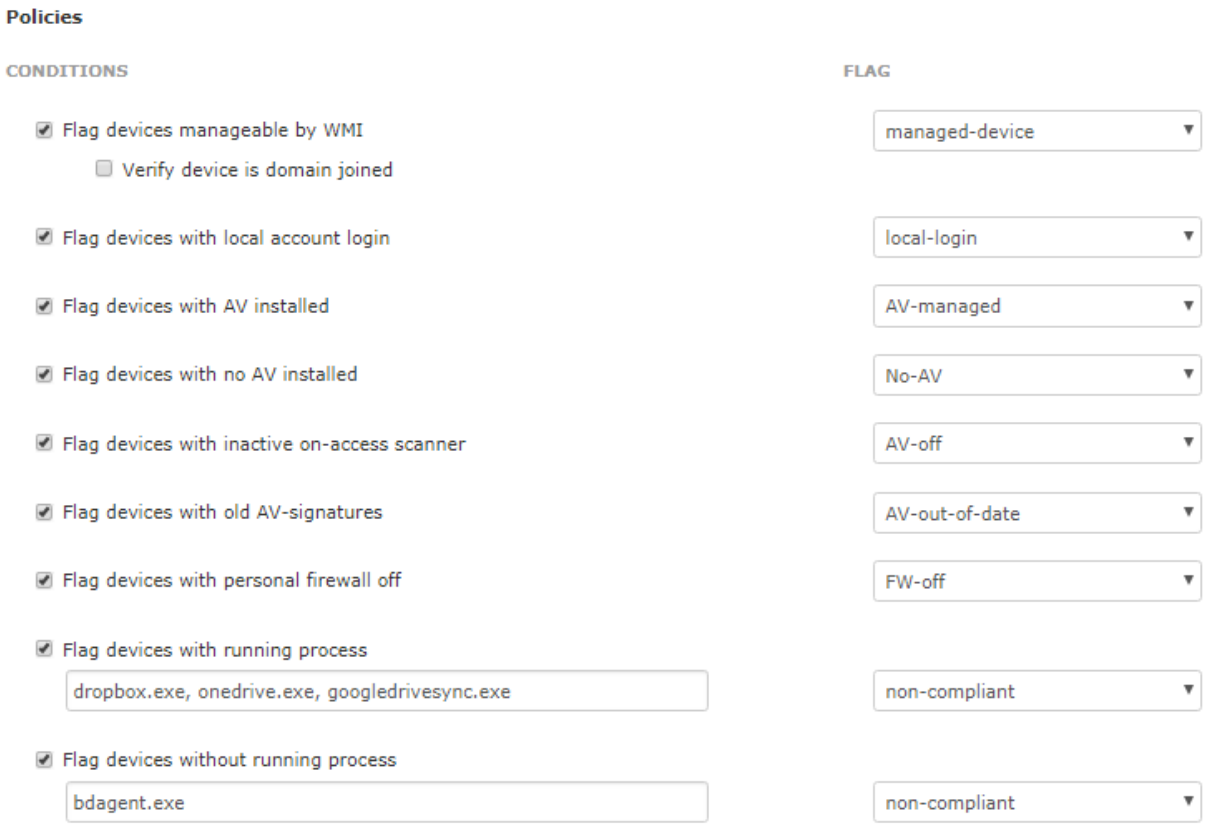
As WMI is a pre-installed component on Microsoft Operating systems, it's recommended you use Microsoft resources from troubleshooting WMI on your network.

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

## Setting and Enforcing Compliance Policies

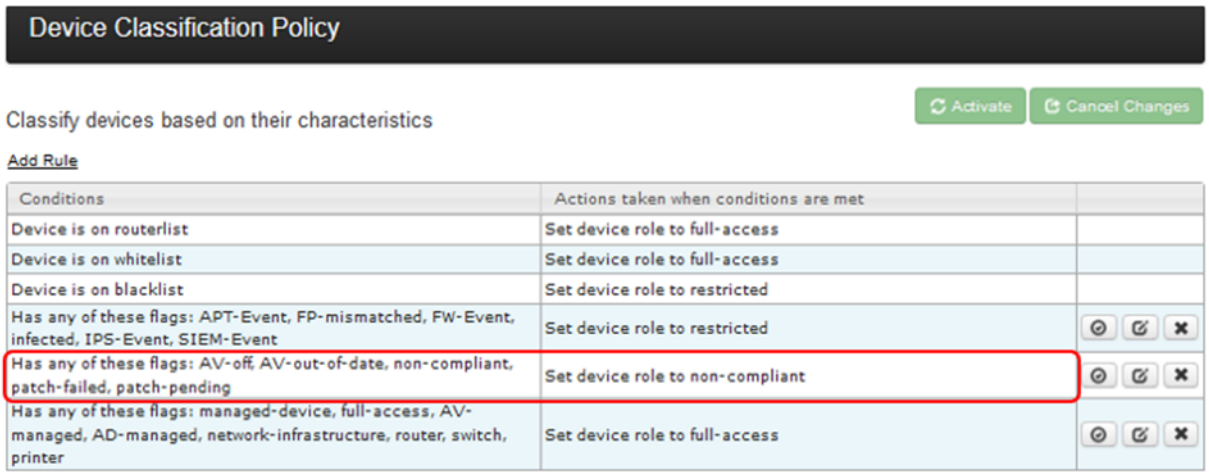
Once the communications between the CGX Access appliance and endpoint devices have been successfully tested, policies can be set to detect compliance with policies.

Select the flags 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 flags on specific devices that meet or fail the conditions.

Using Device & Role Classification policies, devices with specific flags can be assigned different roles.




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

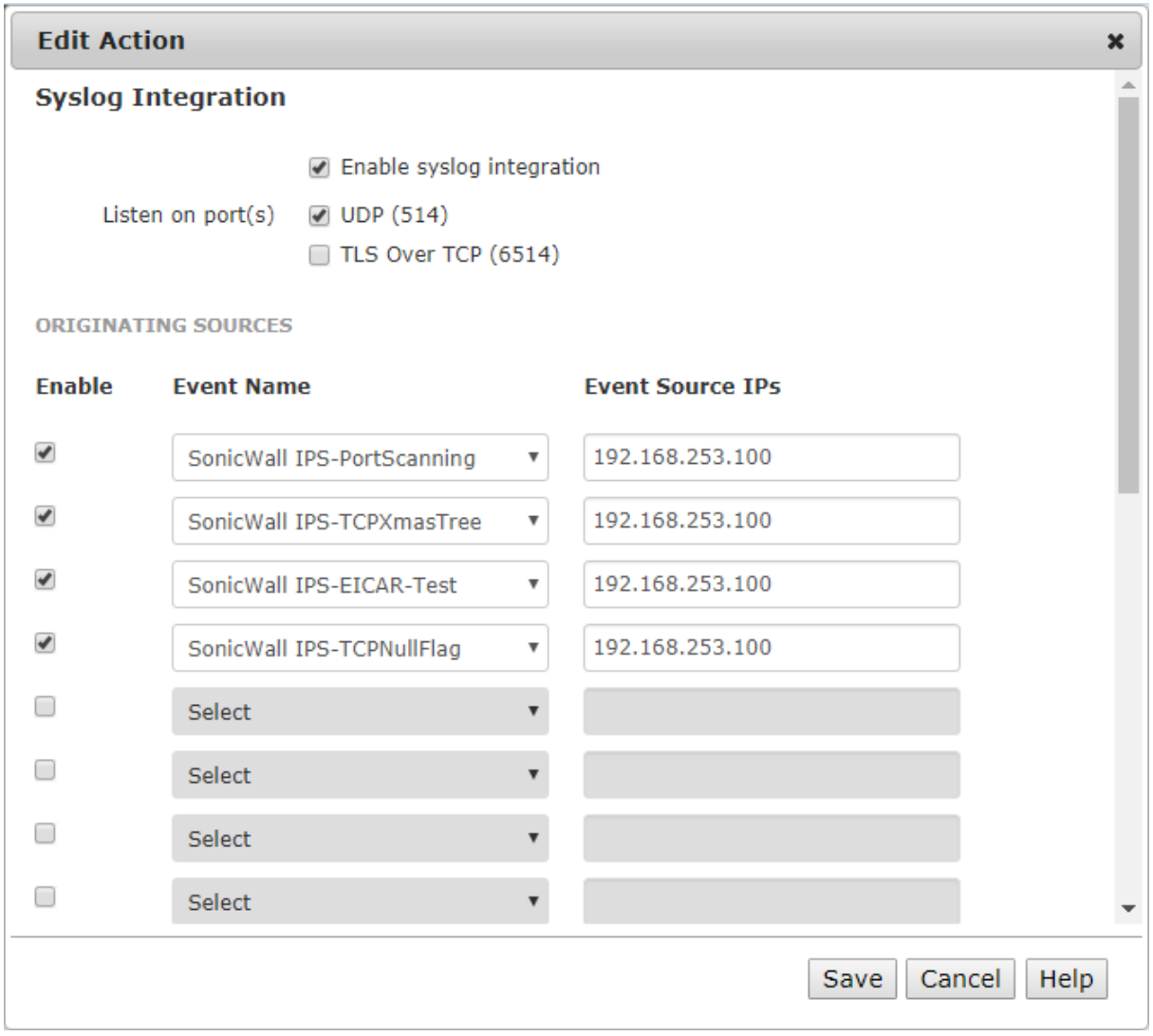
```
ALLOW WHEN PROTO=='TCP' AND PORT==67
ALLOW WHEN ADDR=="192.168.253.100"
DNSALLOW WHEN DNSTYPE==33
DNSALLOW WHEN HOSTNAME=="WIN-EH9KPK2TKSH.iex.demo"
DNSREDIRECT(RemediatePortal)
DENY WHEN TRUE
```

# 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"

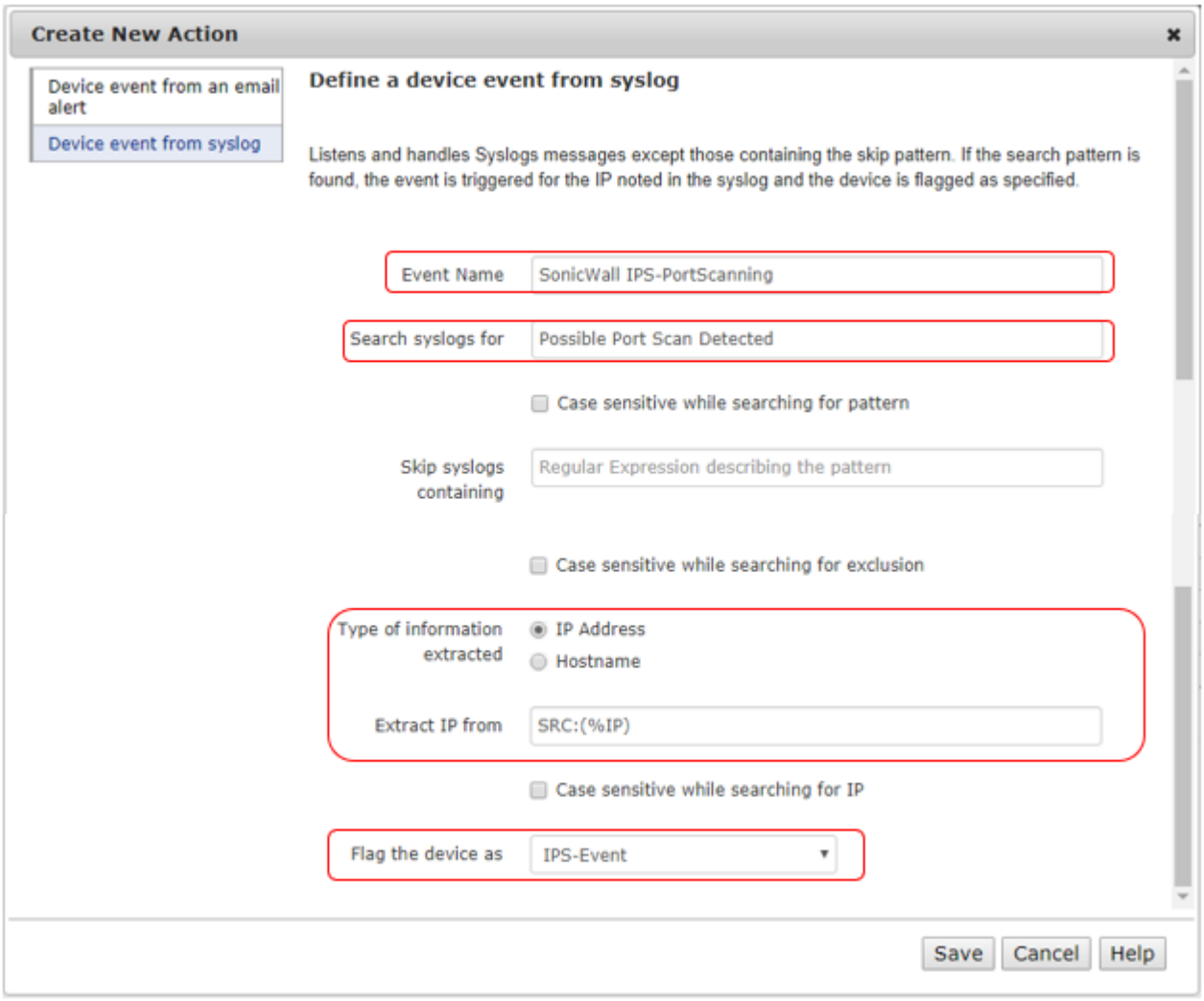



From this screen, an Event can be enabled. The event source IP is the IP address of the security appliance that is sending the syslog message to CGX Access. Multiple IP addresses or IP ranges can be entered.

# 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"




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:

**Flag the Device as**
Choose a flag that should be assigned to the offending device if the event is triggered. Using Device Classification policy, the device can then be automatically quarantined.

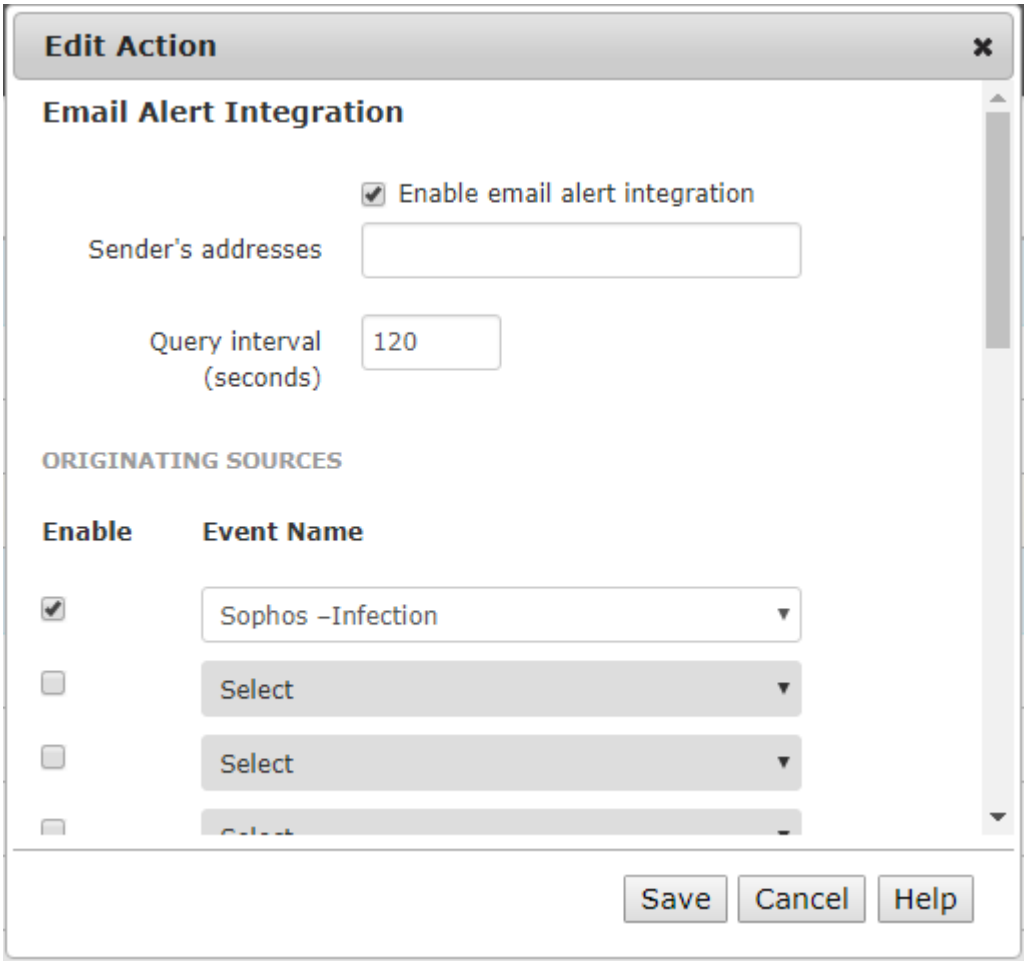
Custom flags names can be created under Configuration → General Settings → Names Used by Policies

# 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"




- From this screen, an Event can be enabled.

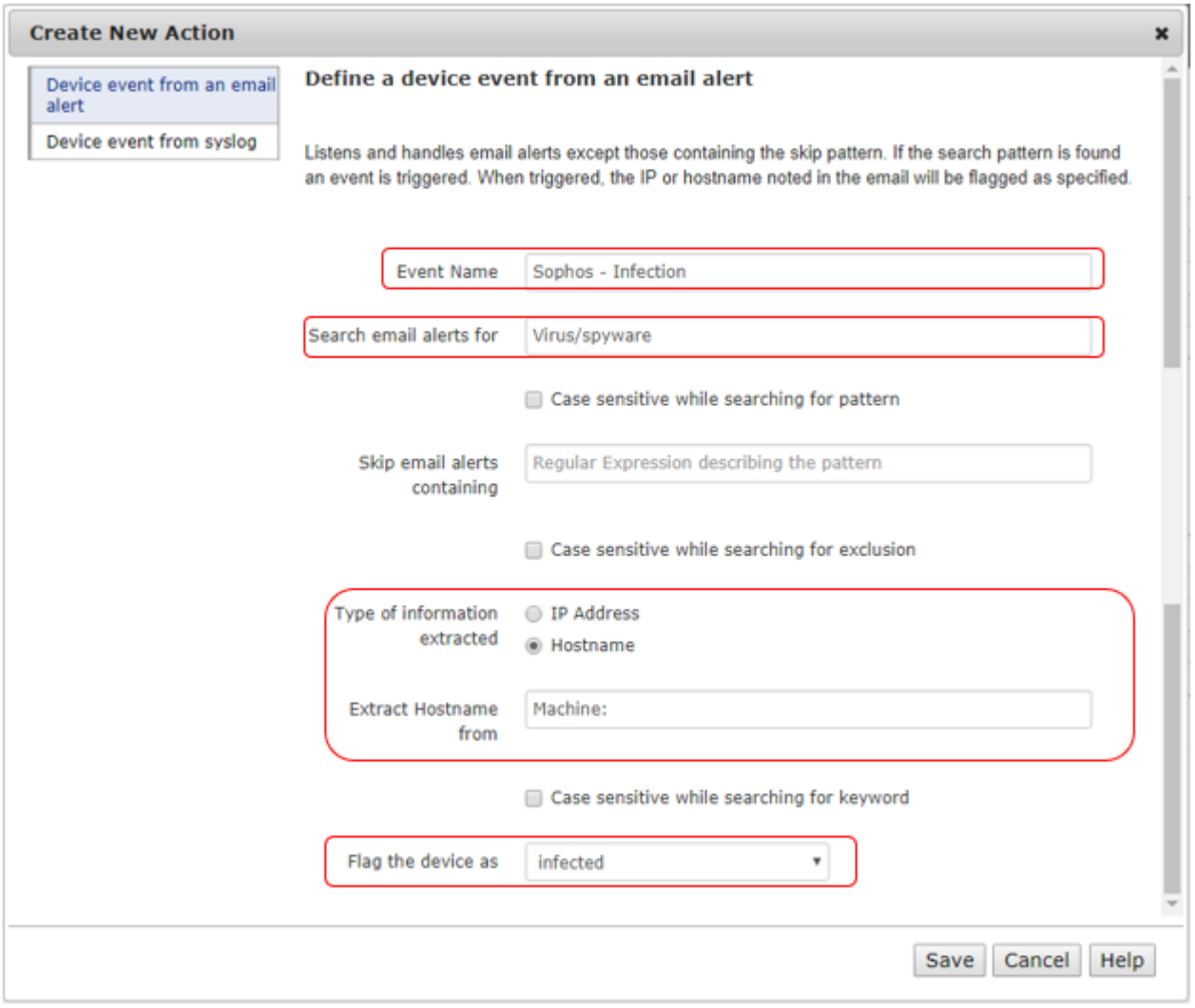
- To limited which e-mail addresses are allowed to send an e-mail alert to the CGX Access appliance, specify the approved e-mails in the Sender's Address section. When blank all addresses are allowed.

- 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"




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:=.

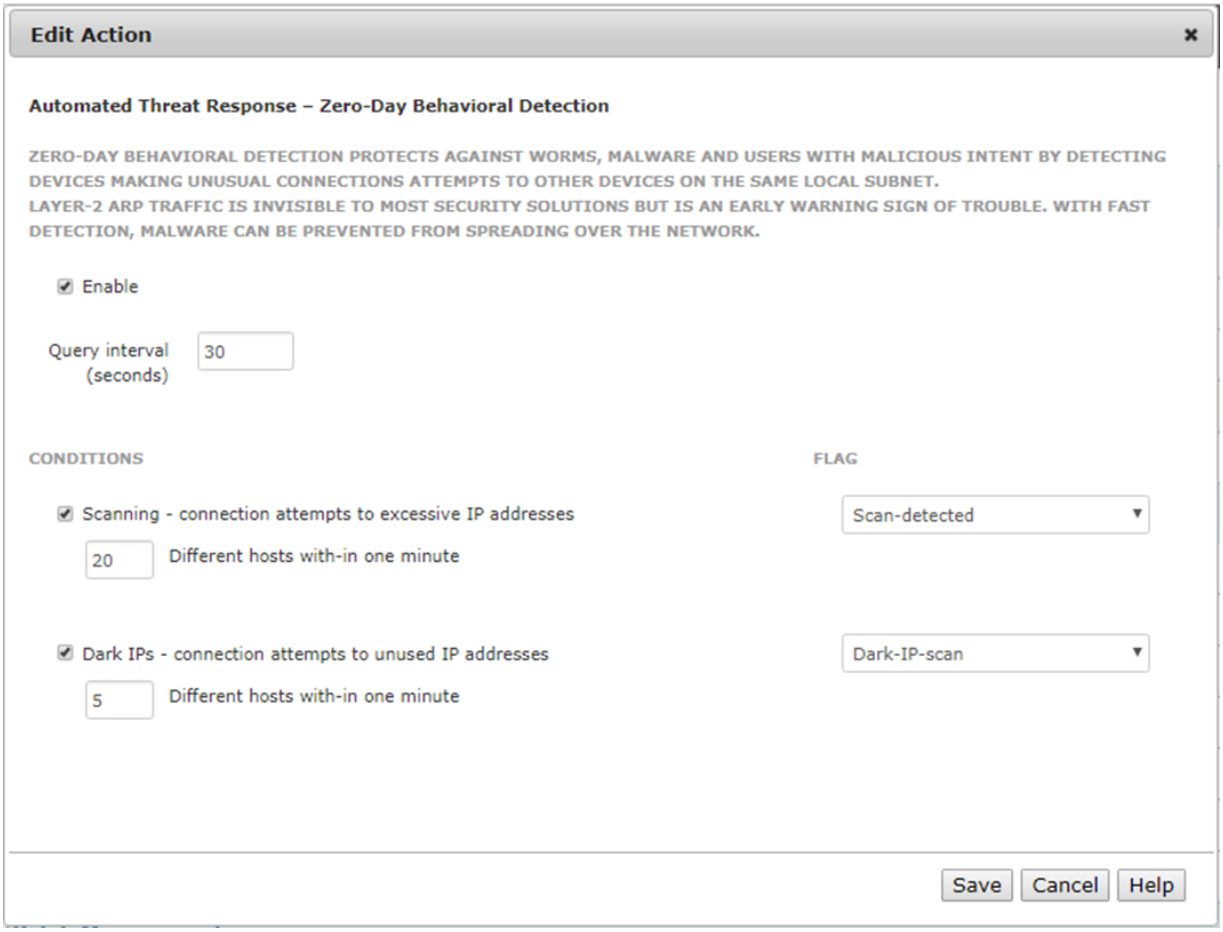
**Flag the Device as**
Choose a flag that should be assigned to the offending device if the event is triggered. Using Device Classification policy, the device can then be automatically quarantined.

Custom flags names can be created under Configuration → General Settings → Names Used by Policies

# Automated Threat Response - Zero-Day Behavioral Detection

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 at 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 Configuration → Integration
- Click on "Automated Threat Response – Zero-Day Behavioral Protection"




With no integration or special requirements, this detection is enabled by default. Devices attempting connection attempts to an excessive number of hosts will be flagged as "Scan-detected". While devices attempting connection attempts to unused IP addresses will be flagged as "Dark-IP-Scan"

# Policy-Based Response

When the “Scan-detected” flag and \ or “Dark-IP-Scan” flag is assigned to a device, the CGX Access can take quarantine actions based on Device Classification policies.

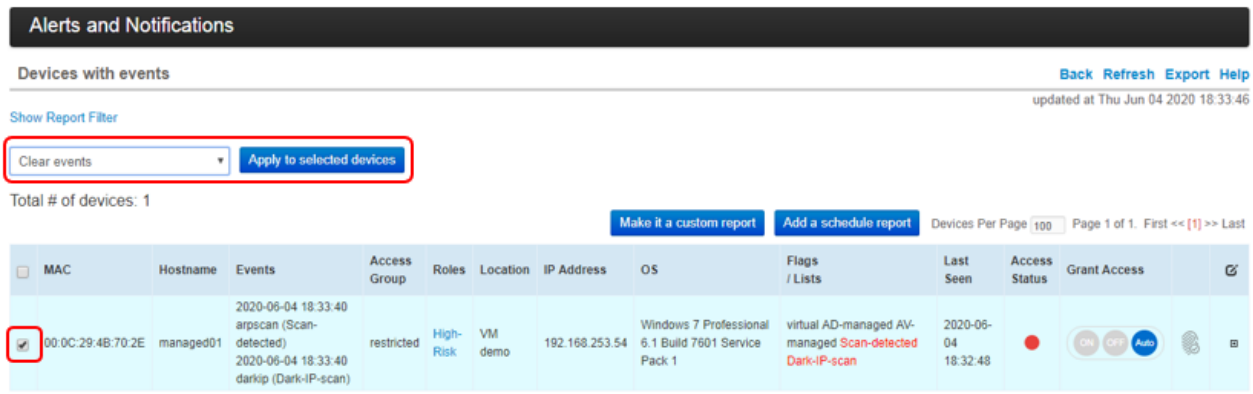
- In CGX Access GUI go to Policies → Device & Role Classification
- Add Rule to take preferred actions when a device is flagged “Scan-detected” or “Dark-IP-Scan”


- The new rule should be dragged near the top of the list, so it has higher priority over other sets of conditions

# 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.

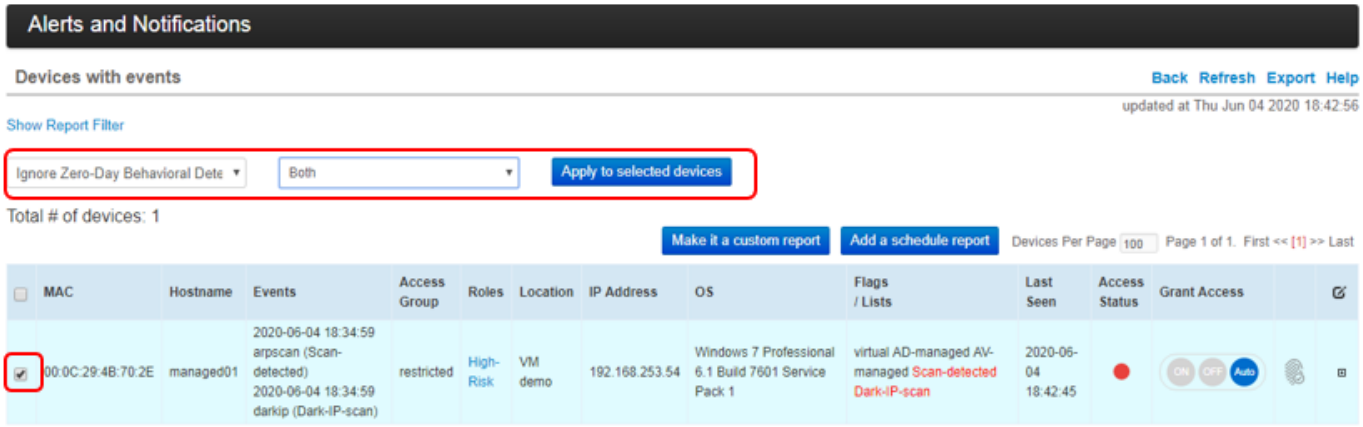
- In CGX Access GUI go to Visibility → Alerts and Notifications
- Click “Devices with Events”
- Select the device(s) that should be cleared, Select the “Clear event” option and Apply



# Handling Exceptions

For network monitoring, it may be necessary to configure exceptions on some devices. To ignore Zero-day behavioral detection, you can flag the allowed devices as “arp-scan-ignoring” and “darkip-scan-ignoring”. These flags 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




**Note:** by default, devices flagged as Network Infrastructure are exempt from zero-day checks.

# 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. 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.

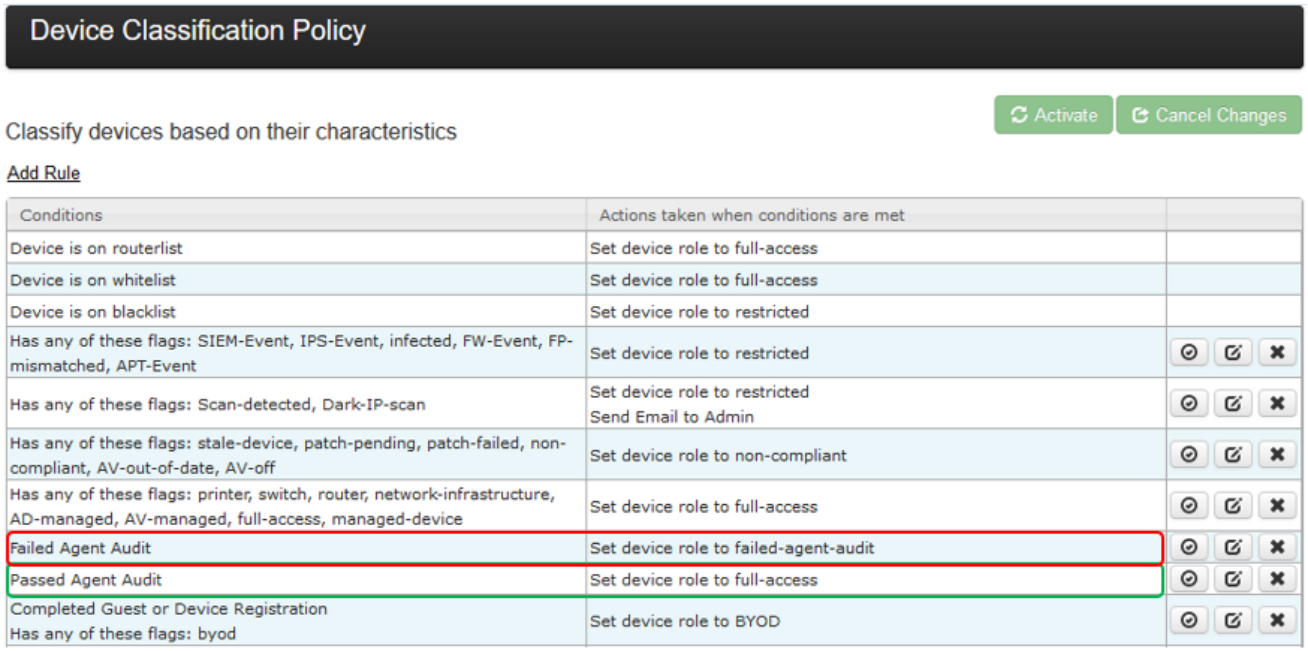
| | CGX Access - Agent | CGX Access – Agentless |
|---|---|---|
| Detection | Agent would detect changes within 10 seconds | Compliance check with integration module depends on the re-check interval |
| Supported OS | • Microsoft Windows<br>• Apple MacOS<br>• Linux | The Operating Systems supported by Integration solution(s) |
| Compliance checks | Compliance check can be customized to Include but not limited to the followings:<br>• Running Process<br>• Registry values<br>• Files and locations<br>• Ini files and contents<br>• Machine names and OS check<br>• Authentication | Agentless solution – Integrations with AD, 3rd-party AV, Patch, and WMI |
| End-user compliance communication | Pop-up Message | HTTP Redirection |
| Real-time Wi-Fi adapters control | When connected to any wired network that has connectivity to CGX-Access (ie. Corporate Network). The wireless network adapter can be disabled automatically.<br>It would be re-enabled once wired NIC is disconnected | N/A<br>Can use Windows Connection Manager as a substitute |
| 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

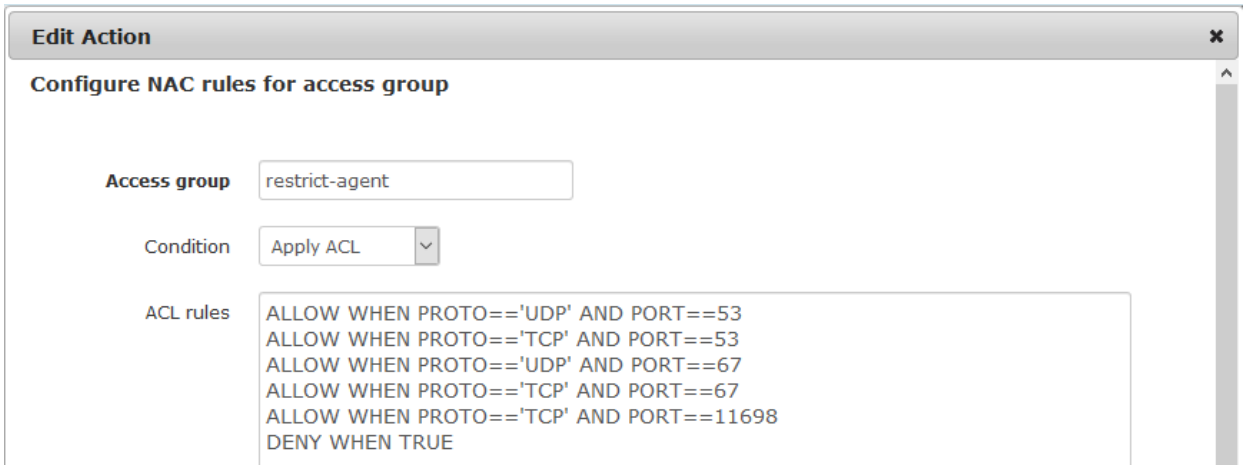
Easy NAC virtual appliances come with default agents and default polices that can be used for testing or as a baseline to start building your custom compliance policies.

By default, Device Classification 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 → Device & Role Classification




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.

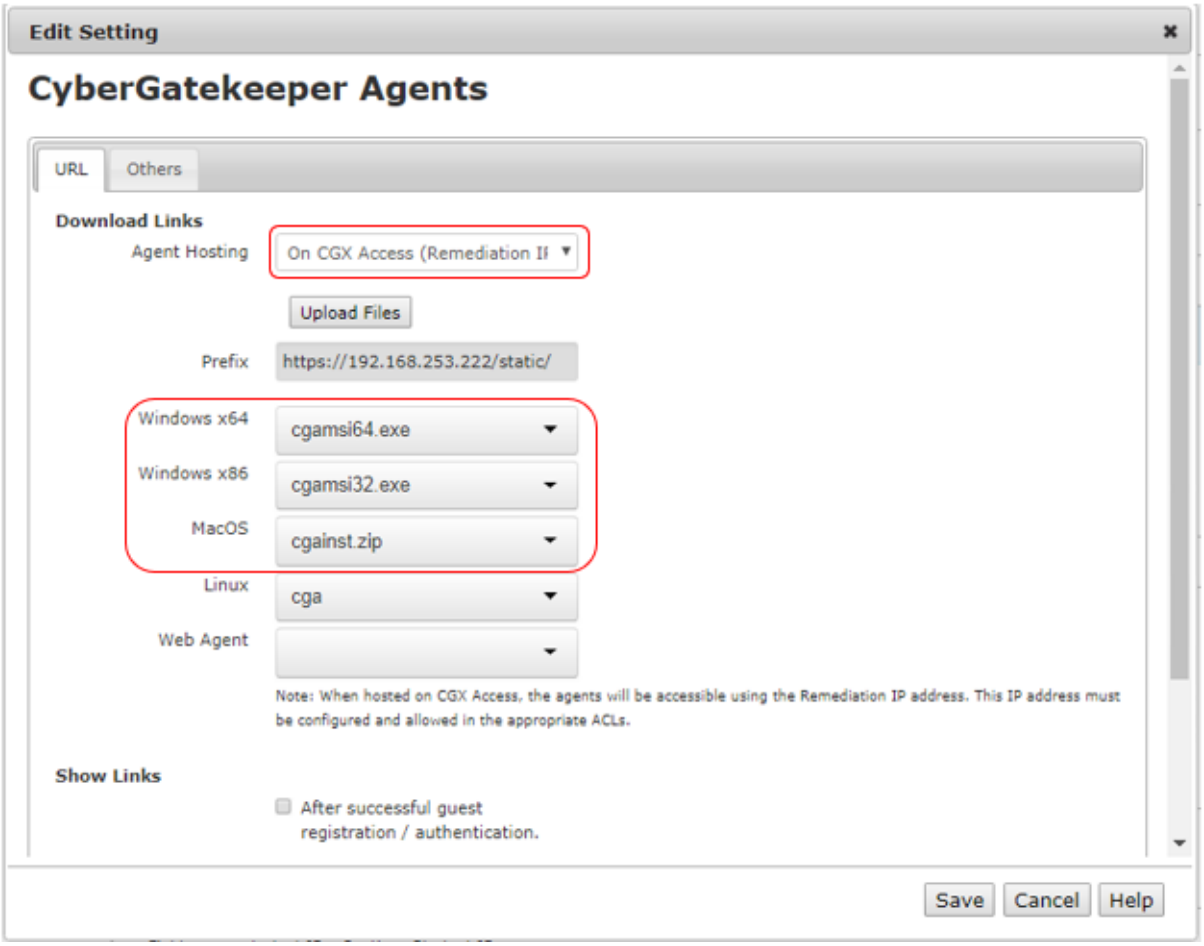



It is recommended the default "restrict-agent" ACL be edited to allow access to approved remediation resources such as the AV server, patch server, etc.

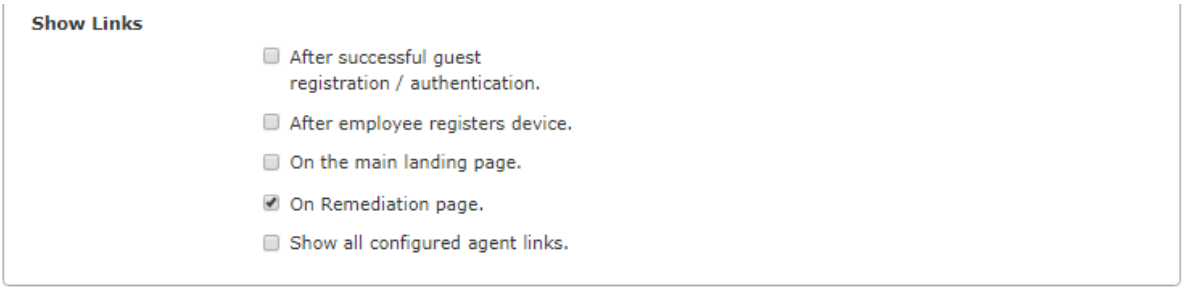
# Hosting Agents

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

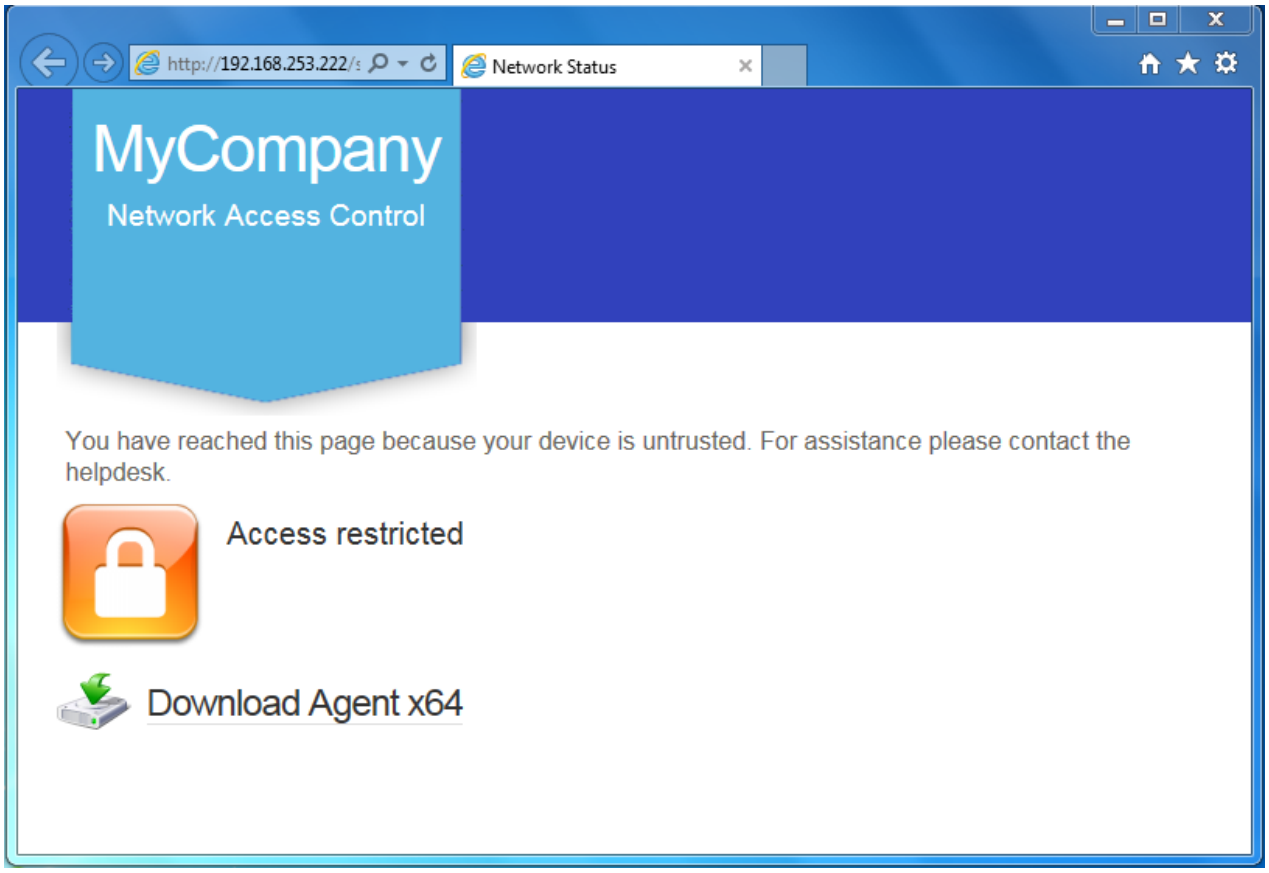



To host agents on the appliance, it will be necessary to use the Remediation IP address. Once the above settings are configured; you can decide when to show the agent installers to your end-users.



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”.



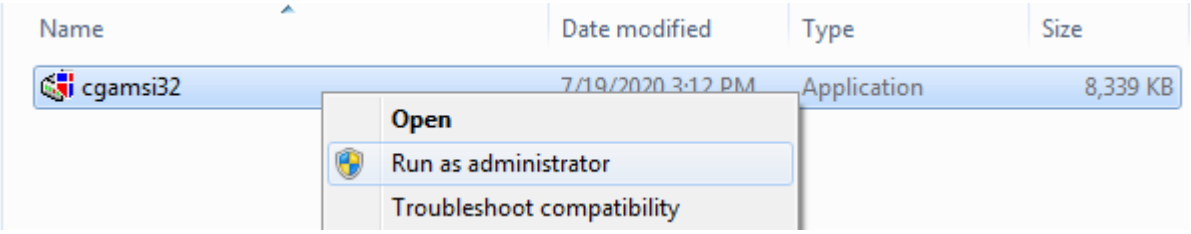

# Installing Agents

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 is quick to download and install.

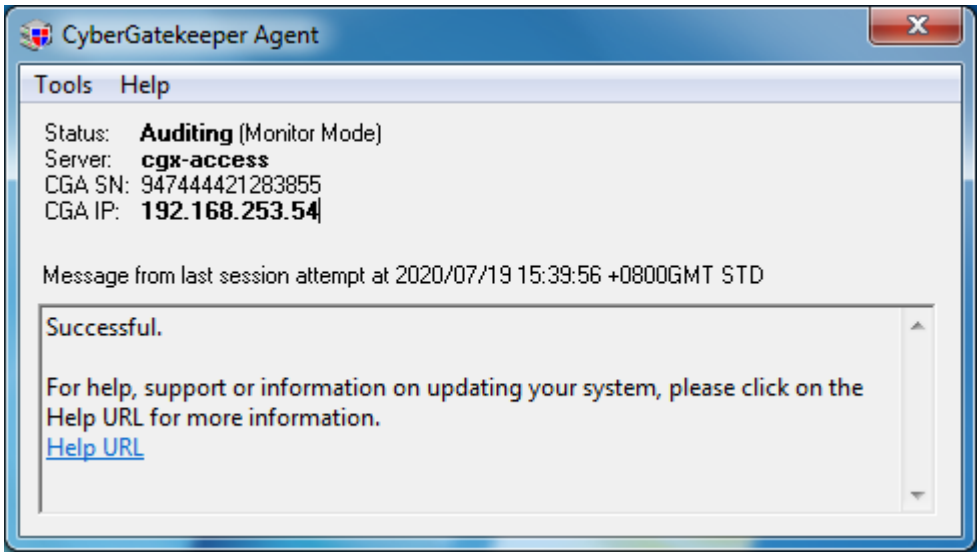
Most organizations choose to use a software deployment tool or AD Group policy with a computer startup script to install the agent automatically for their managed devices. Contact InfoExpress support for a sample script.

In the case of manual deployment, administrative rights are required.

- Right-click the installer file and chose 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 click the agent viewer will show the current status




# 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:

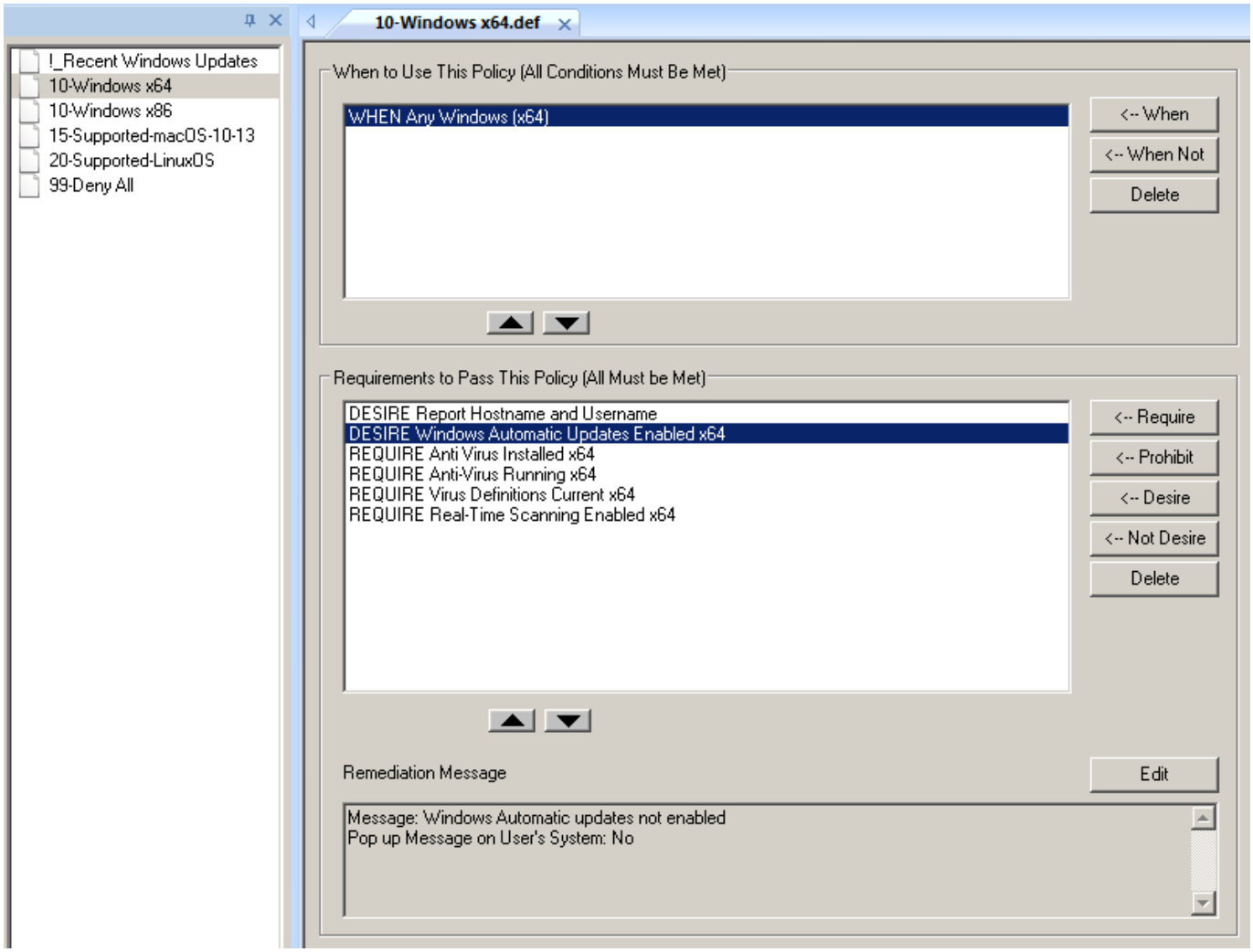
- Creating compliance tests
- Creating compliance policies
- Uploading compliance policies to CGX Access appliances
- Building agents for different operating systems

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.

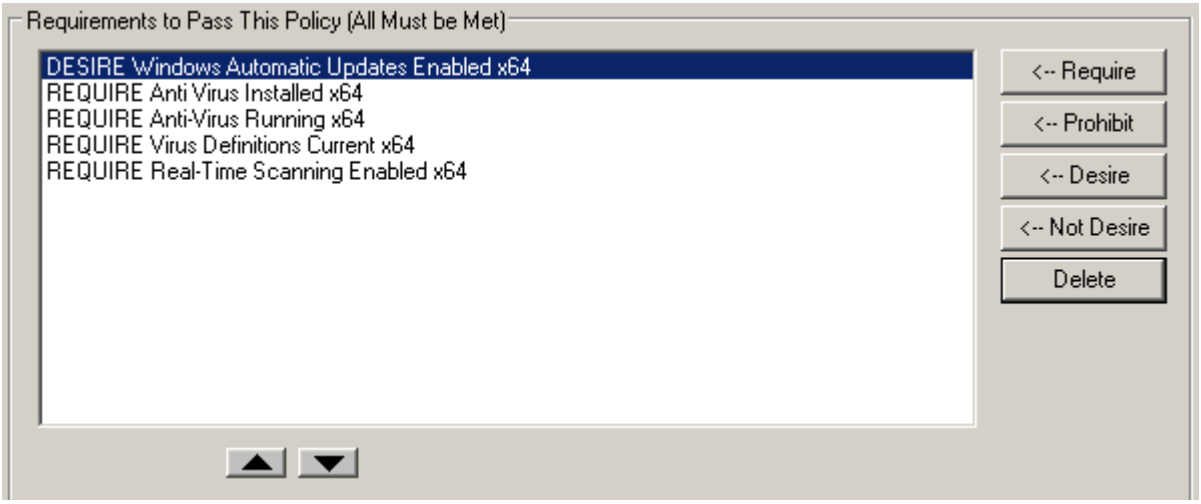
The **PROHIBIT** command is used to prevent certain conditions and passes if the test condition is not true. If any **PROHIBIT** command is not met, the agent would FAIL to pass this policy and hence the audit.

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, eve 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.

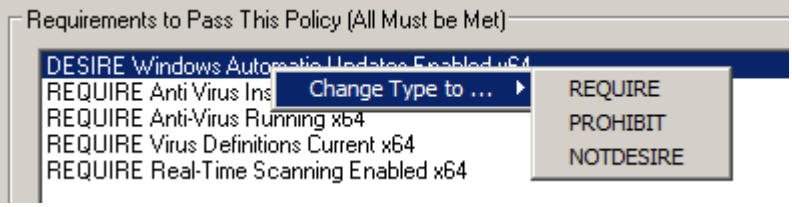
However, because of the nature of the DESIRE or NOTDESIRE command, it would still be pass audit, even if it fails this test, so the next requirement would still be checked.

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 Scanning 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 perquisites 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

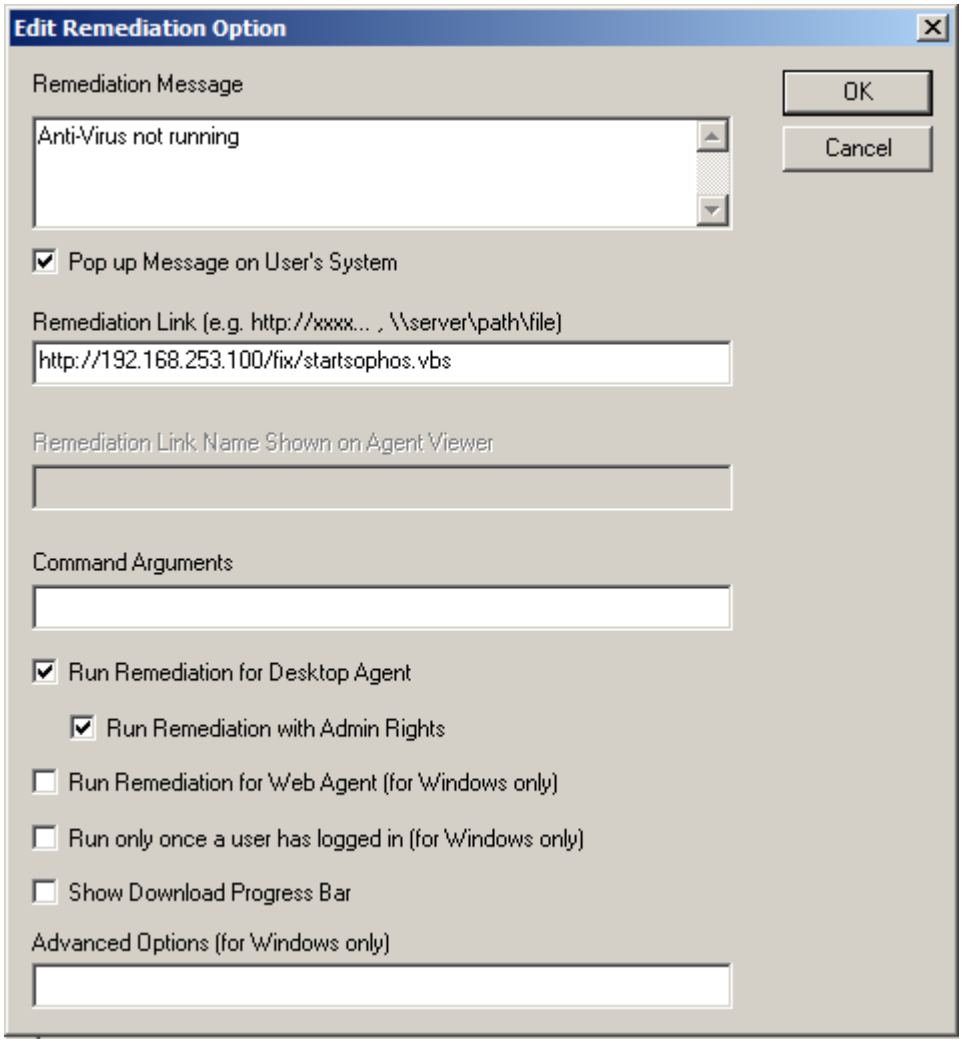
If an agent fails a policy requirement, the administrator has the option of running a remediation action, displaying a remediation message to the user or both.

- 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.




## 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 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.

# 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:

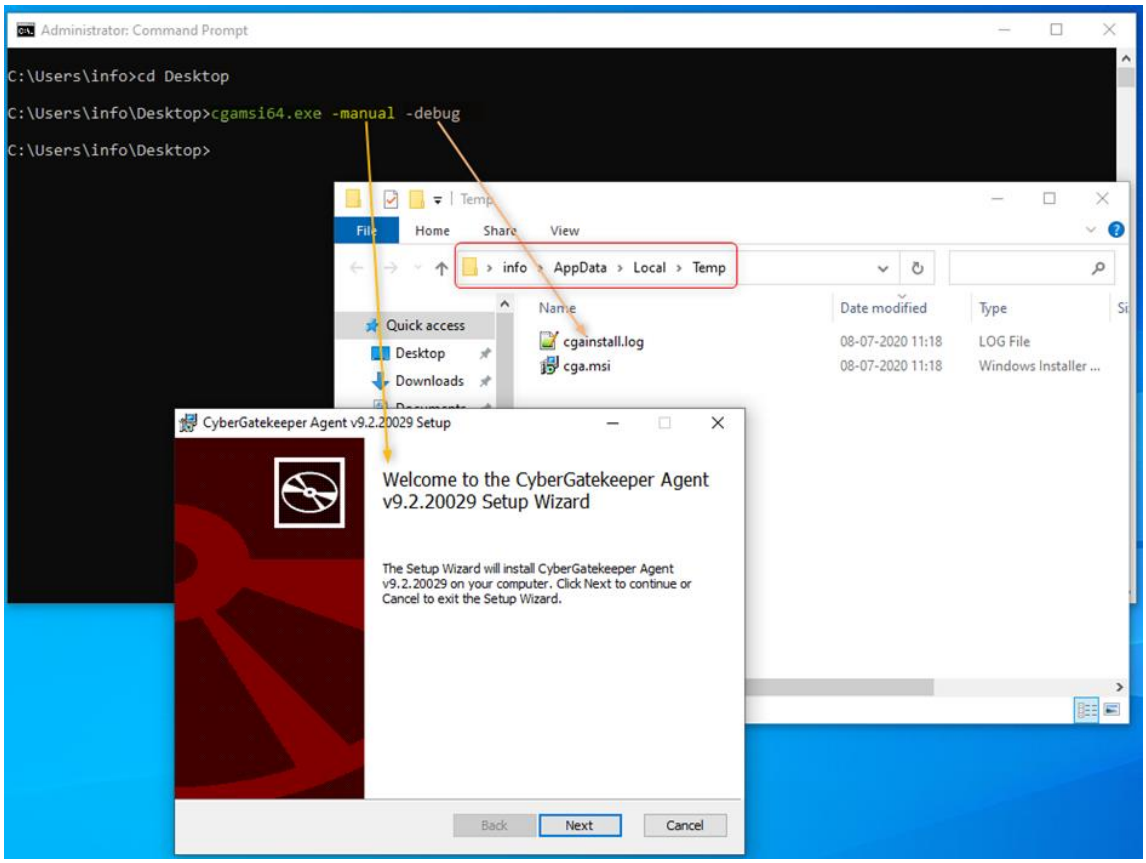
cgamsi32.exe or cgamsi64.exe and use any of the options below:

| | |
|---|---|
| `-debug` | Generates installation log at `%tmp%\cgainstall.log`. *You can send this log to support when requiring assistance for installation issues* |
| `-log` | Enables agent debug logging in agent install dir [filenames=IEXCGAxxxxx.log] |
| `-manual` | Interactive install. Shows install window and progress. |

For Example:

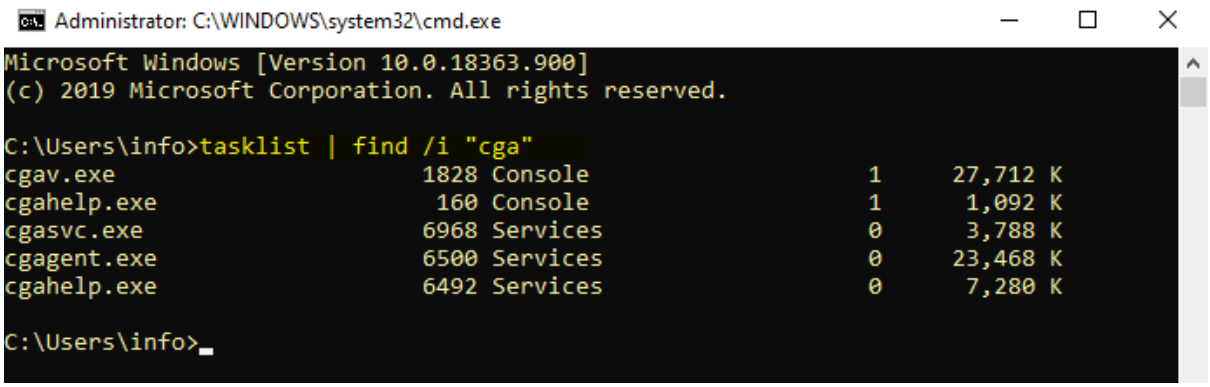
```
> cgamsi64.exe –manual –debug
```

This is 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. [*if hostname is used while agent building*] | Check is your DNS is configured to resolve CGXA hostname |
| `Failed. Unable to connect to CyberGatekeeper <CGXA>` | > Ping <CGXA> | to check CGXA reachability *(if your firewall allows ICMP)* | 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 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. |

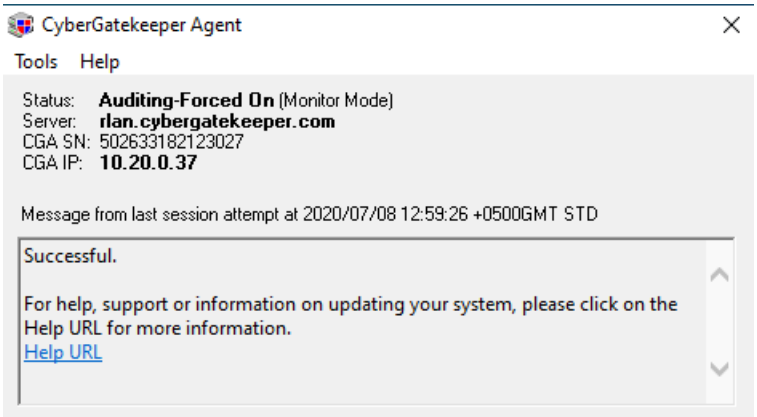
**Different Domain error:** This error occurs when the agent and the policy on the CGX Access were built from a different Policy Manager. It can also occur if no policy has been pushed to the CGX Access appliance. The agent and the appliance share a secret key, and this key is generated and provided 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:

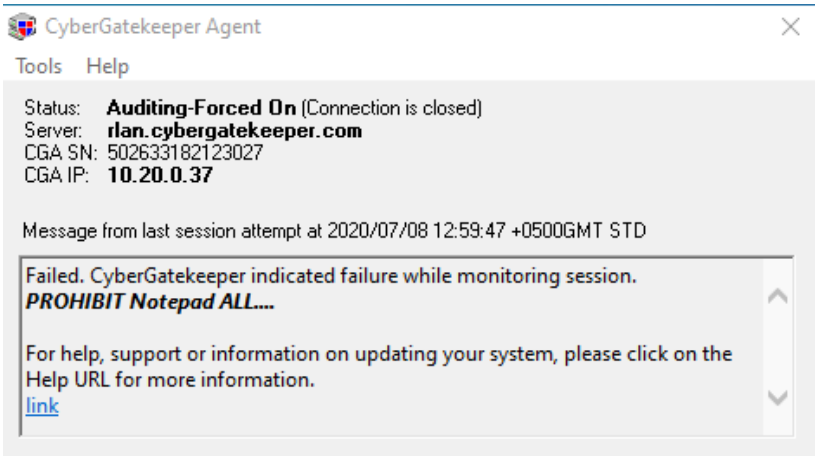
- Uploading the policy to the appliance, from the same Policy Manager that built the agent.
- Import the correct Shared Settings into the Policy Manager and re-upload the policies to CGX Access. (If using default agents, contact support for the default Easy NAC shared settings).
- Re-building and re-distributing 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

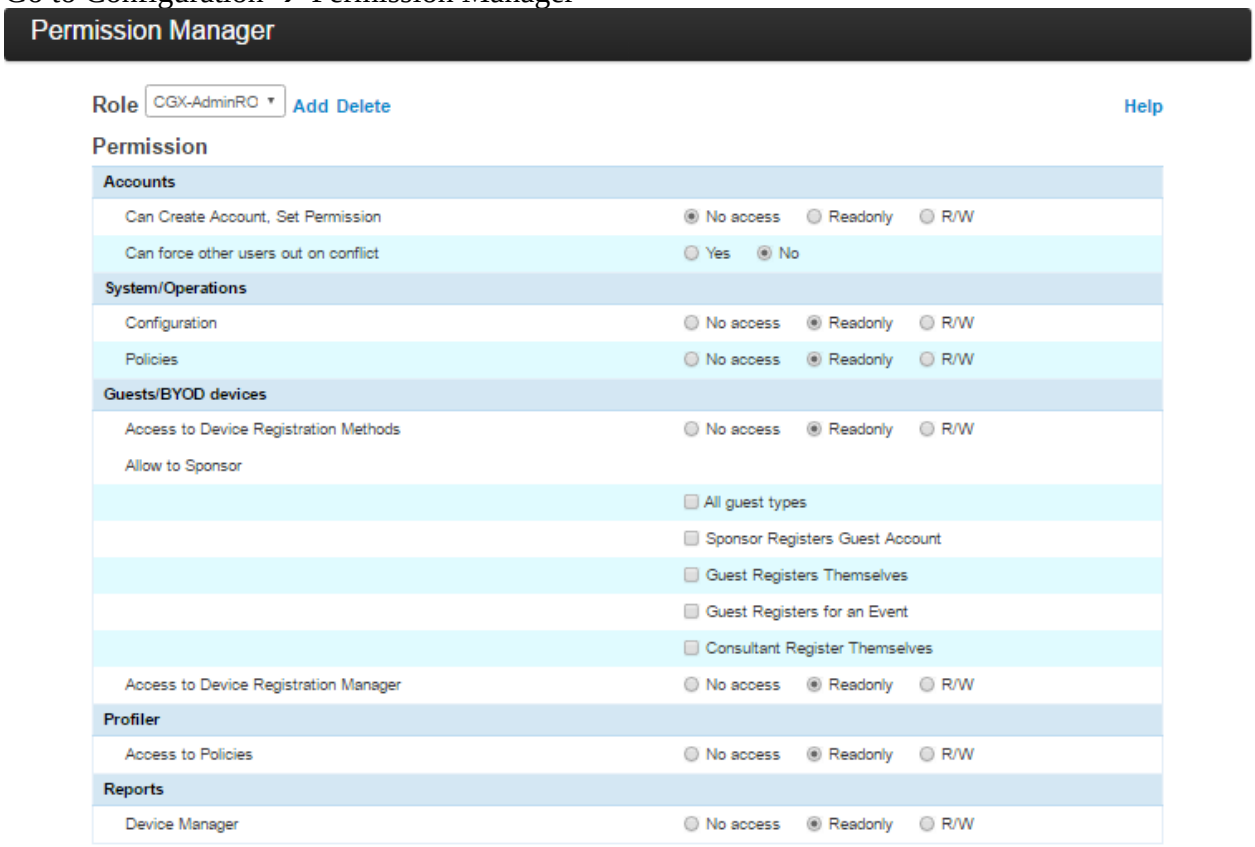
CGX Access can query the Active Directory server to validate permissions for administrators to access the management GUI. CGX Access uses management accounts stored in Active Directory. Different levels of access are given to admin users based on their AD group membership.

### 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.

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

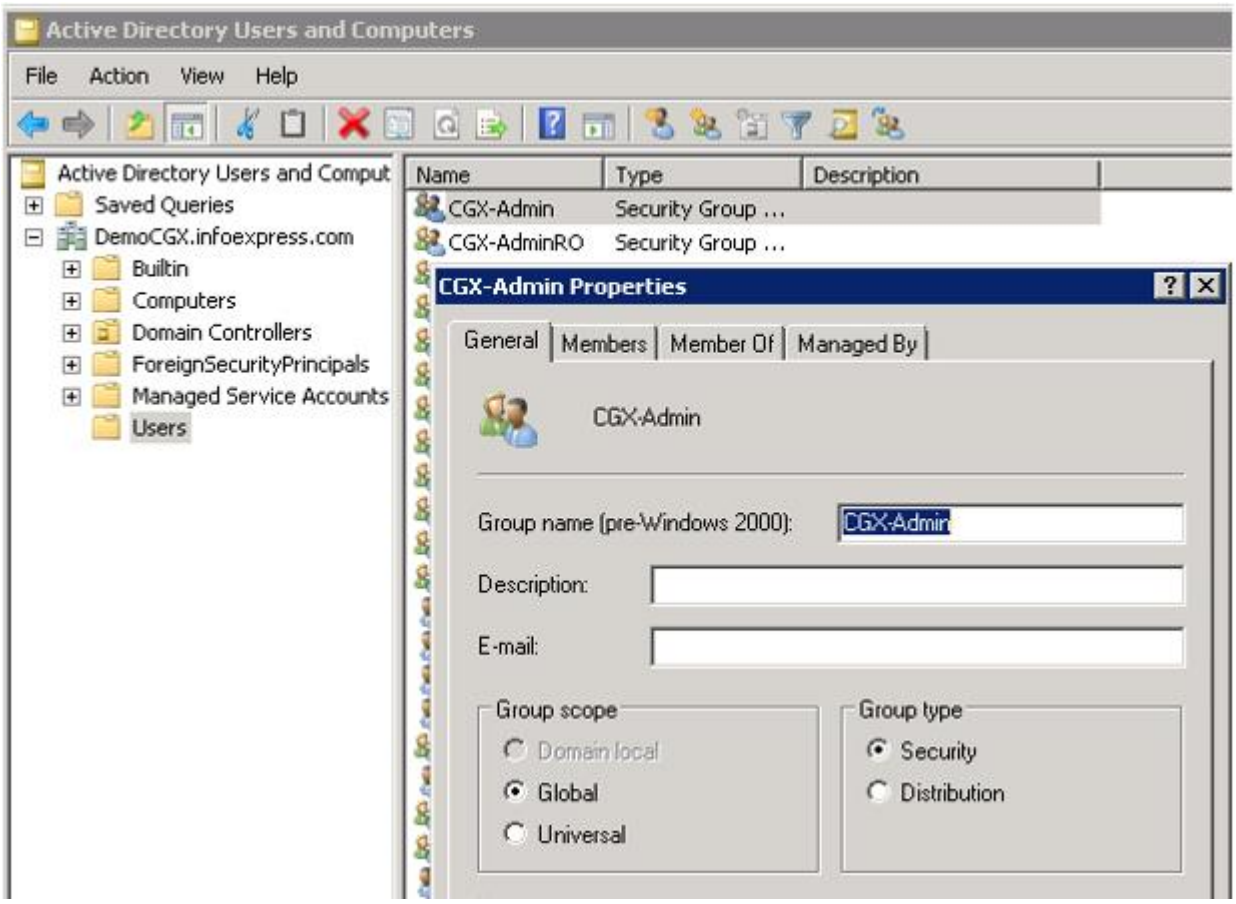



These roles correspond to groups in Active Directory.

## 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 Radius for CGX Admin Login or BYOD Authentication

## Radius Server Configuration

**Note:** Free RADIUS ser**ver** was used in this guide

- On Radius, Configure CGX Access as a client to allow query
- Add VSA id 2939 in dictionary with following attributes

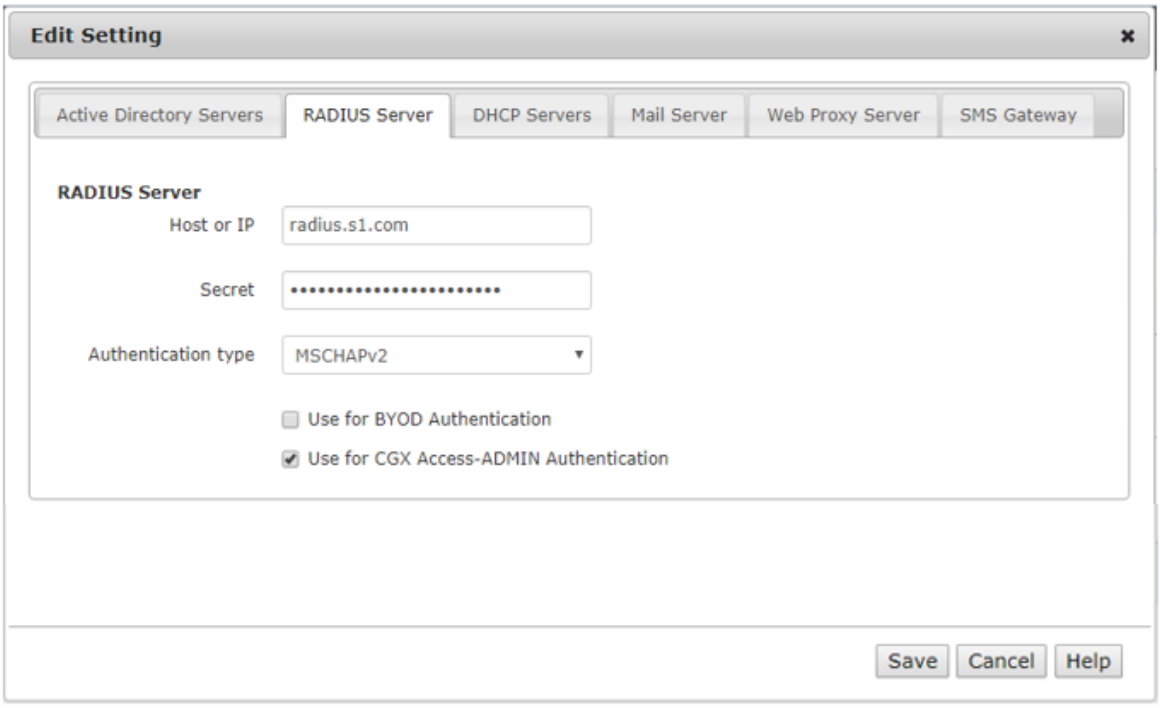
```
VENDOR InfoExpress 2939
BEGIN-VENDOR InfoExpress
ATTRIBUTE    iexgroup    11    string
END-VENDOR InfoExpress
```

- 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
```

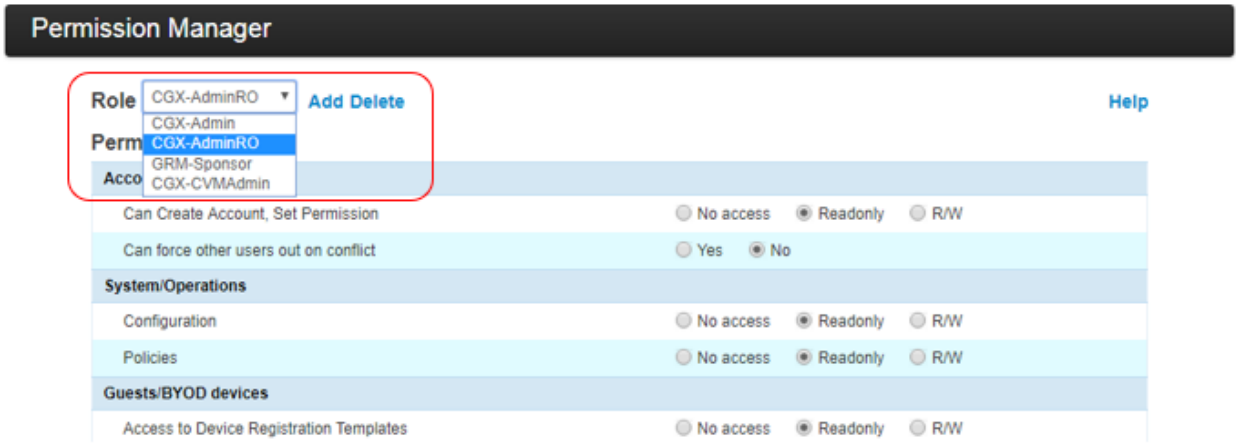
## CGX-Access Configuration

- Go to Configuration → General → Servers → Radius Server
- Configure your Radius Server details (PAP or MSCHAPv2)



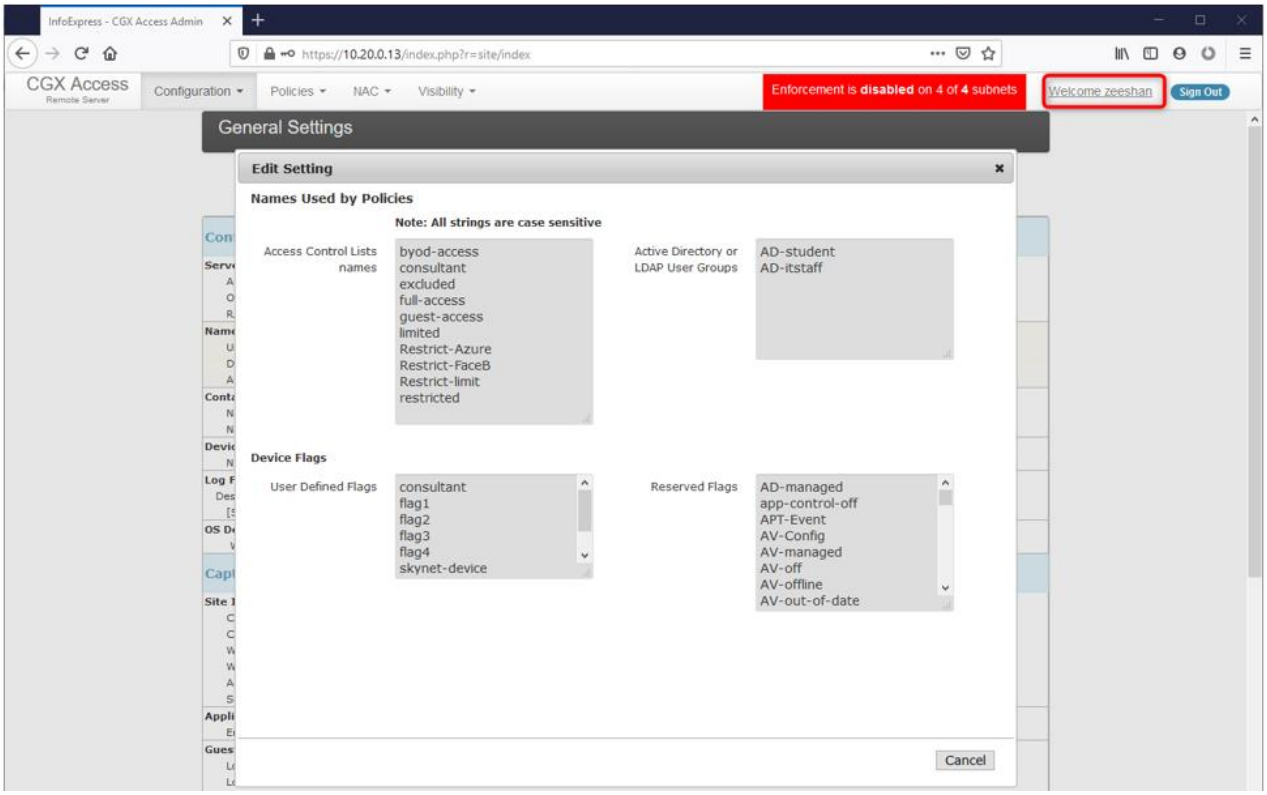
For assigning group level permissions, you can either use predefined groups or create your own group with custom permissions.

- 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 main.css file |
| | | /images | contains the images referenced by the css file |

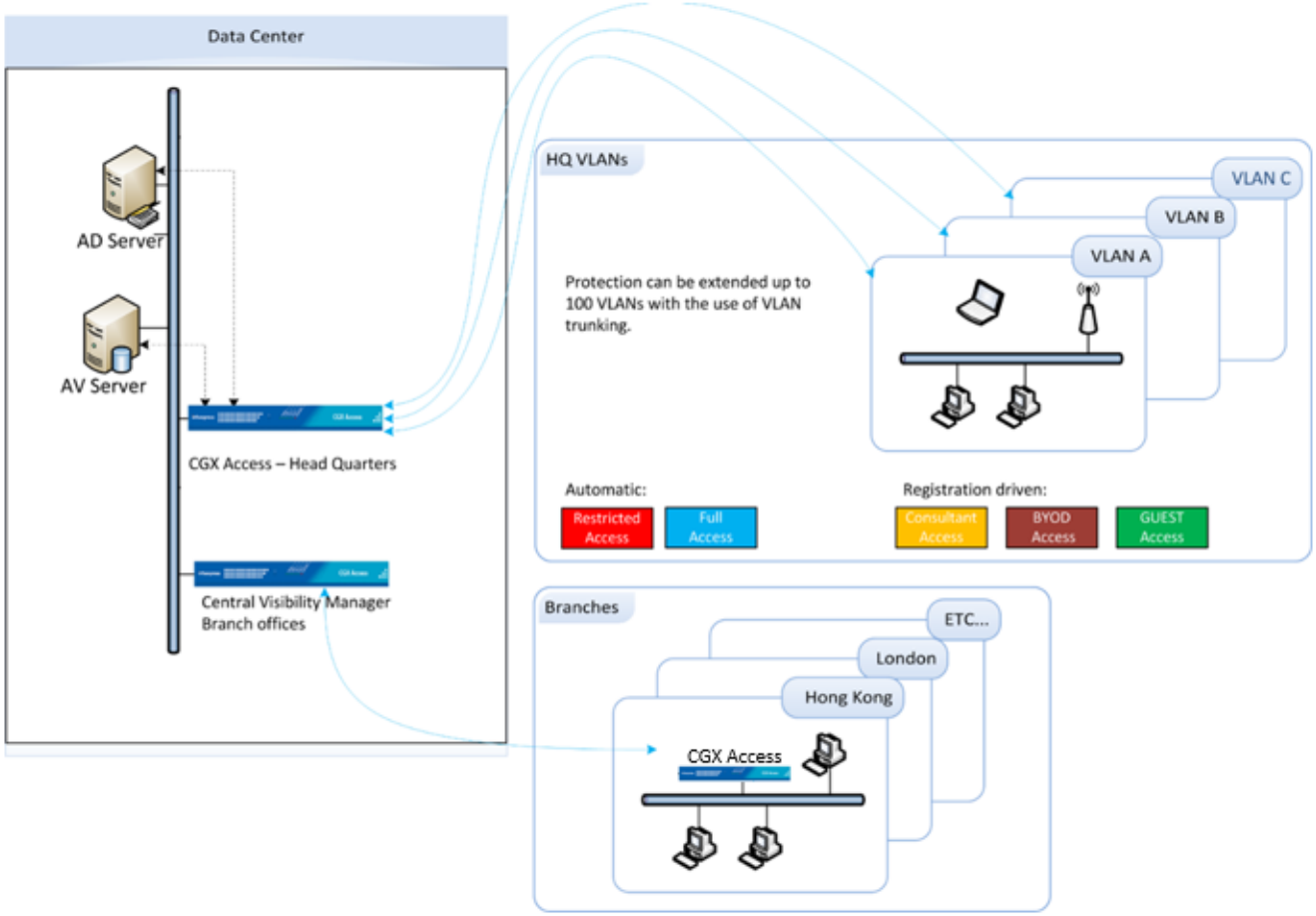
Only the *main.css* file and images are needed on the CGX Access, The .less files do not need to be uploaded

**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.**

# Central Visibility Manager

## CVM Overview

It's common to deploy multiple CGX Access appliances in multiple offices or for scalability in larger networks. 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, so it used to consolidate the management of multiple appliances.

## Configuring a Central Visibility Manager

The Central Visibility Manager uses the same virtual 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:**

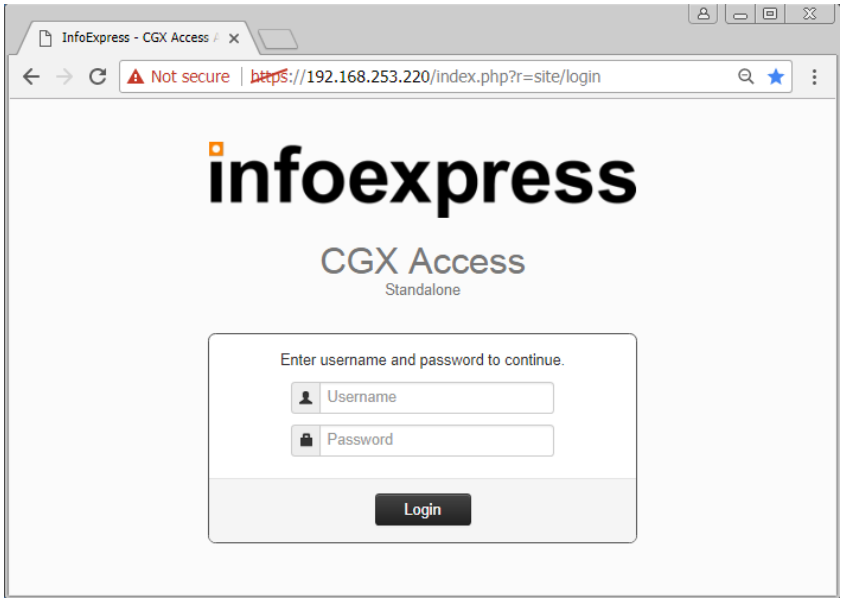
- admin - used for initial setup and configuration as well as SSH access for maintenance tasks
- cguser - used for uploading files through ftp

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)

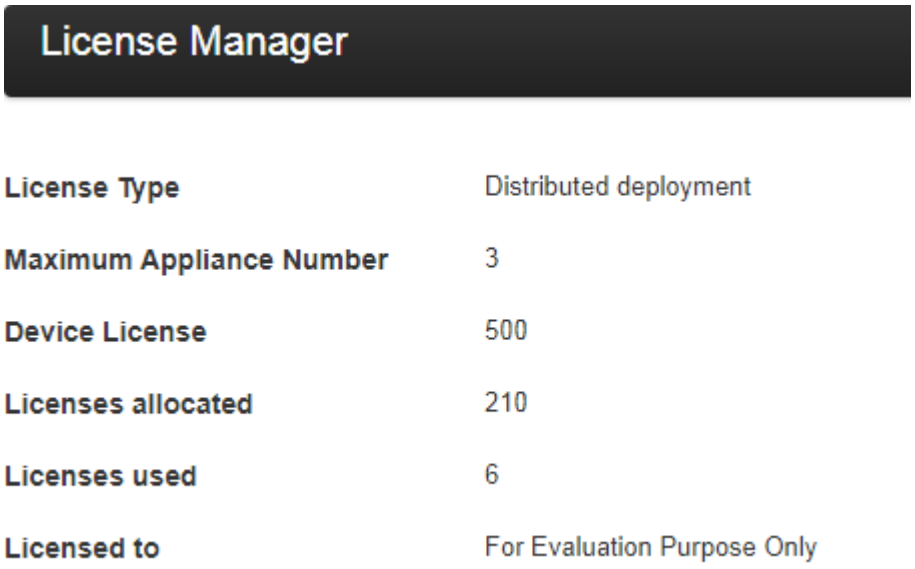


Login as user admin (default password admin). A modern browser such as Chrome is strongly recommended. Older versions of IE or Firefox may not display the pages correctly.

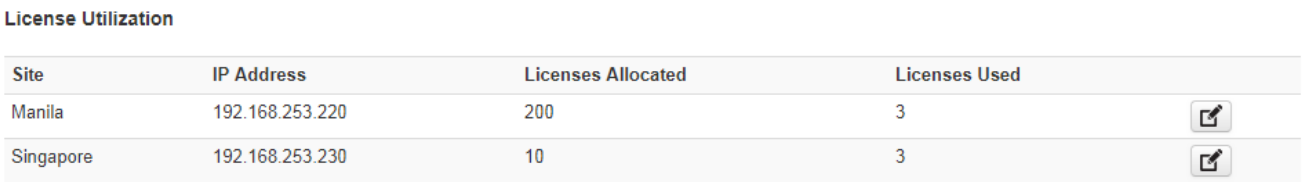
Using the web GUI additional setting can be configure:

- (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

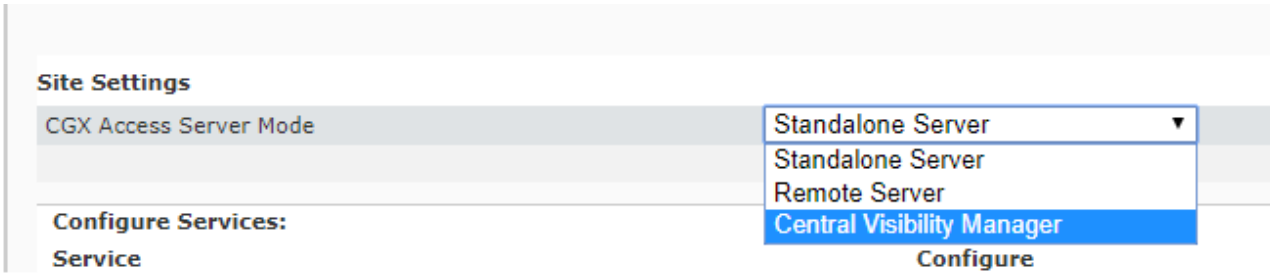



The License Manager will show the maximum number of GX Access appliances that CVM can manage. If using a Distributed license, you will also see the number of devices that can be managed, and the current allocation of the license. With the distributed license, customer can allocate the license across different appliances, as shown below.

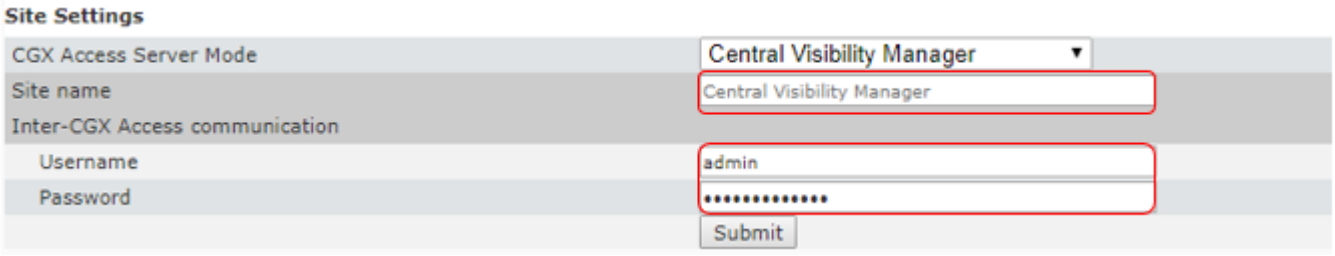



Once the initial configuration is done the new server can be switched to a Central Visibility Server.

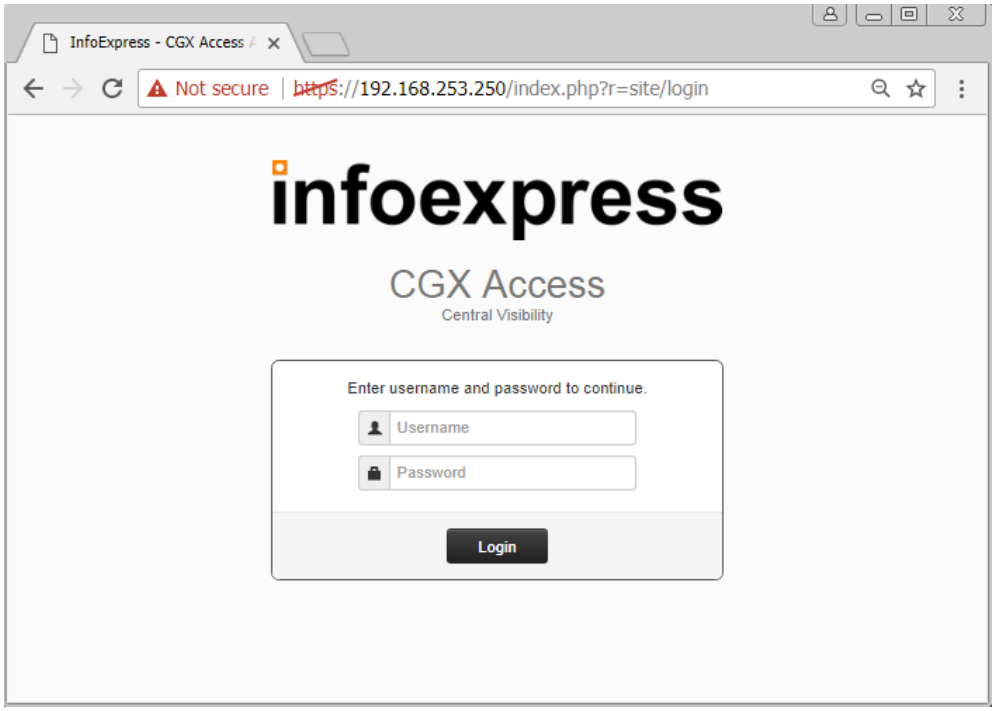
- In CGX Access GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" from Standalone Server to Central Visibility Manager




- Set both the Site name and an account for Inter-CGX Access communication.
  - 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 _
  - The username and password credentials are only used to secure Inter-CGX traffic. They do not need to correspond to any actual account.




- Click **Submit**. You will be logged out of CGX-Access and the changes will take effect.



# Configuring a Remote CGX Access Appliance

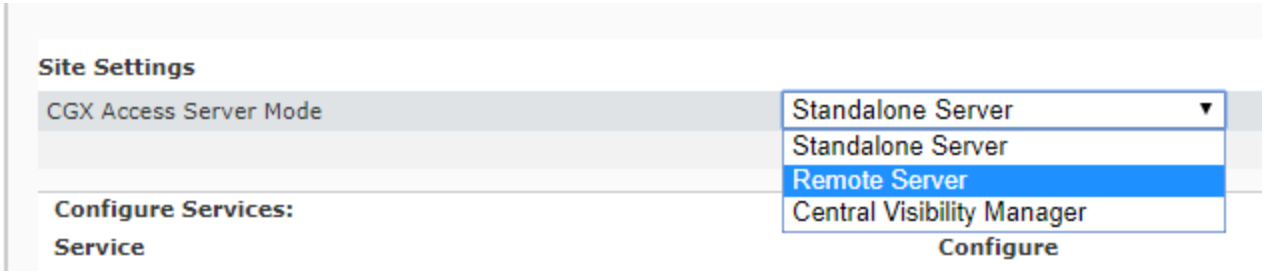
Once a Central Visibility Manager has been configured, new or existing standalone CGX Access appliances can be configured to be manageable from CVM.

If the Remote Server will be a new deployment and not a conversion of an existing Standalone Server, first perform an Initial Configuration as covered on Page 13. At a minimum, the Remote Server should have:

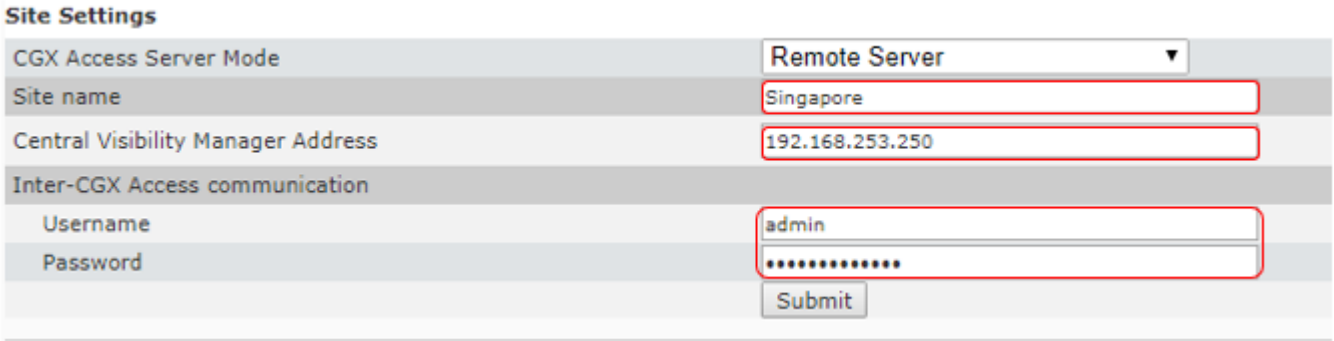
- Have a primary IP address assigned
- Have a Host name
- Have a DNS server

Once the server has a basic configuration it can be switched to a Remote Server:

- In CGX Access GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change "CGX Access Server Mode" from Standalone Server to Remote Server




- Set the Site name, Central Visibility Manager IP Address, and the account for Inter-CGX Access communication.
  - Site Name should only consist of the characters A-Z, a-z, 0-9, and _
  - The username and password credentials must be the same as those set on the Central Visibility Management Server.
  -

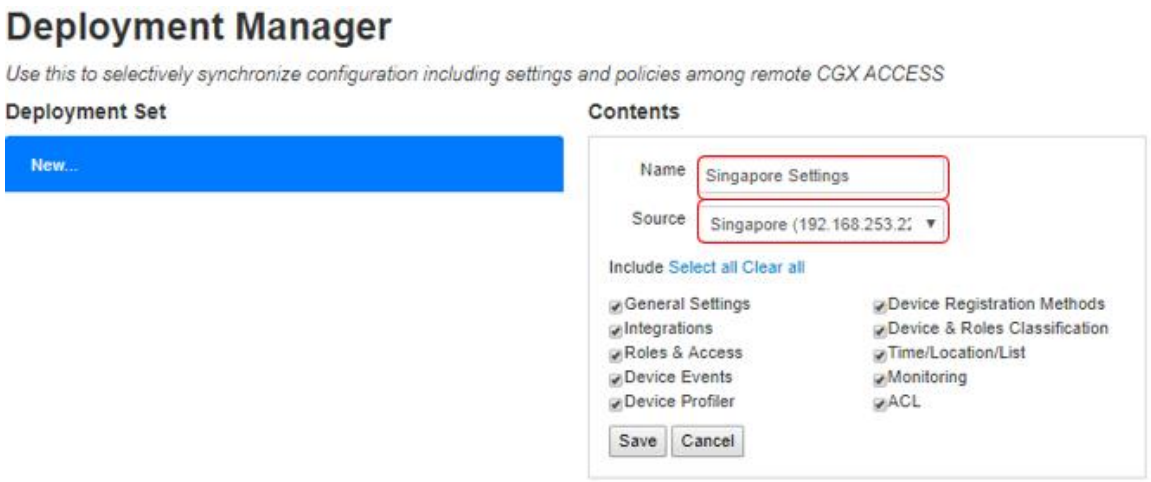



- Click **Submit**. You will be logged out of CGX-Access and the changes will take effect.
- Within two minutes endpoint state should be replicated to the Central Visibility Management Server.

# Deployment Manager

The Central Visibility Manager includes a Deployment Manager that is used to accelerate deployments or configuration changes among different CGX Access appliances.

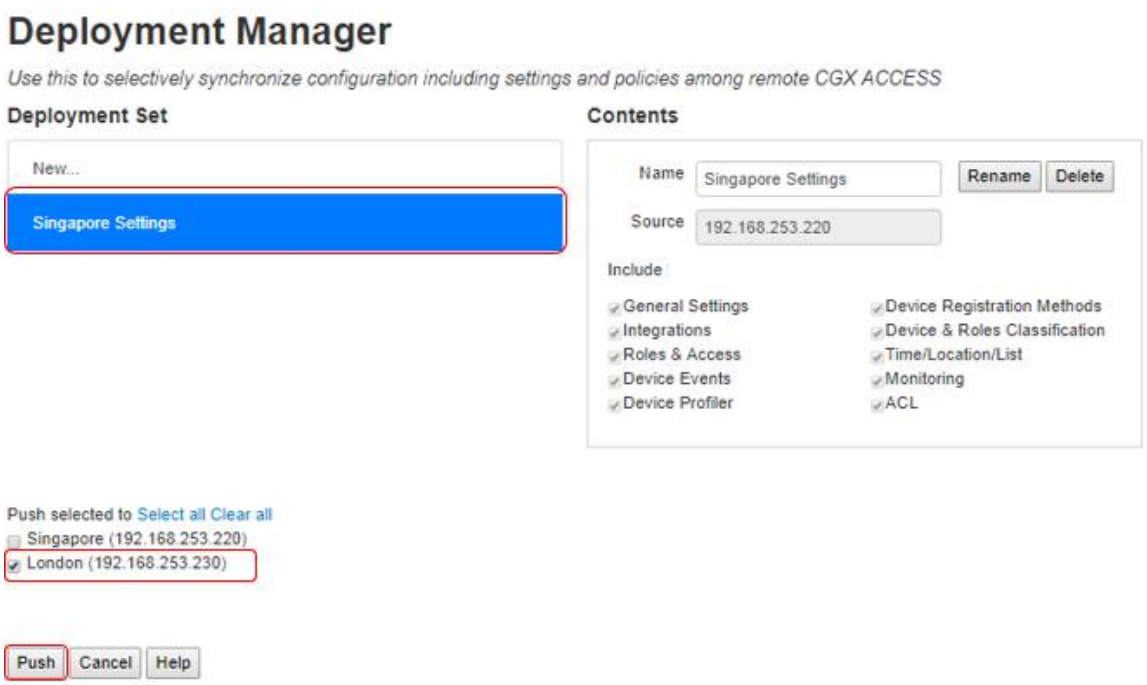
- In CVM GUI go to Configuration → Deployment Manager
- Create a Deployment Set



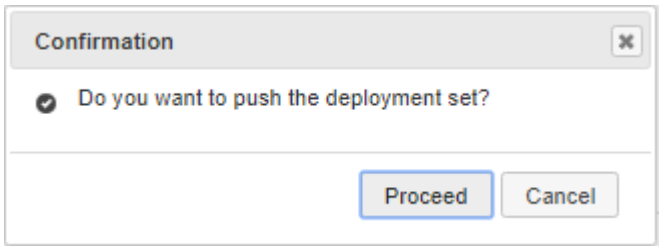

1. Specify a name
2. Select the Source appliance to copy the settings from
3. Choose which settings to include in the Deployment set
4. Click Save

- Push a Deployment Set

1. Select a Deployment Set
2. Select the location(s) to push to
3. Click Push



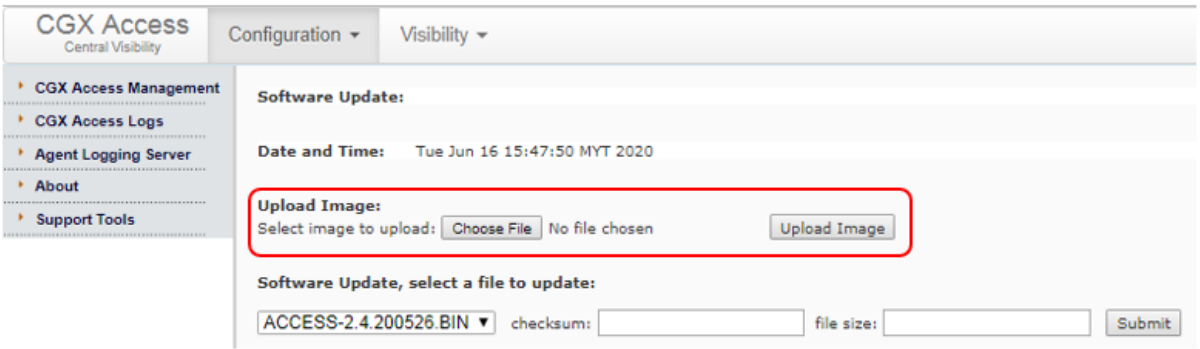

4. Confirm the Push



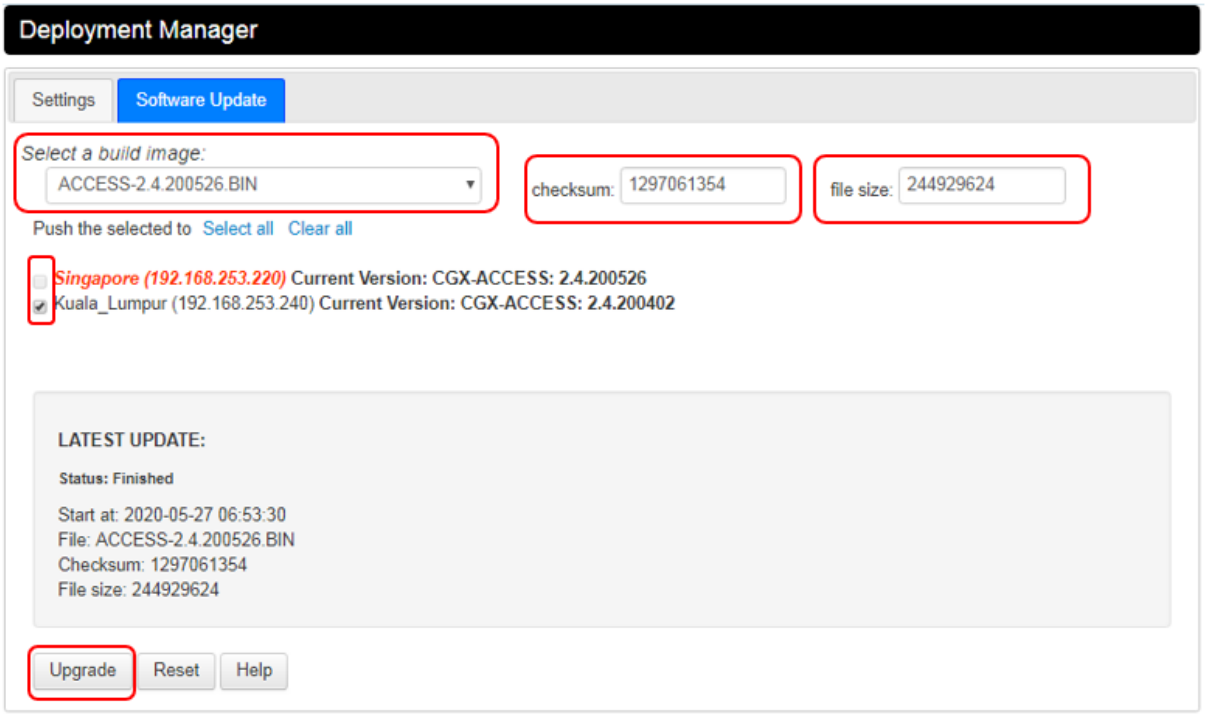

## Software Updates

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**



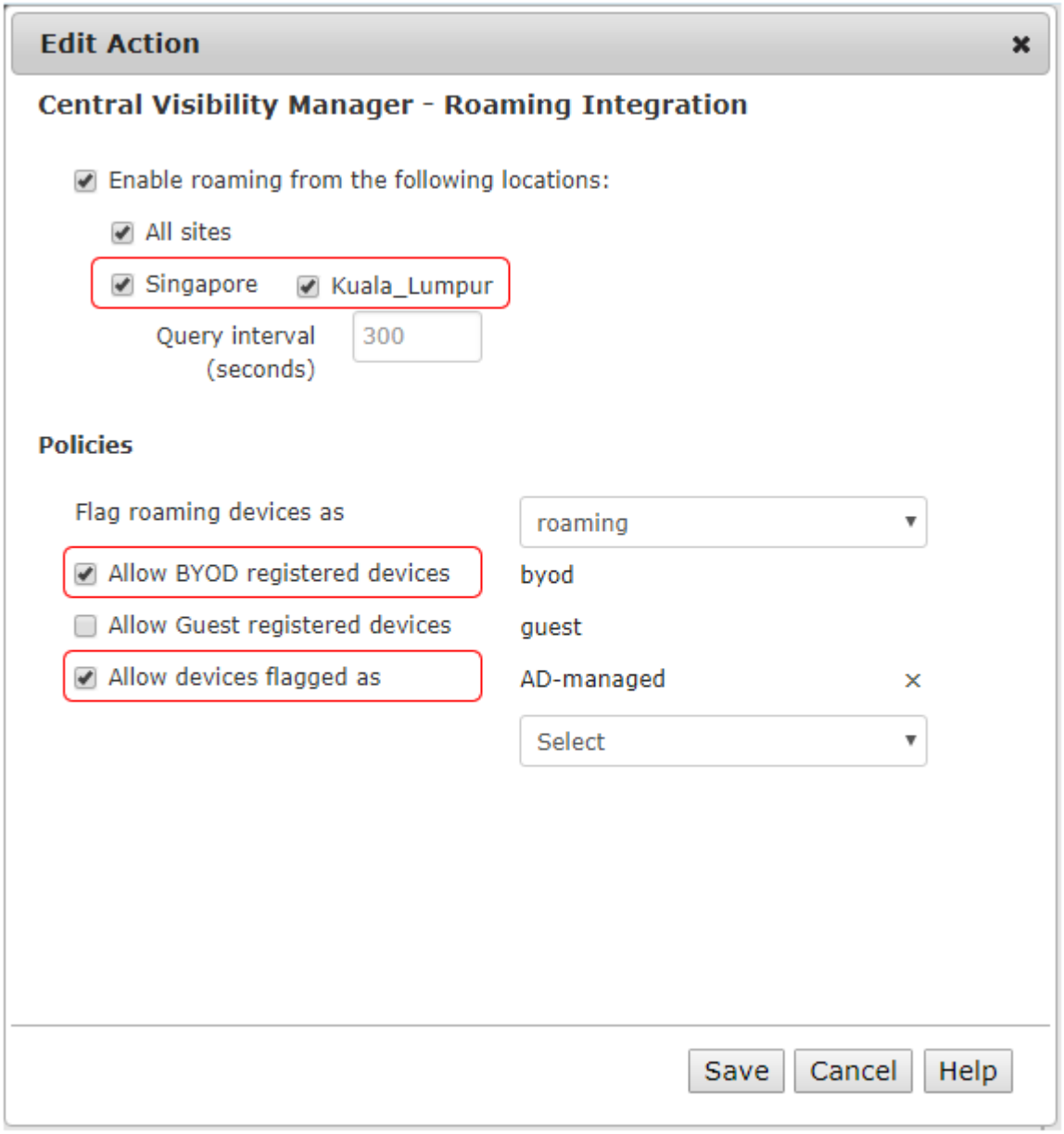

The images will be downloaded to the appliances and if the Checksum and file size are accurate, each appliance will upgrade. Allow 5-15 minutes for upgrades to occur. Remote appliances will be rebooted after upgraded

**Note:** The CVM should use the same software version as the remotes. As a best practice, it's recommended to first upgrade the CVM, before pushing the upgrade to remote appliances.

# 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 Remote, 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




In the above example, only “BYOD” registered devices and devices flagged as “AD-Managed” will be allowed to roam from either of the sites. These roaming devices will be flagged “Roaming”, so using this “Roaming” flag, the devices can be assigned limited access to the network, as desired.

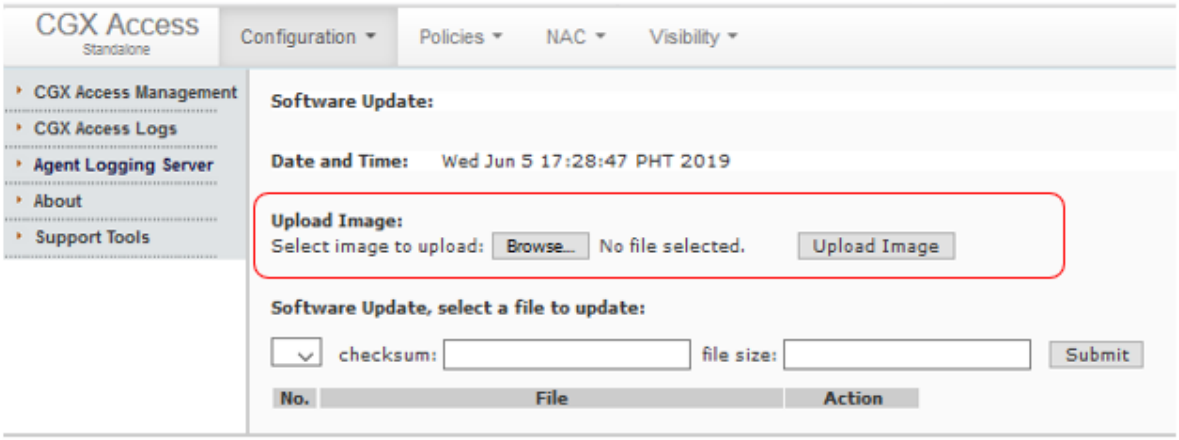
# Maintenance and Support

## Upgrading firmware

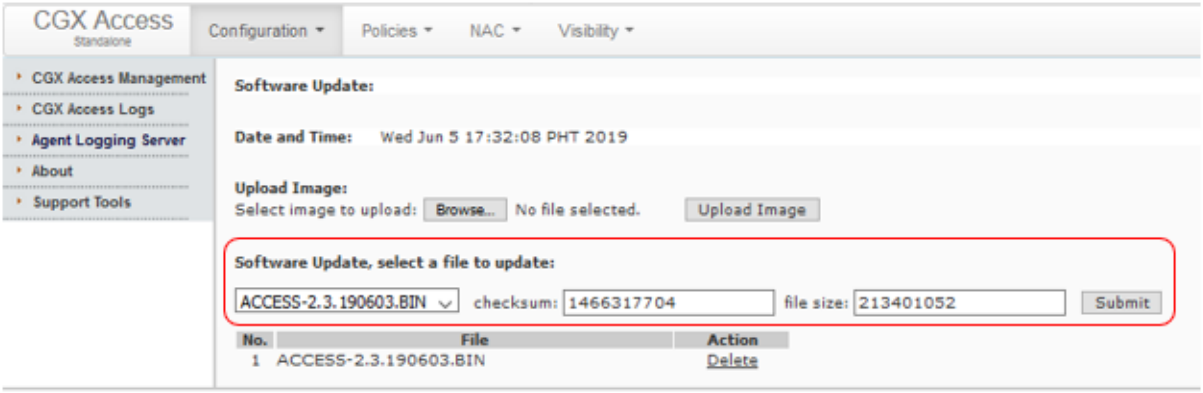
Firmware updates may be provided by InfoExpress to upgrade the CGX Access with new functionalities or fix existing issues. A binary update file (BIN file) will be provided with a checksum and file size. An example of the BIN file may be CGX-Access-2.3.190301.BIN, with a checksum of 1067271049 and file size of 195473389.

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




- Once uploaded, complete checksum: and file size: then **Submit**




The CGX Access will warn of loss of connectivity, and then may ask for a reboot. Connectivity will be lost, and you will have to reconnect if an SSH session was used. Allow 5-15 minutes for upgrade to occur.

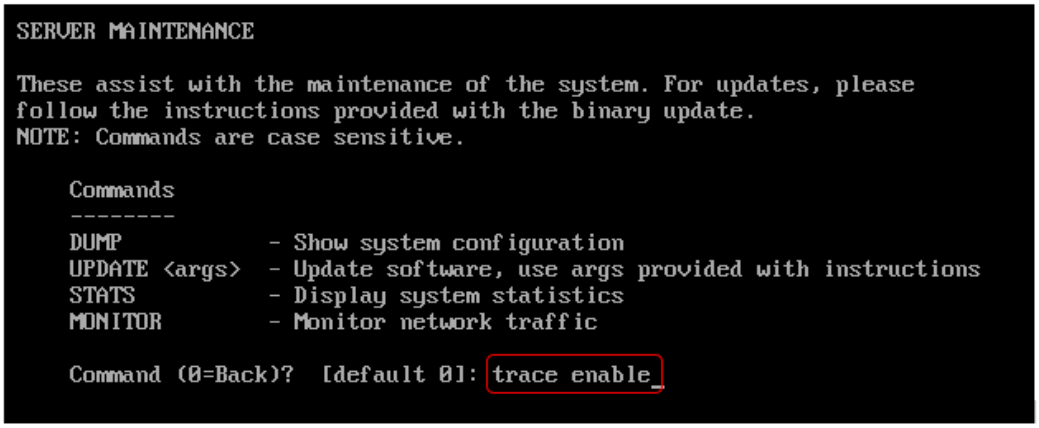
# Collecting Logs (Dump2)

For troubleshooting purposes, InfoExpress support may ask administrators to collect Dump2 Logs.

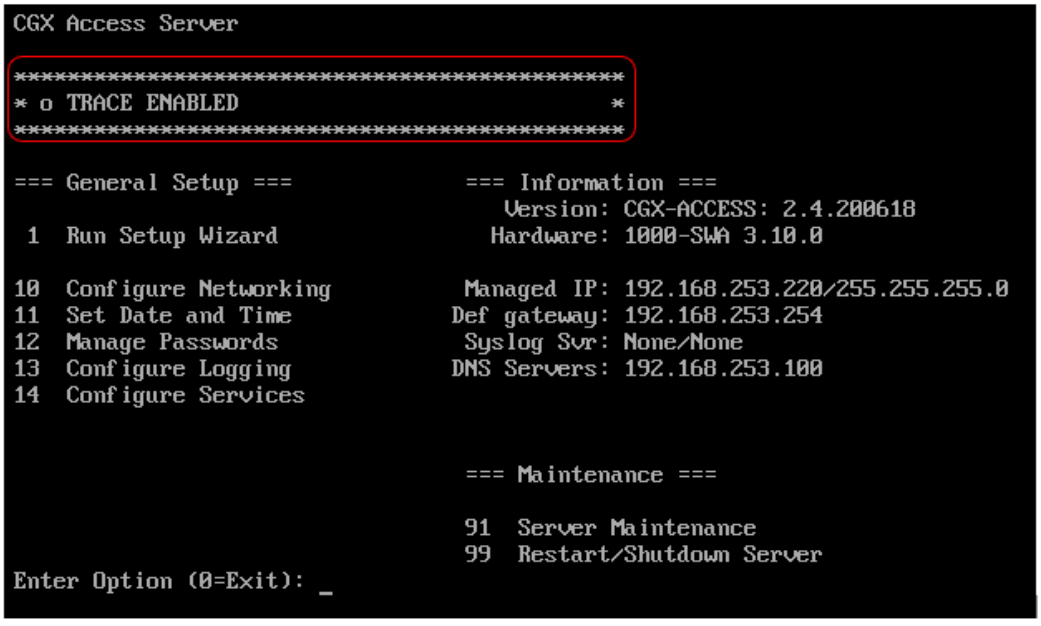
**Note:** Before collecting dump2 logs, please check with Support if you need to enable debug logging and the duration of logging required.

**Enable Debug Logging**

- In CGX Access SSH Console, use Option 91 - Server Maintenance
- Type “trace enable”




- Confirm TRACE ENABLED is shown at the top of the SSH Console

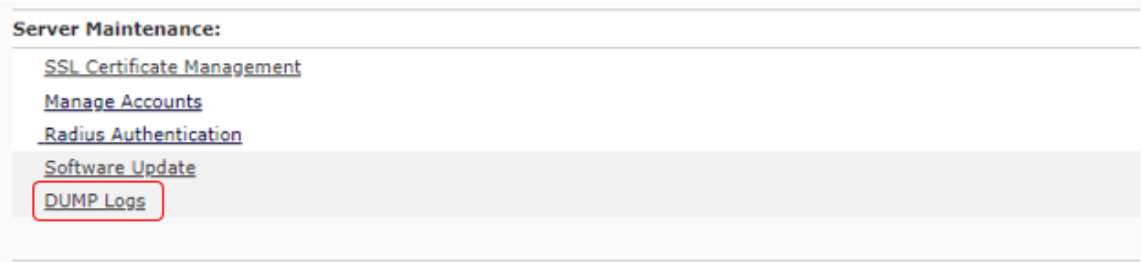



- Wait for few minutes, as advised by Support, before collecting the logs.

**Note:** Collecting the logs will disable Trace Enable

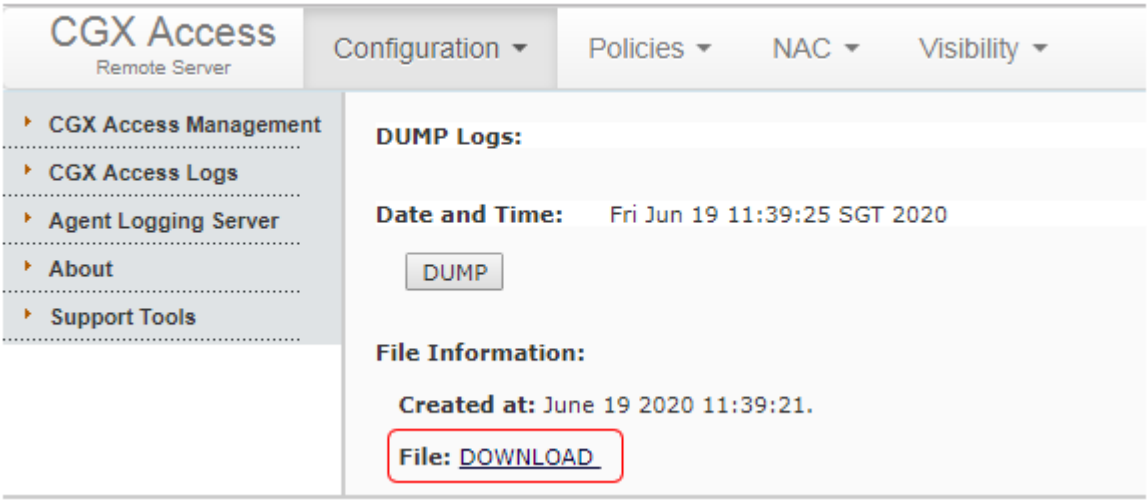
**Collecting Logs (Web GUI method)**

- In CGX Access GUI, go to Configuration → Appliance Settings
- Scroll down to Server Maintenance → Dump Logs




- Click the DUMP button and confirm dump

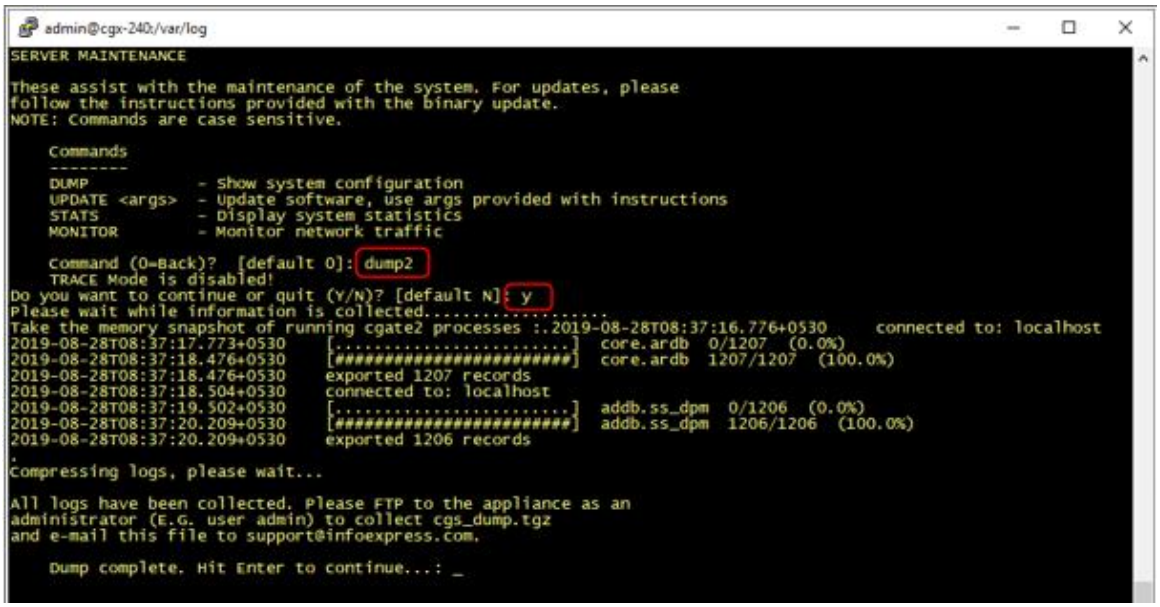

- Wait for Dump process to complete – It may take 5 to 15 minutes depending on number of endpoints. Longer if the system has had core dumps.
- Once complete, download the file and send to support.



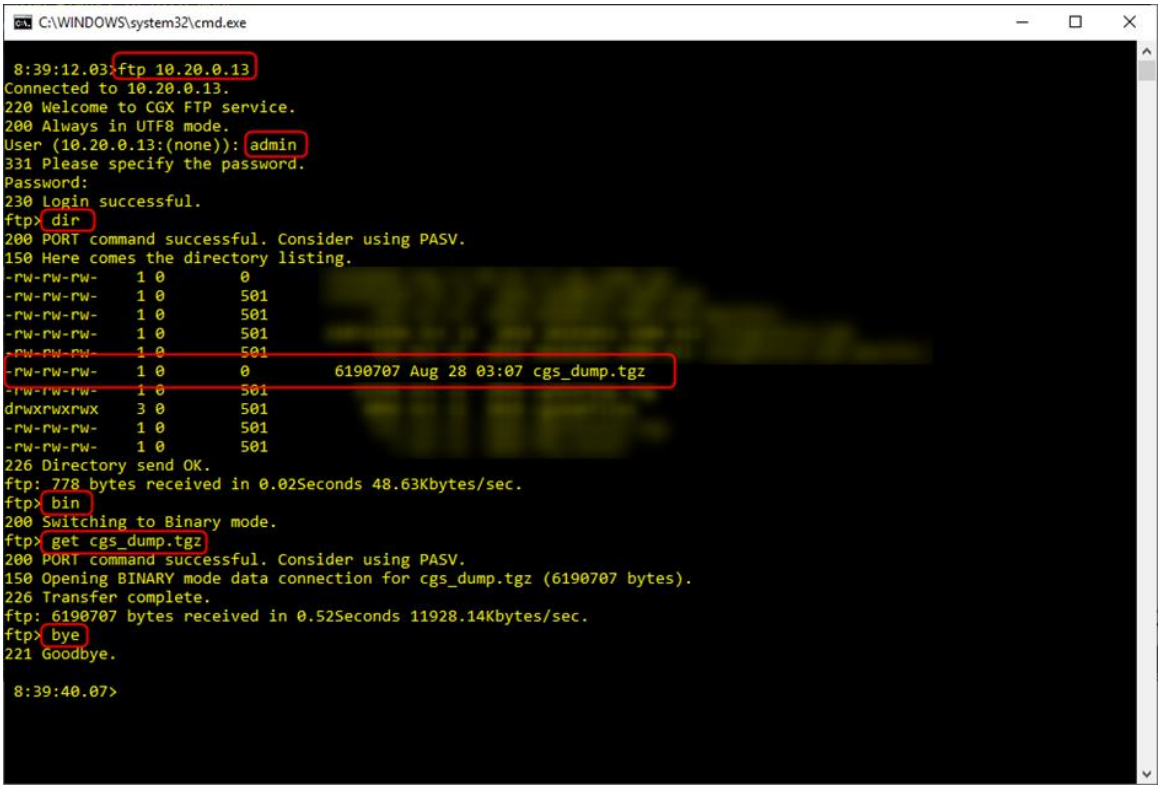

**Note:** If the web interface is not available, the SSH CLI method can be use to collect the logs.

**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.




- FTP to CGX Access appliance with Admin account to download the logs and send to support.



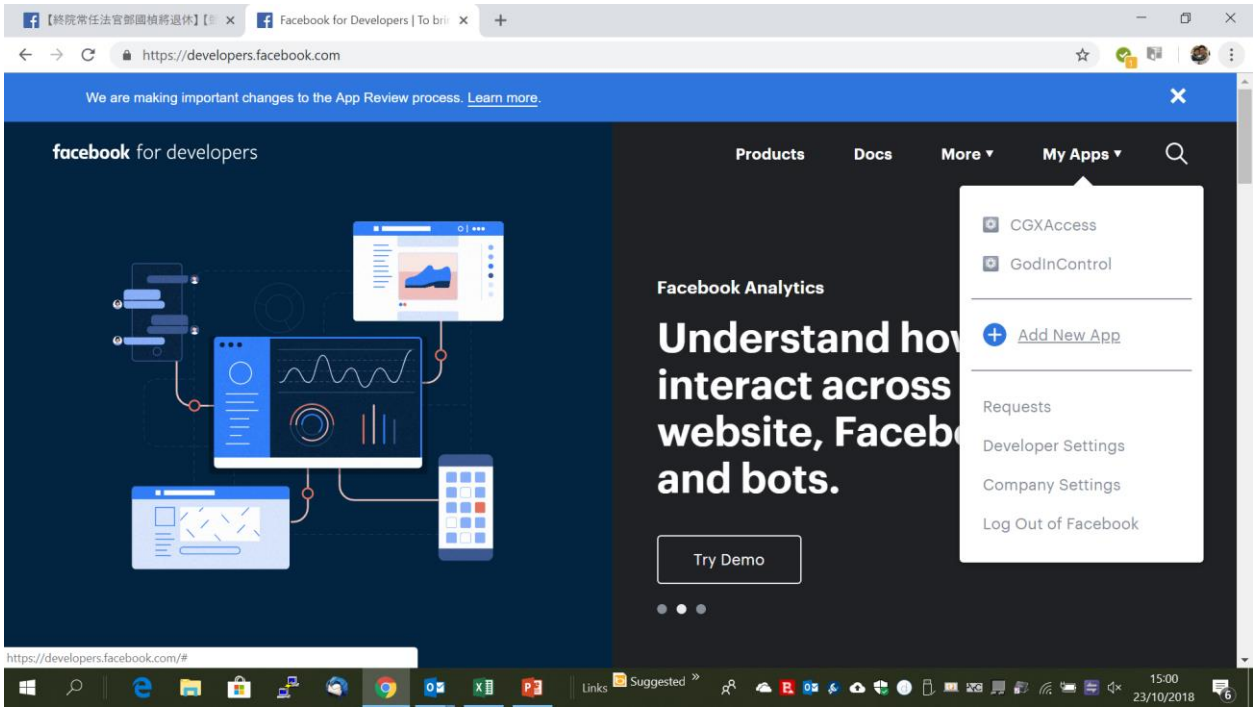
# Appendix A – Facebook Login App Setup

CGX Access can authenticate a guest user via their Facebook account. Technically, Facebook allows authentication to a Facebook App only. For the authentication to work, we would need to create a Facebook app for your installation.

To do so, first login your browser with a Facebook account. This is the account that would be able to see all the login user sessions. It is recommended to have a new account setup and don't use a personal account for this function.

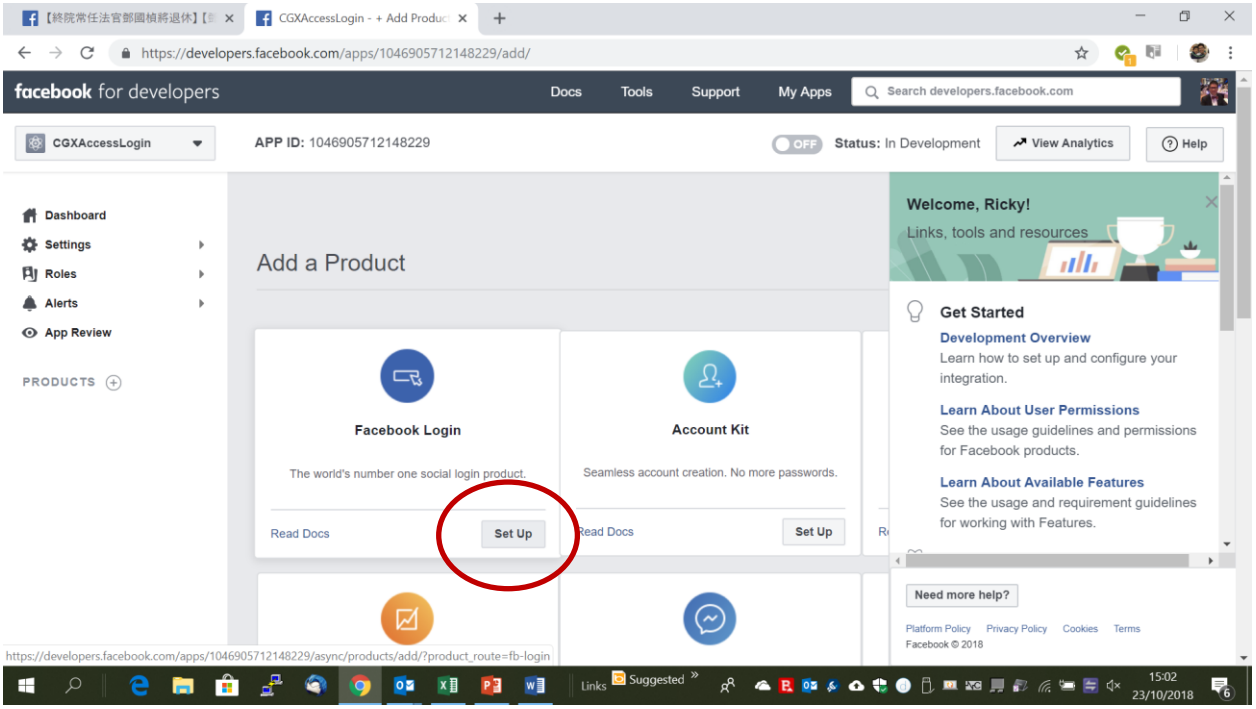
Then visit http://developer.facebook.com You will then see a screen similar to below.

- Select My Apps → Add New App
- Give a name for your App and confirm.

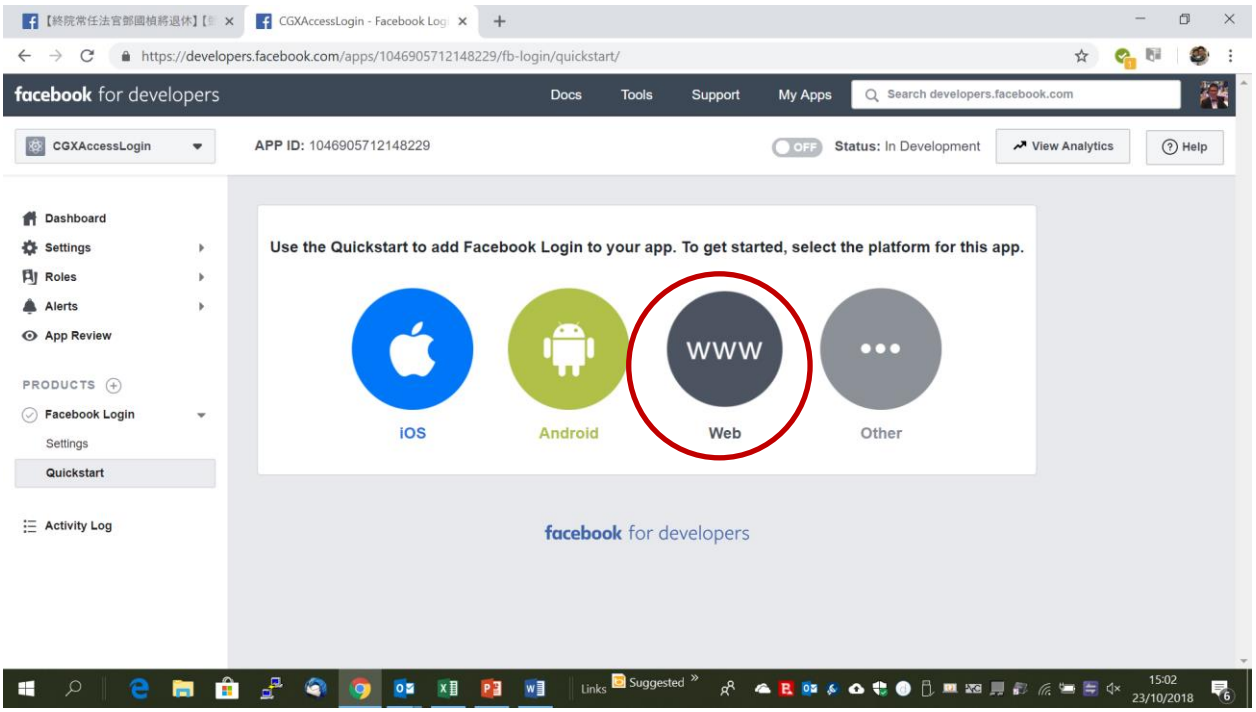


You should then be able to see your name of the App showing on the upper left-hand corner and would see a similar screen below

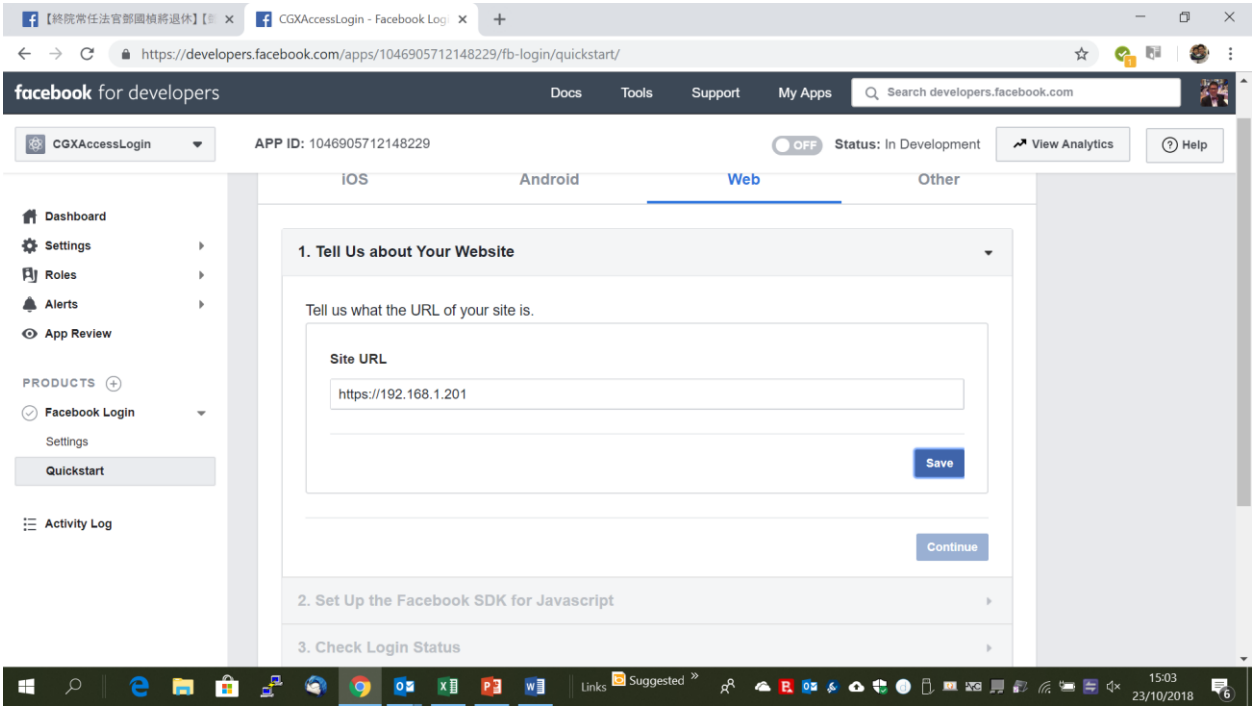
- Select the “Set Up” button in Facebook Login



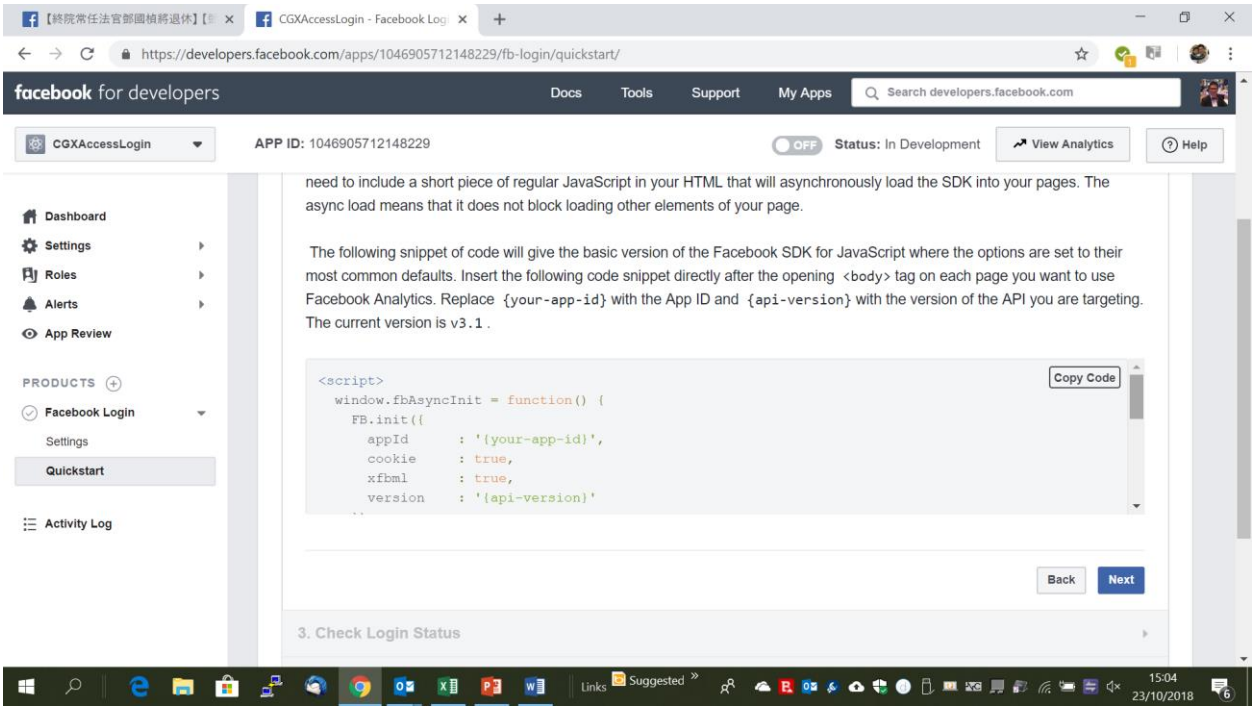

- Select web “WWW”



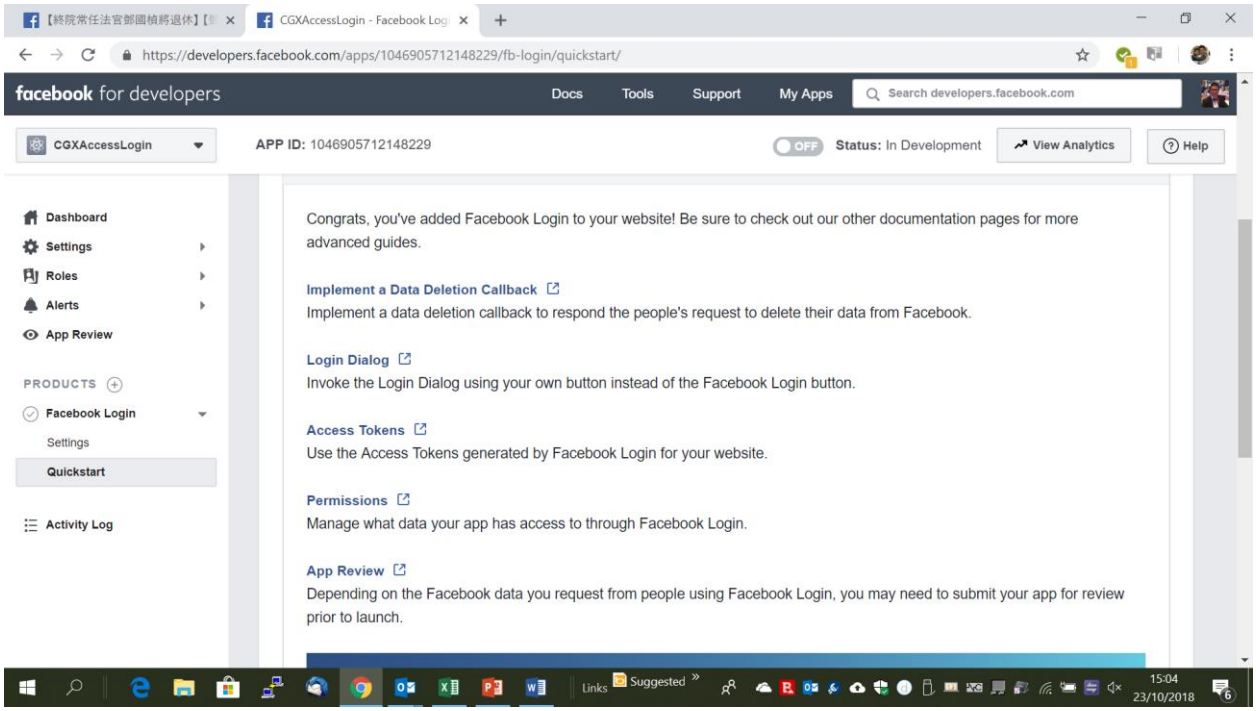
- Site URL: Should be replaced with the URL of your CGX Access Captive Portal




- Click SAVE and Continue

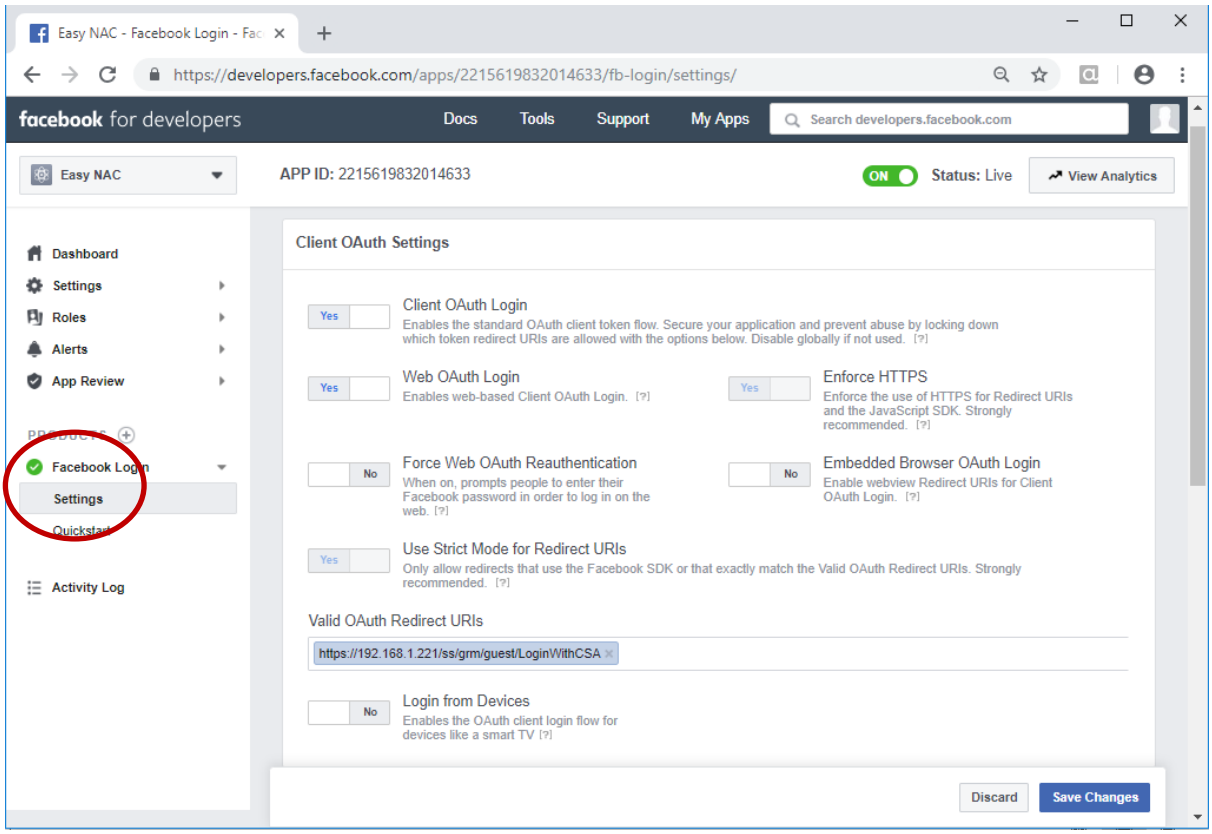



- Click Next Until you see this Page



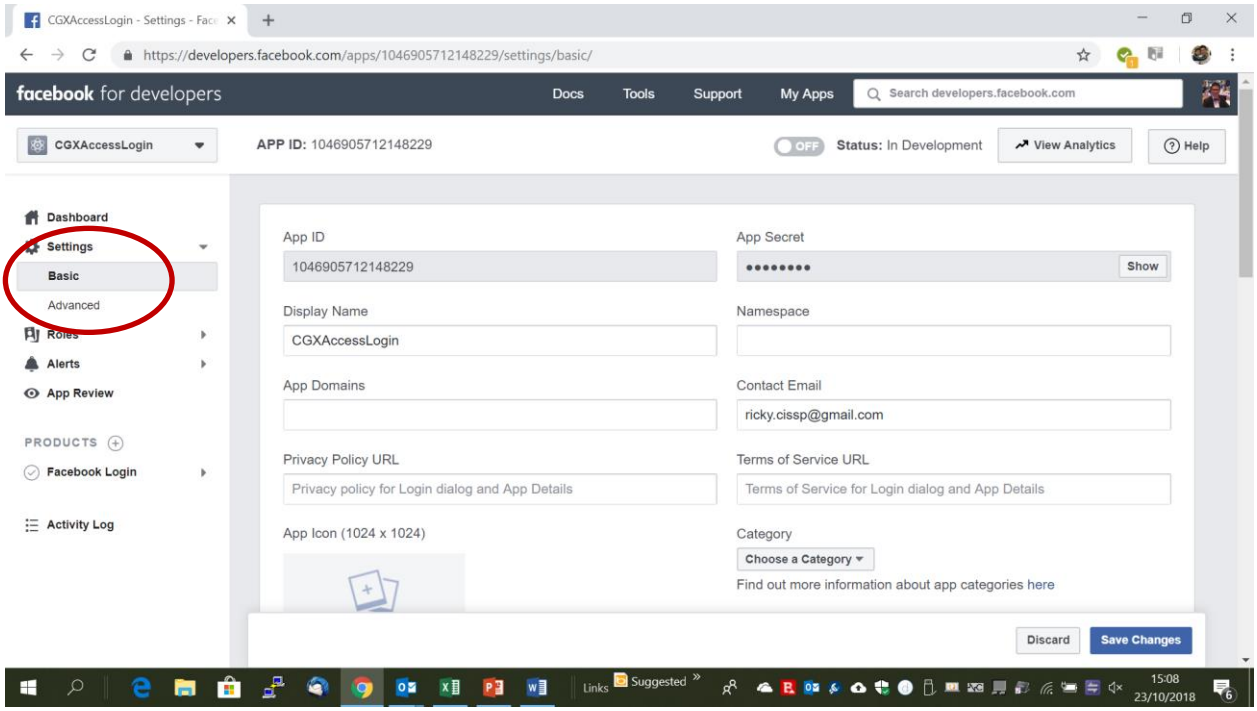

Under Facebook Login on the left

- Select “Settings”

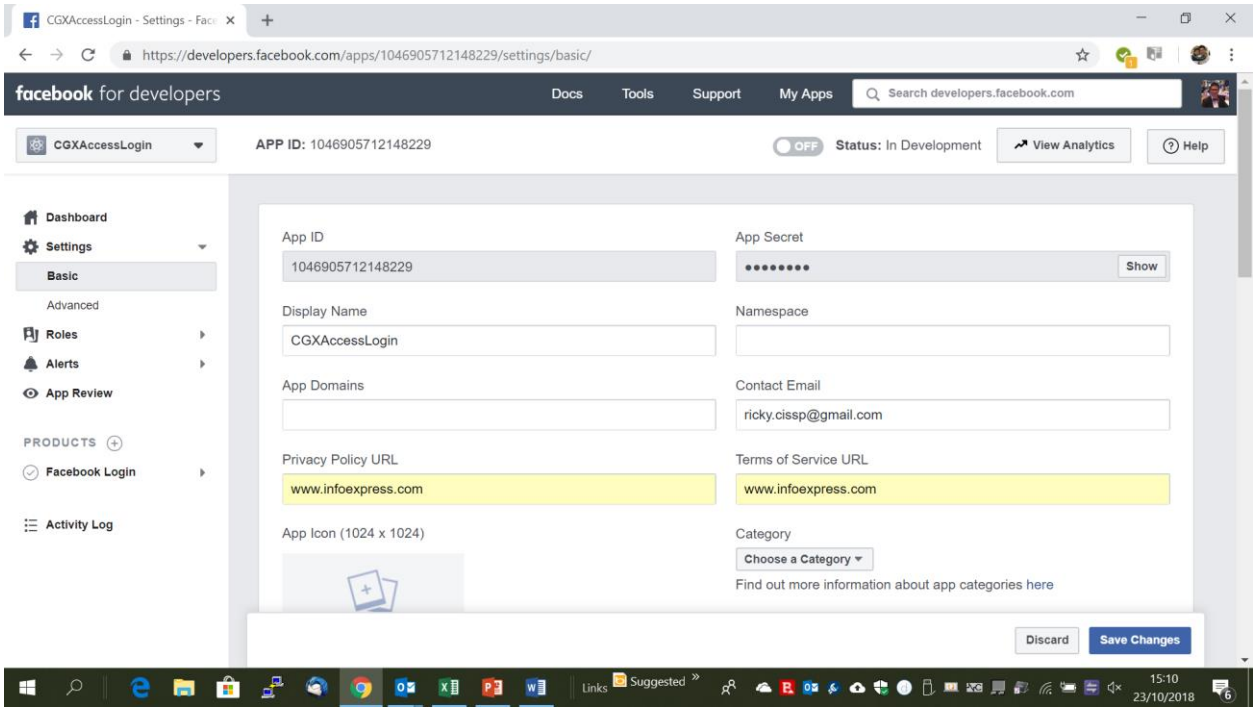



- Change the Valid OAuth Redirect URIs to https://captive_portal_ip/ss/grm/guest/LoginWithCSA

- Replace the CAPTIVE_PORTAL_IP with your captive portal IP. The URL above is also case sensitive.
- Save changes
- Navigate to the Basic under the Settings

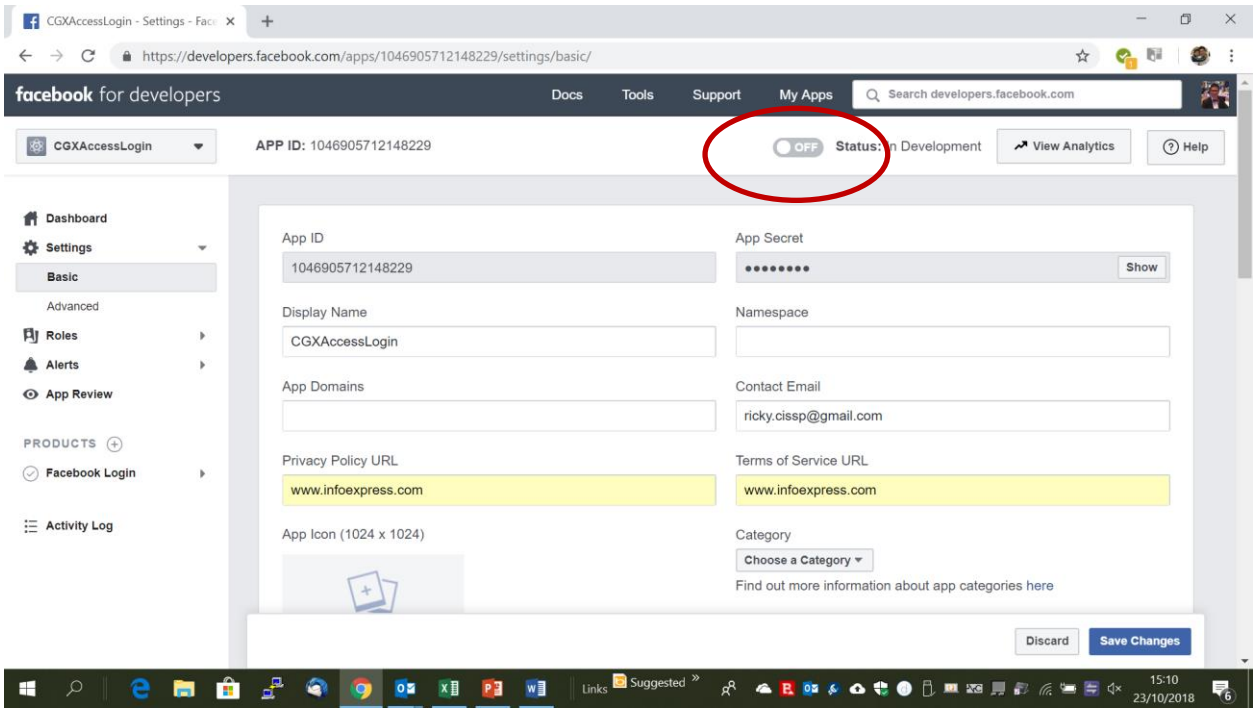



- Copy the AppID and App Secret. We will need it for the configuration of the CGX Access later.

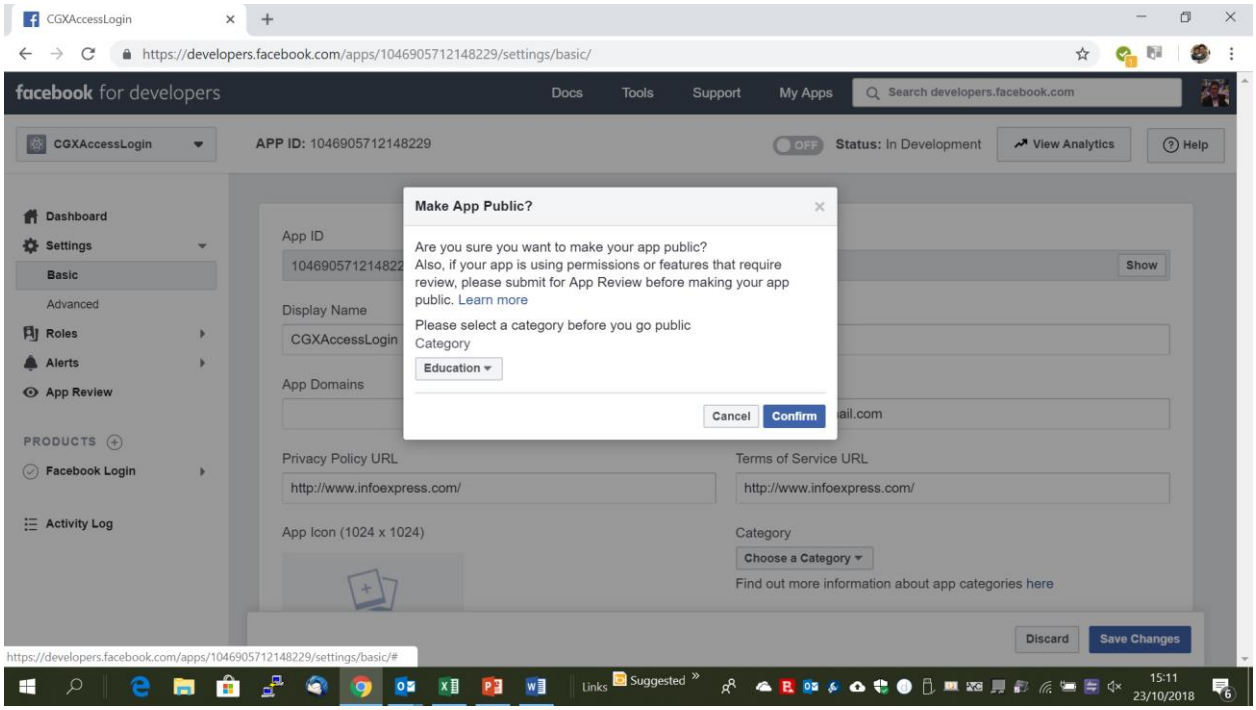



- Configure the Privacy Policy URL and the Terms of service URL as necessary.

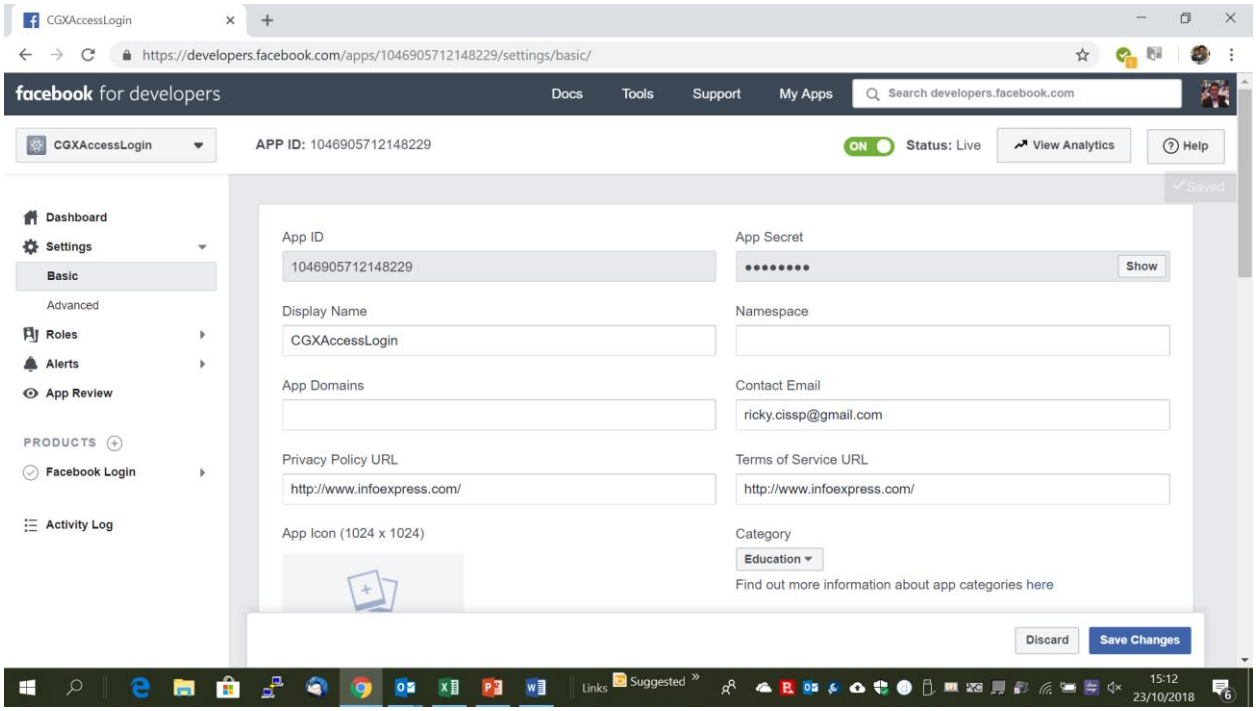
- Save Changes




- Click the ON/OFF switch next to the APP ID: above. This would prompt you the screen below

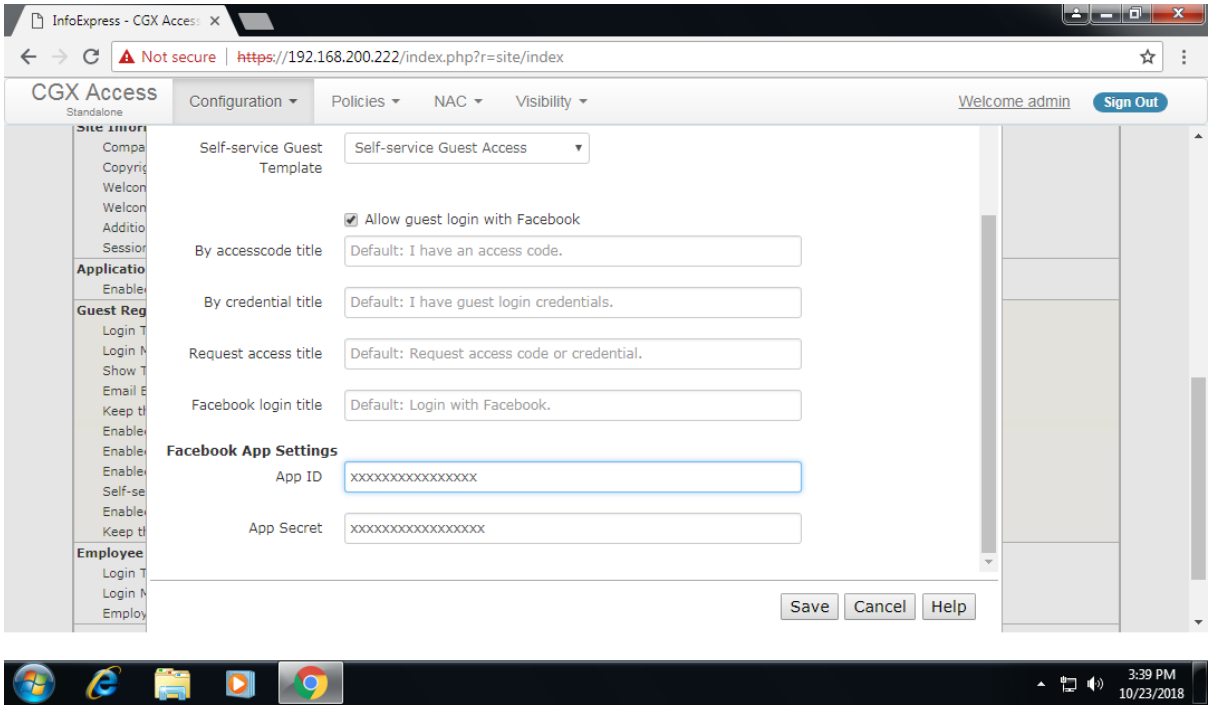



- Select a category that might fit and click Confirm and then Save Changes

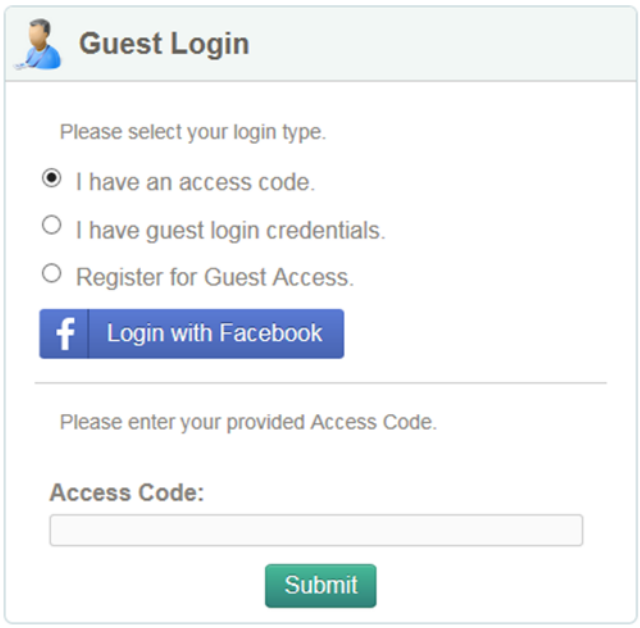



- The app is now in product. We would need to setup CGX Access now

- Login to CGX Access and under Configuration → General Settings → Guest Registration
- Check the box "Allow guest login with Facebook"
- Copy your AppID and App Secret here from your Facebook app created above.




- Click Save and you should now see the Login with Facebook button in the Captive Portal.




**NOTE**: The ACL use to restrict pending guests, must allow both DNS and internet access to Facebook. InfoExpress has provide a default ACL named “Restrict-FaceB”.

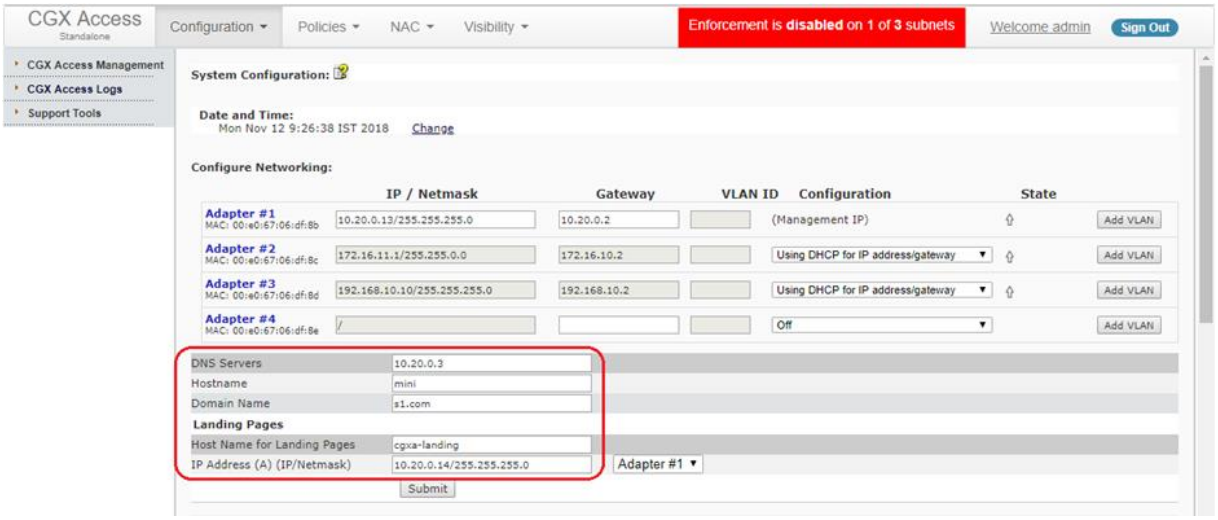
# Appendix B – Certificate Management

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

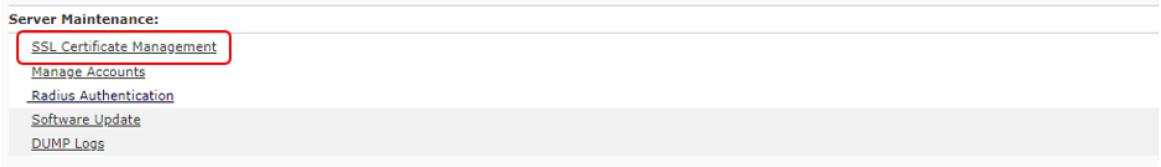
**Please note:** CGX Access could be using 3 hostnames, one for management-IP, Captive portal, and Remediation portal. Therefore, it is advised that you create a wildcard certificate. (*.domain.com)

- 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

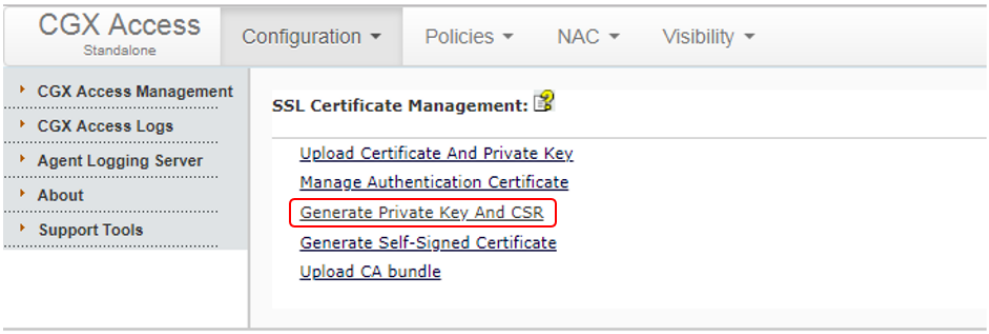



**Note:** Hostnames should match as to be entered in the certificate. Some settings may not be configurable until DNS server and Domain name is configured.

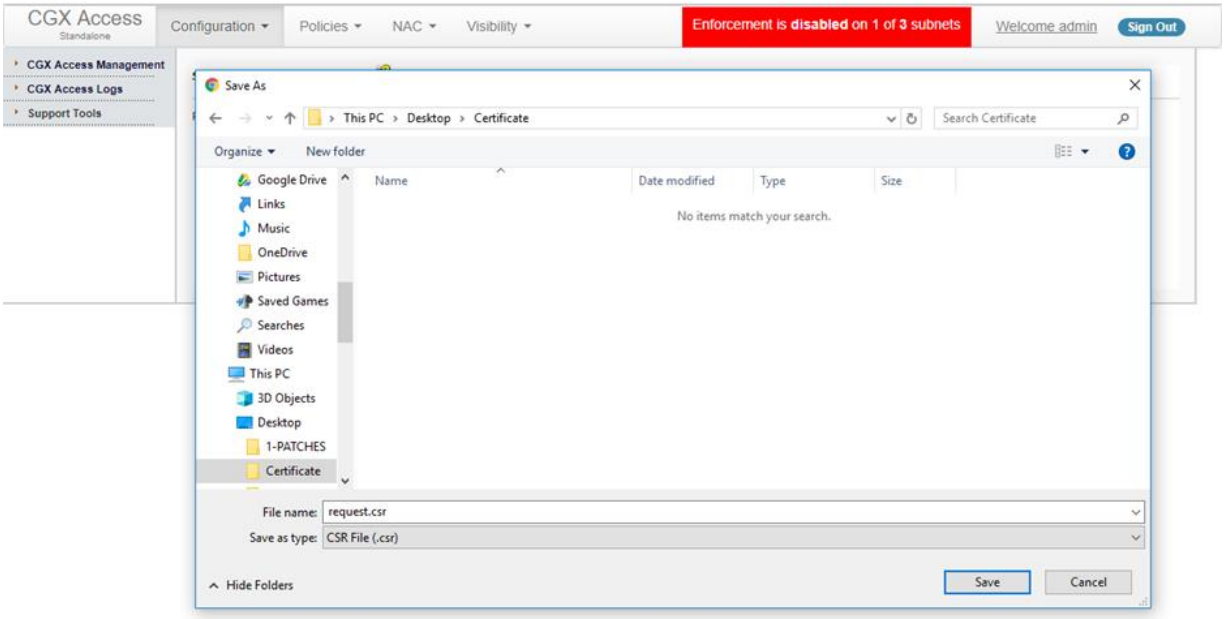
- Scroll down and Click **SSL Certificate Management**



- Click on **Generate Private Key and CSR**



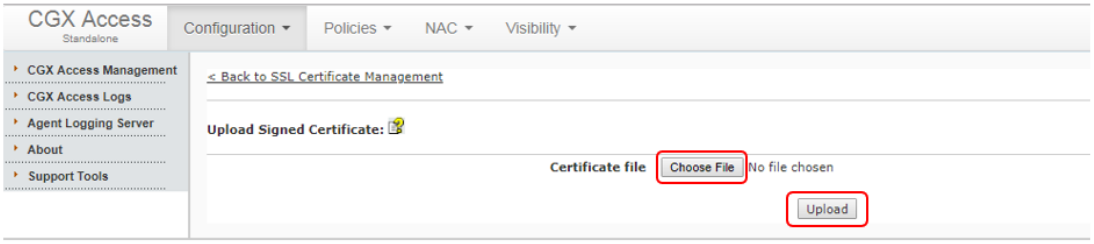

- Enter required details and click on **Generate**

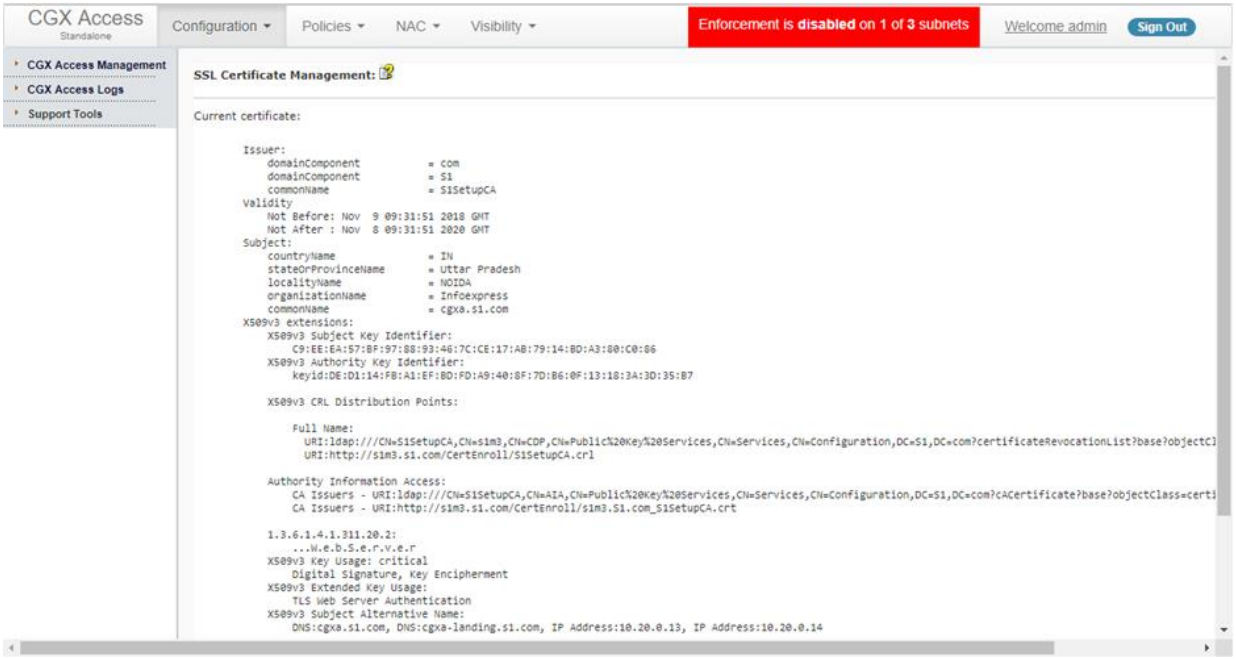

- Save the generated CSR
- Provide the CSR to certification authority (CA) to generate the certificate

- Once you obtain the certificate from CA, Click on **Upload signed certificate**


- Choose certificate file to and upload

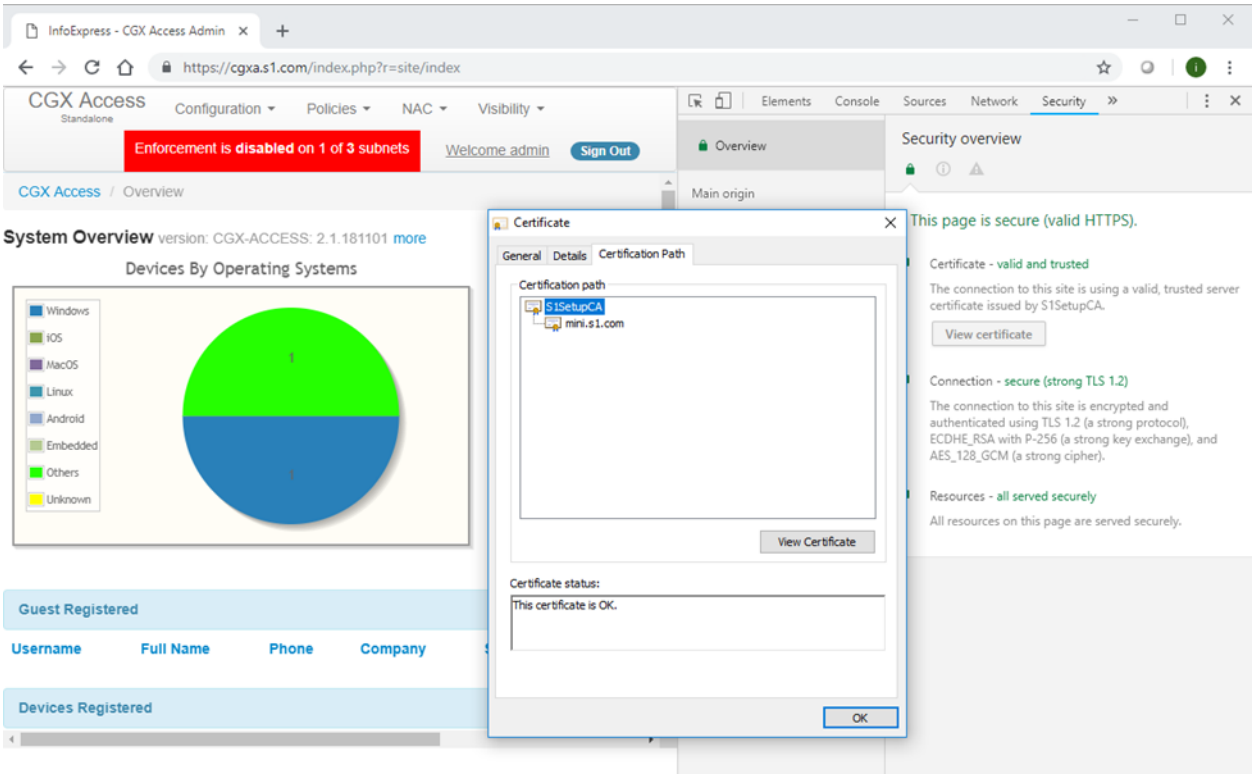



- New certificate will be uploaded and details will be shown

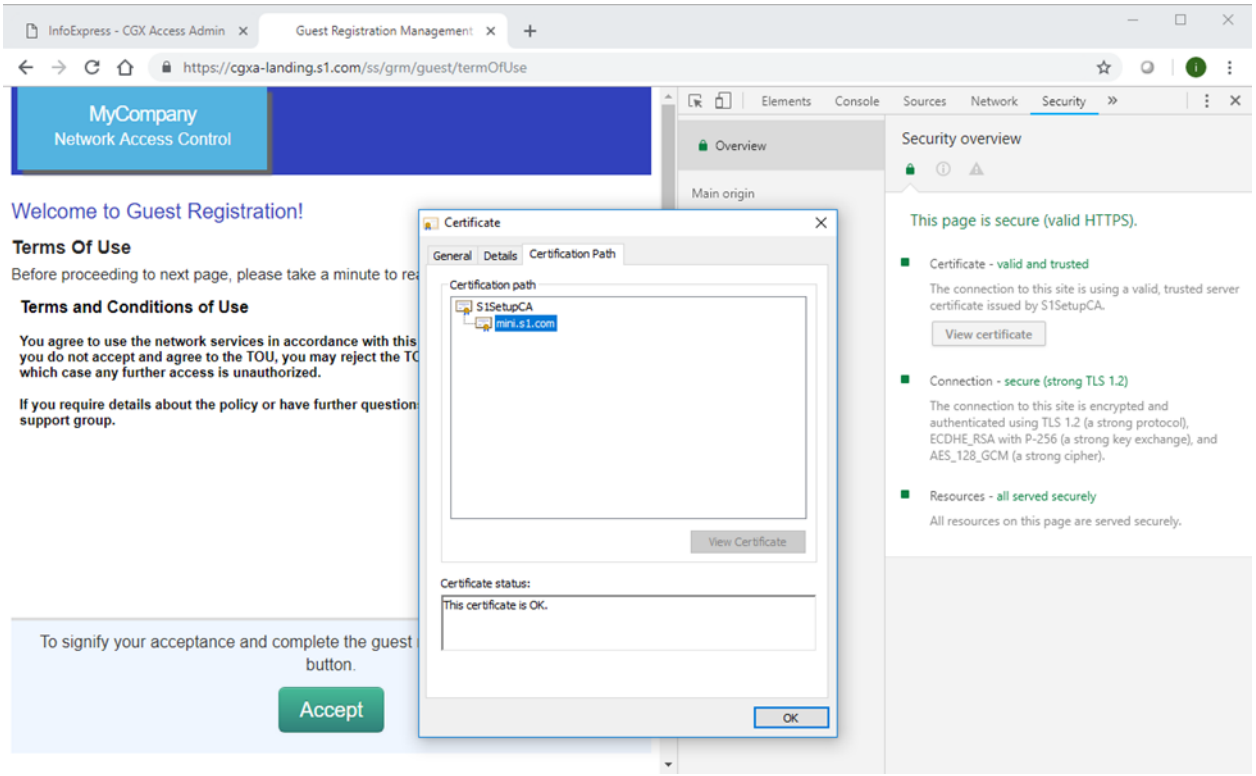



- Reboot CGX Access for new certificate to take effect

- To Check certificate, browse CGX Access using hostname



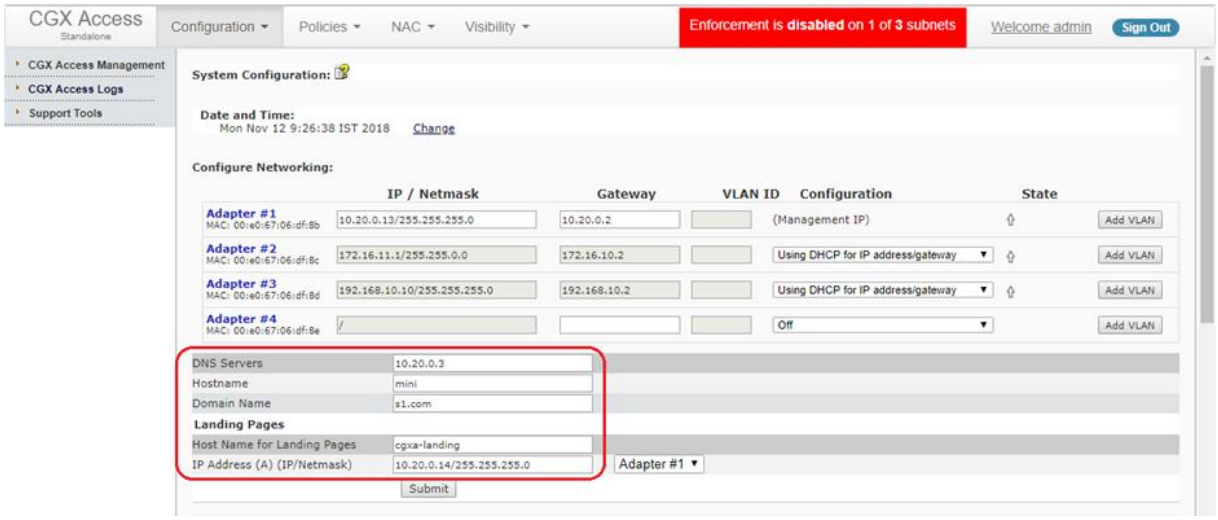

**Note:** You can also browse the Captive Portal page (This example used Subject alternative name and hence the same certificate was valid for both hostnames.)



# Option 2 - Upload certificate and private key to CGX Access. (When CSR is not generated)

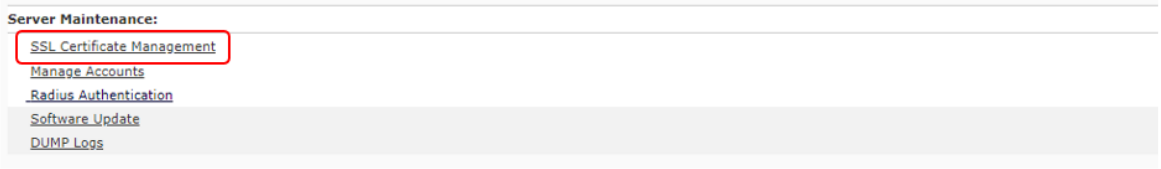
**Please note:** CGX Access could be using 3 hostnames, one for management-IP, Captive portal, and Remediation portal. Therefore, it is advised that you create a wildcard certificate. (*.domain.com)

- 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



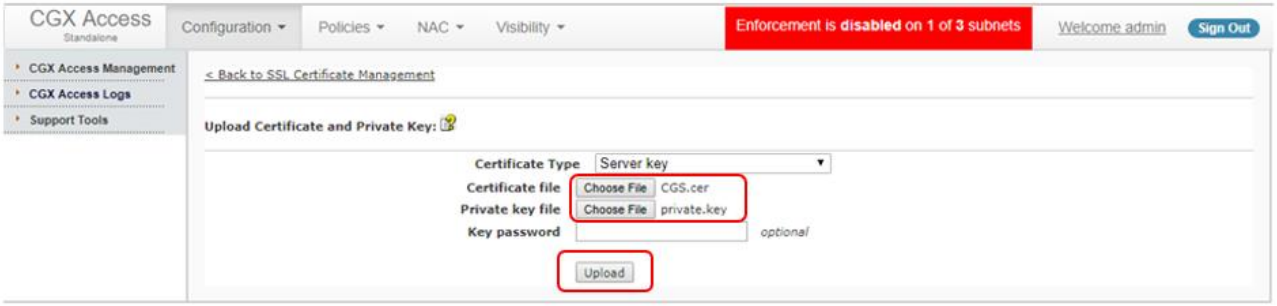

**Note:** Hostnames should match as to be entered in the certificate. Some settings may not be configurable until DNS server and Domain name is configured.

- **Scroll down and Click** SSL Certificate Management

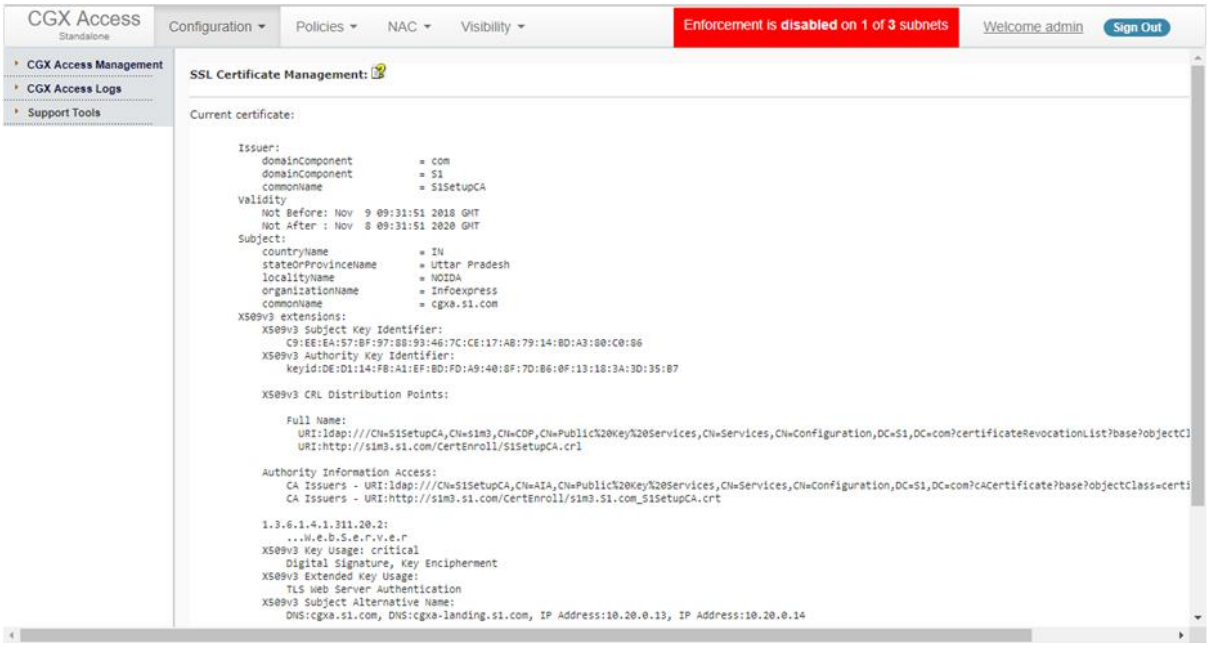


- Click on Upload Certificate and Private Key


- Choose files to upload. (Enter password if required)
- Click Upload

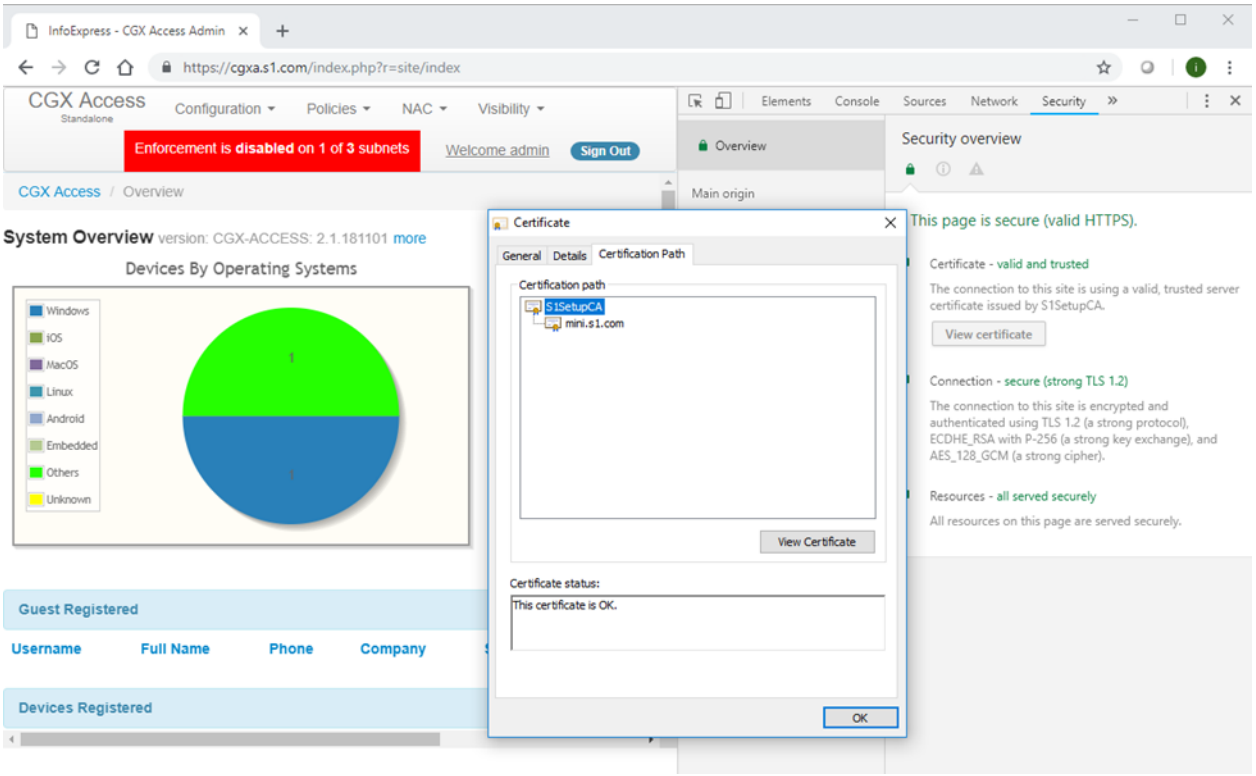



- New certificate will be uploaded and details will be shown

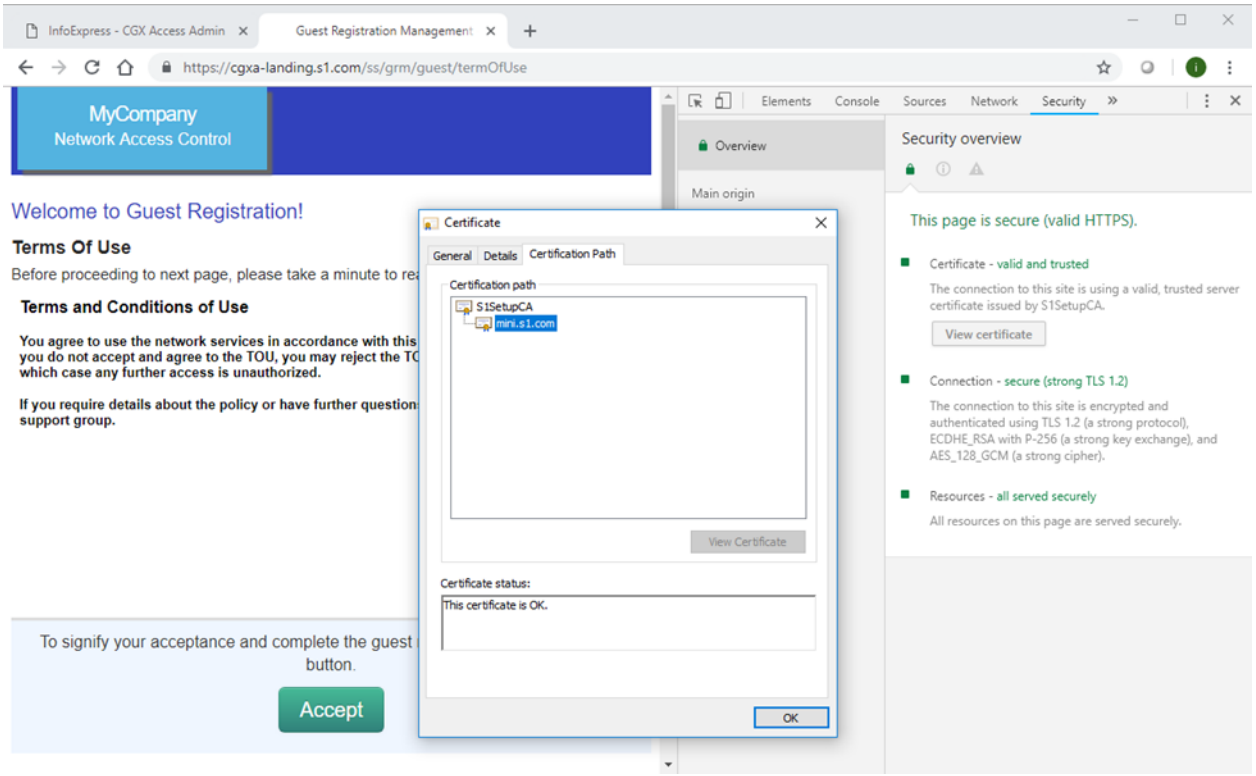



- Reboot CGX Access for new certificate to take effect

- 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.)



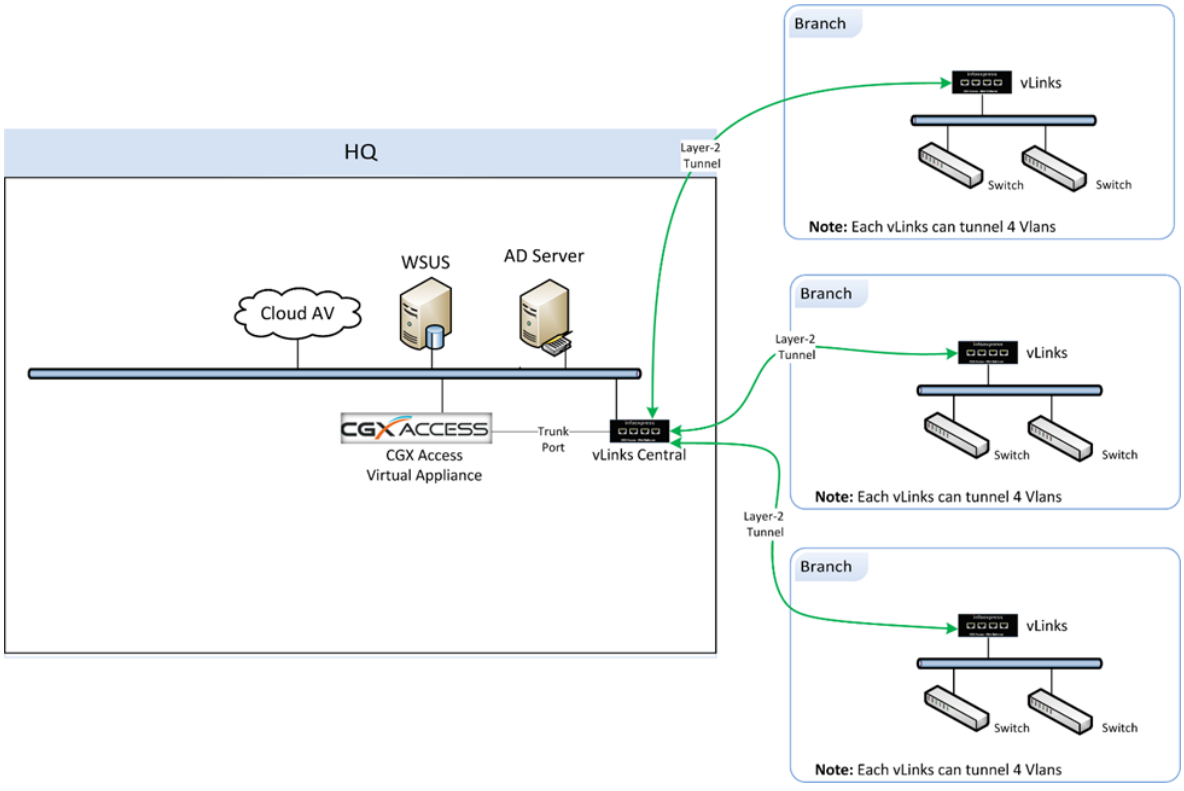
# Appendix C – vLinks Deployment

## 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.

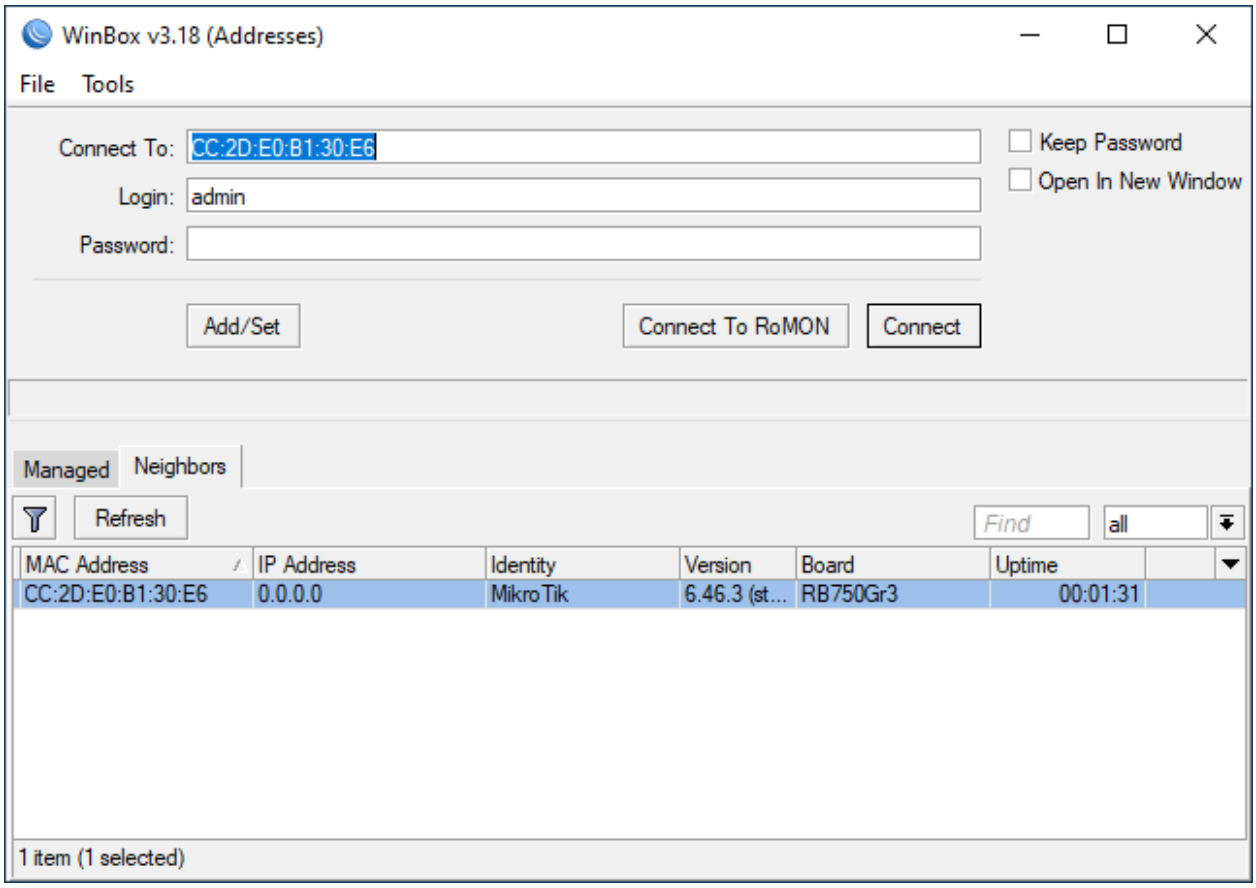
At the main site, a vLinks Central will consolidate the layer-2 traffic from multiple vLinks and share it with the CGX Access appliance using a port directly connected to the CGX Access appliance. With this connectivity in place, CGX Access will detect rogue devices at the branches and quarantine these 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

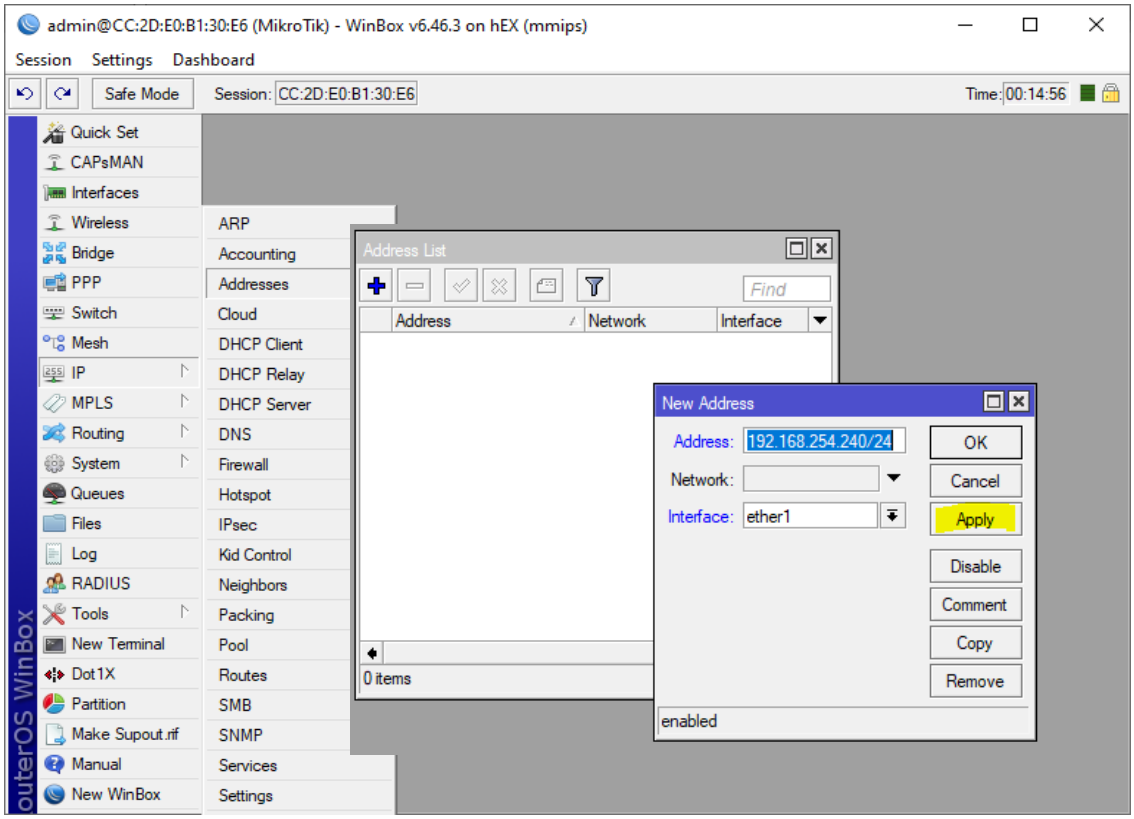
The vLinks Central hardware is manufactured by MicroTec. To configure this box, download the WinBox application at https://mikrotik.com/download. Connect the appliance (adapter 1) to your PC using an RJ45 cable and connect to it via it's MAC address or DHCP assigned IP address.



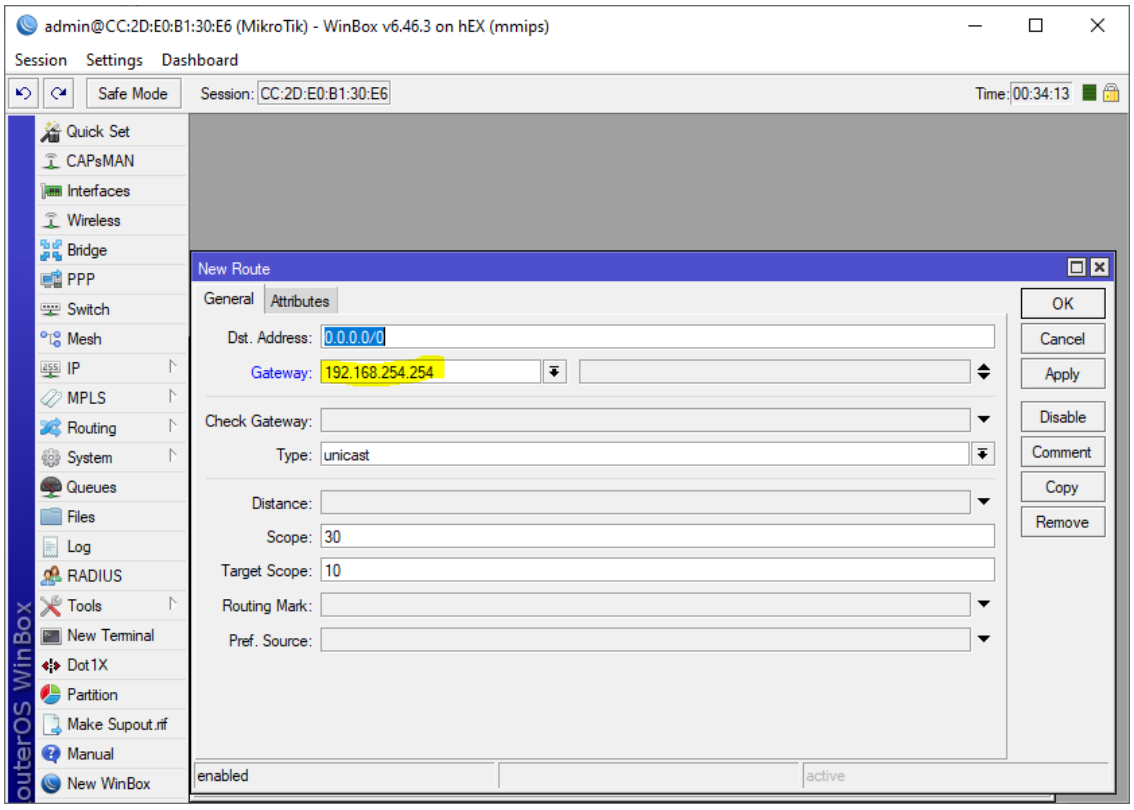

The default account is admin. The default password is blank.

Perform the following steps to assign a static IP, default gateway, and admin password:

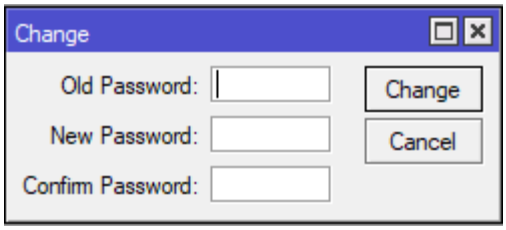
1) Configure a Static IP address - Go to: IP > Addresses >




2) Configure a default route - Go to: IP > Routes > Click +



3) Configure a password - Go to: System > Password



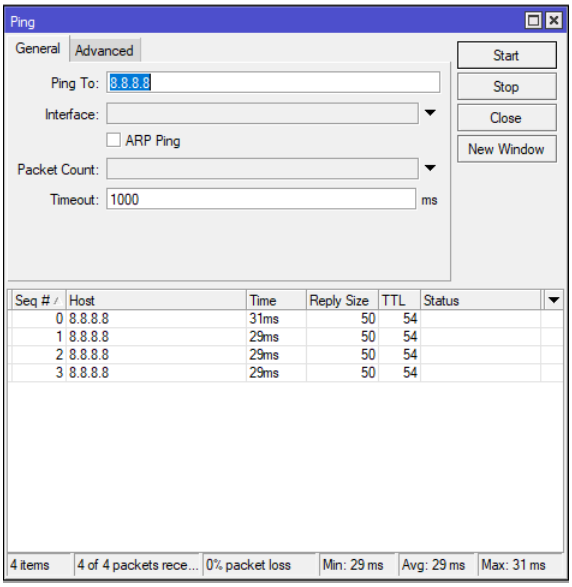

4) Shutdown box and place on the network: System > Shutdown

**Note:** Configurations changes made on vLinks Central take effect immediately, there are no added steps required to save the configurations.

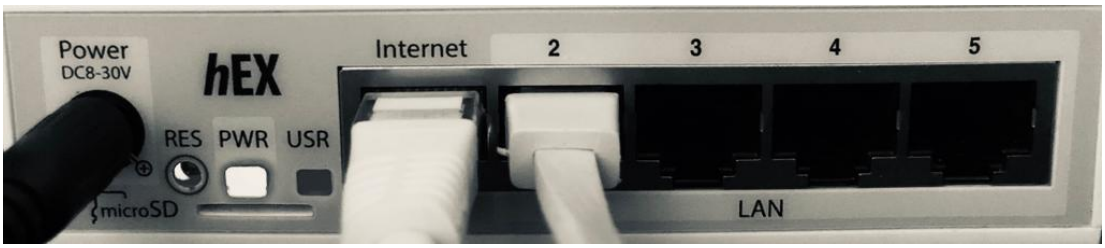
5) Physical Placement - Place the vLinks Central box on the production network using Adapter 1.


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.

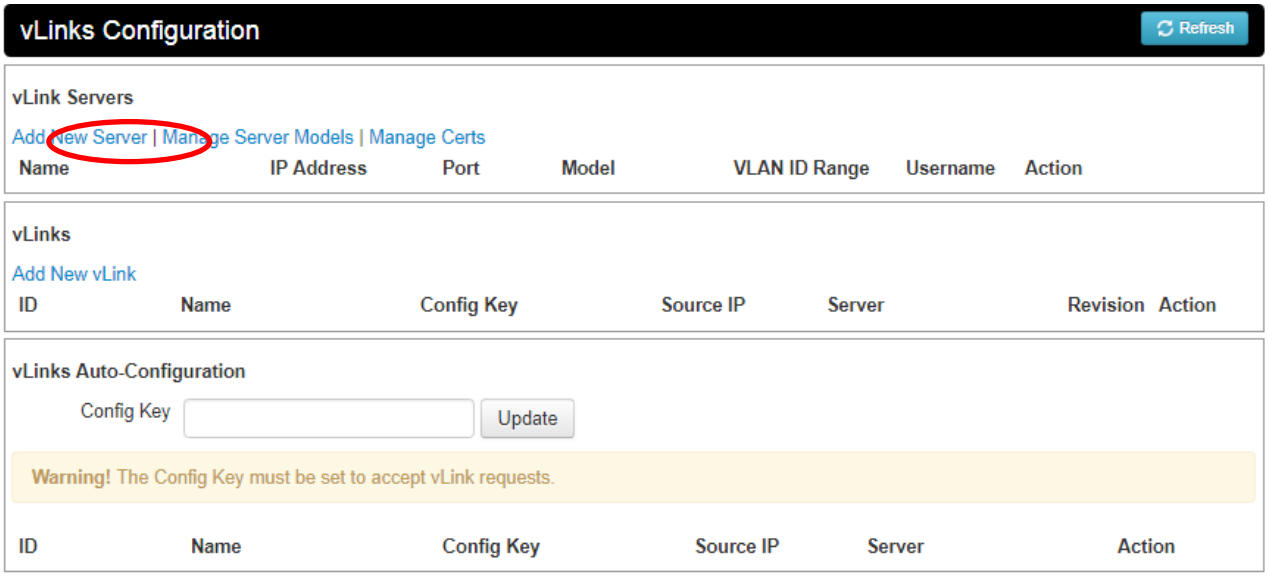


7) Connect a second cable using Adapter 2 directly into any open port on the CGX Access Appliance. Take note of the port used on the CGX Access appliance for later configuration. This is a direct connection between the vLinks Central and CGX Access appliance.

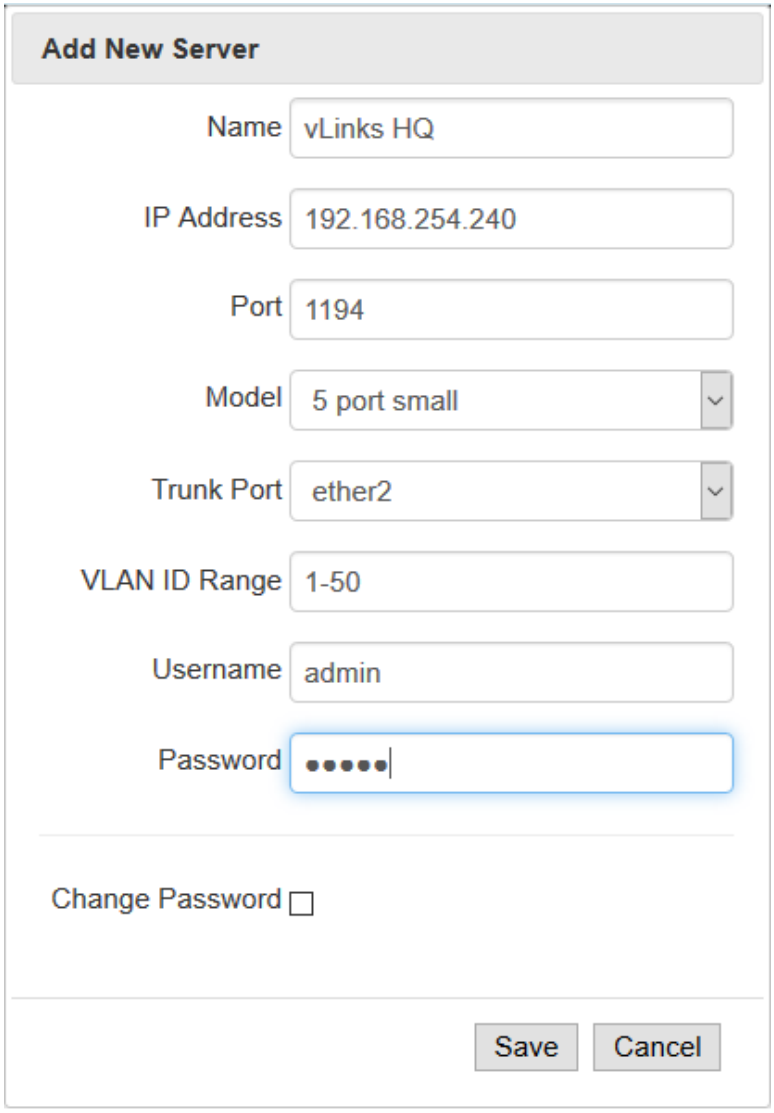



8) Once connected to the CGX Access Appliance, Login into CGX Access web interface.

Go to: Configuration > vLinks Manager



9) Select Add New Server and complete the registration process




**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 in blank. It recommended you create a secure admin password.

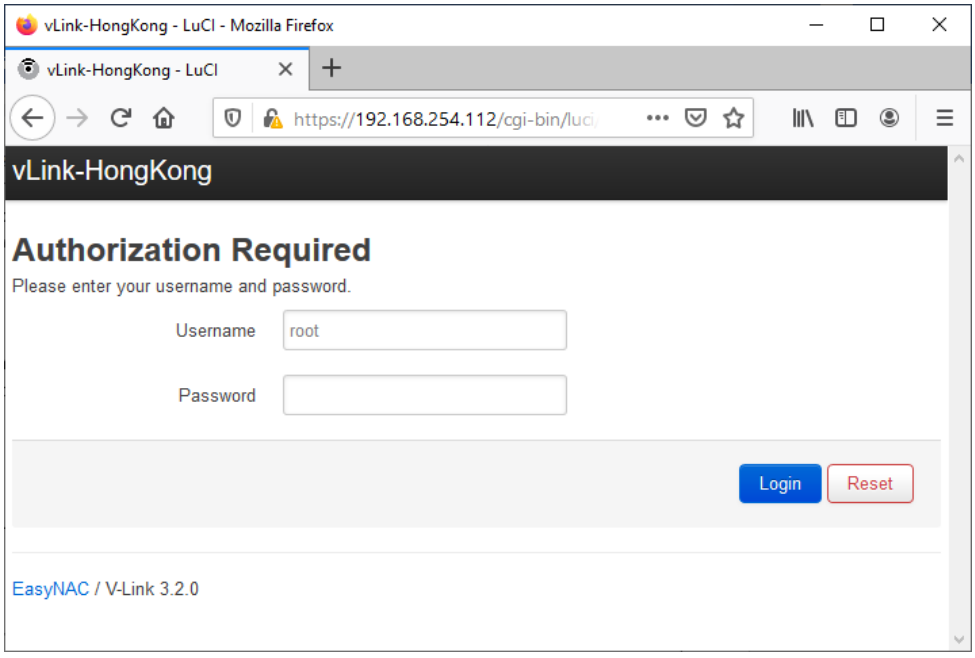
Once saved, the above settings will be pushed to the vLinks Central server and the vLinks Central will be ready to accept connections from vLinks Remote network extenders.


# 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.

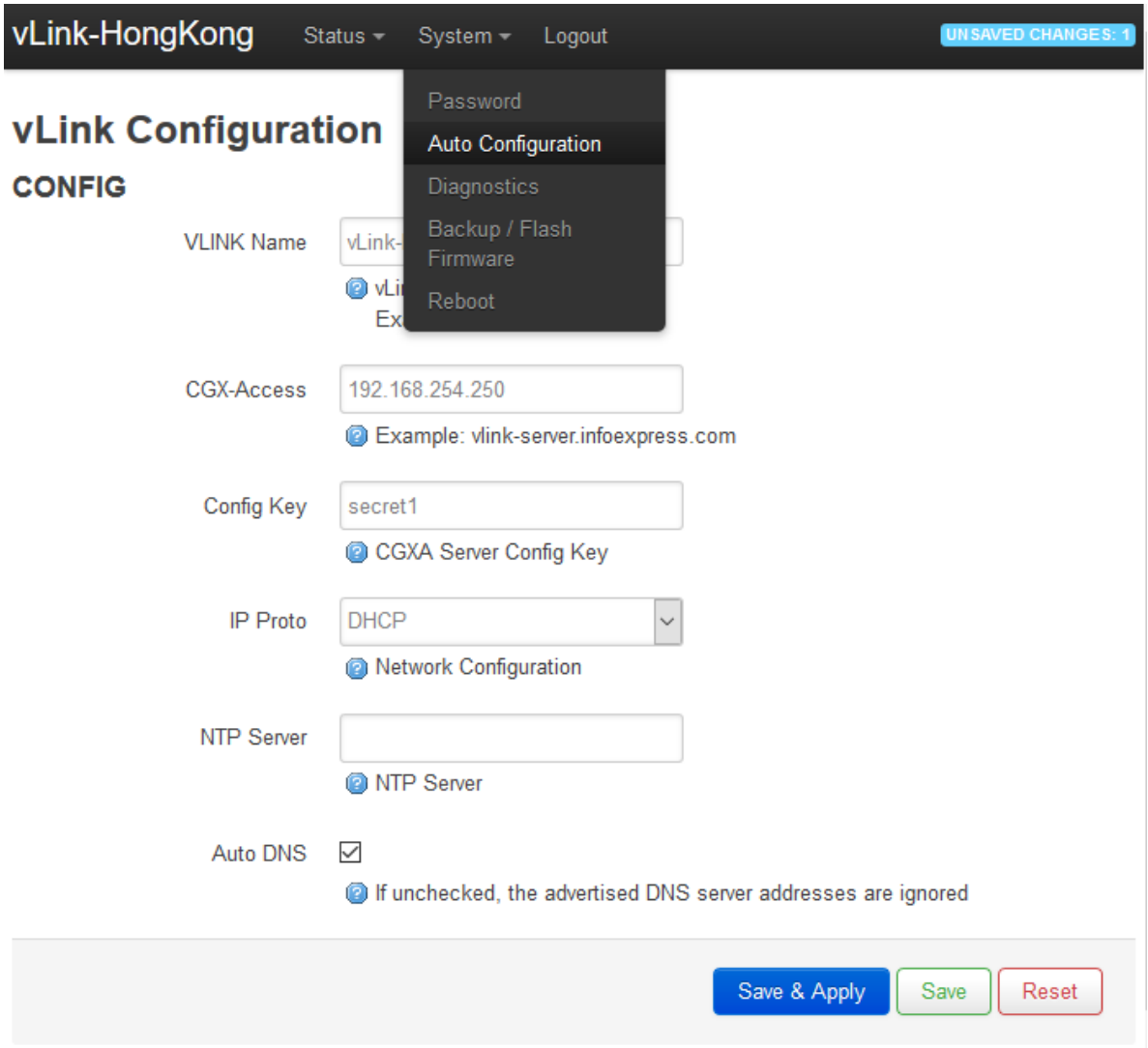
1) To allow Auto Configuration a Config Key must be set within the vLinks Manager.


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

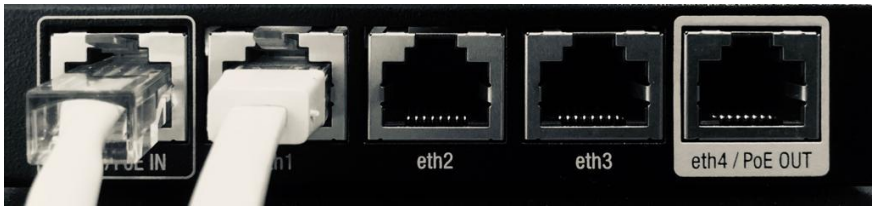
**IP Proto** – Use this field to change to a Static IP if required. For simplified deployment, DHCP is recommended as each vLinks Remote will have the same configuration and can then be used on any network.

**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

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.

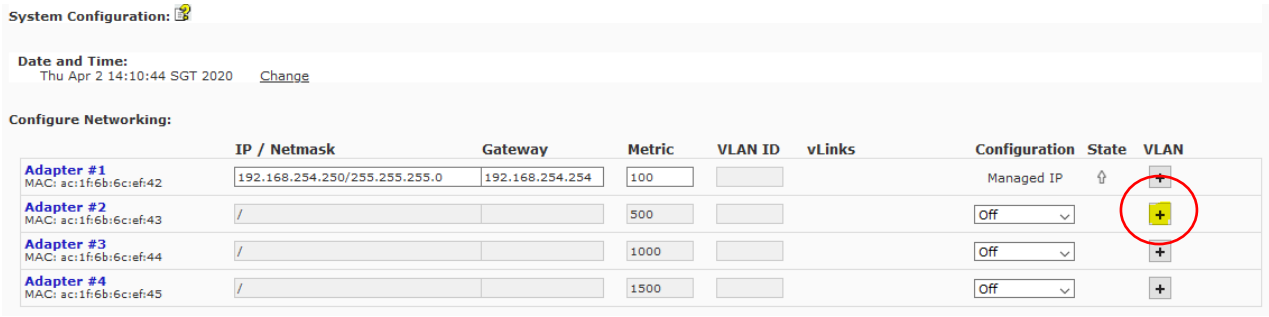


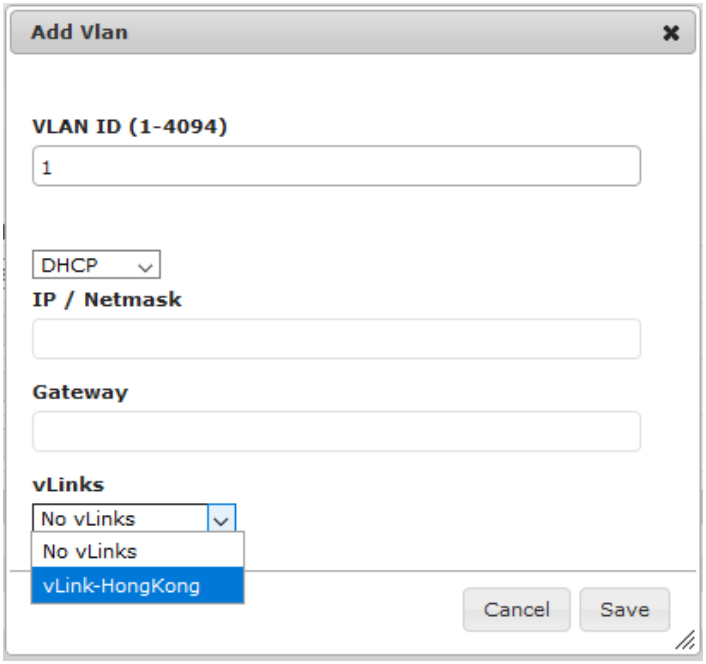

5) Accept vLinks Remotes - Once placed on the remote networks the vLinks Remotes will connect to CGX Access to request configurations: Configuration > vLinks Manager Click the Accept button as shown below.


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



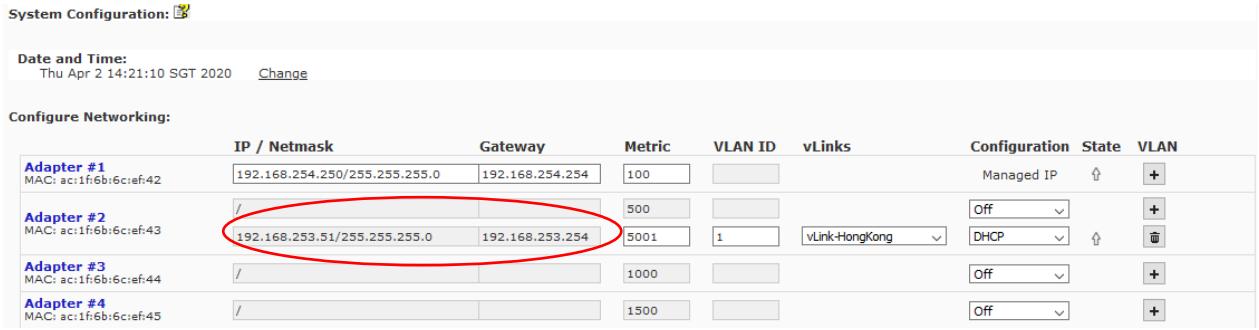

**VLAN ID** – Specify any unique VLAN ID that was defined during the vLinks Central. Normally 1-50 by default. On vLinks Remote each Adapter(eth1-eth4) that is active will use a VLAN ID.

**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.

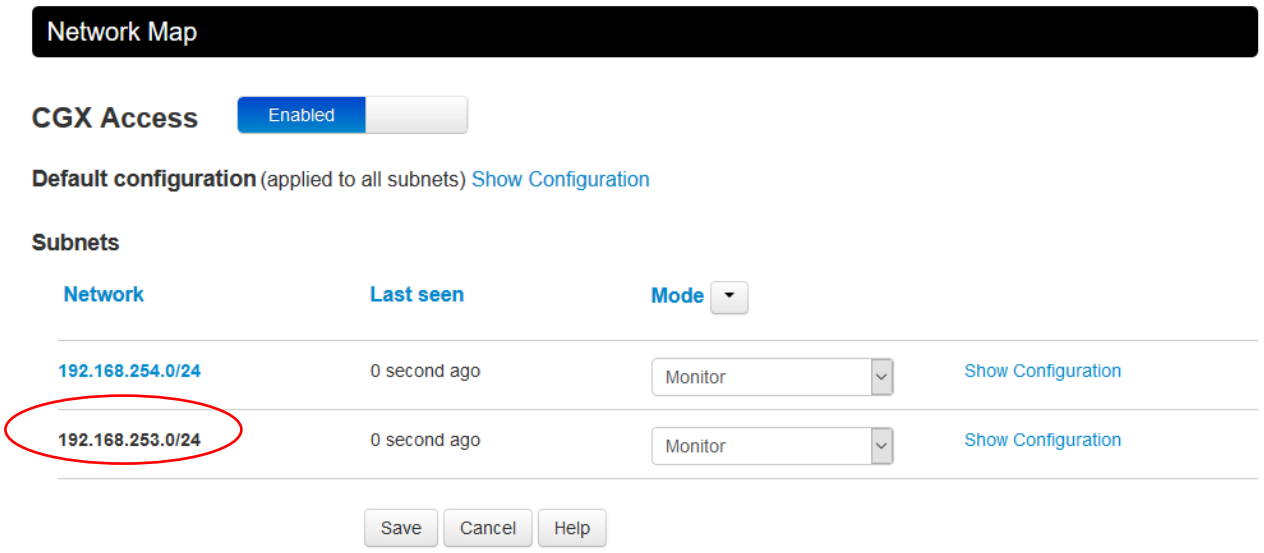
**vLinks** – Use the dropdown box to select the appropriate vLinks for this remote network. If the vLinks box is not shown, confirm it has been accepted during the Auto Configuration stage.

**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.




If successful you will see an IP address has been obtain, and device monitoring will be active. Go to: NAC > Network Map




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.

**End of Document**