

EASY NAC

CGX ACCESS QUICKSTART GUIDE MICROSOFT HYPER-V

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

Copyright © 2024 InfoExpress Incorporated. All Rights Reserved. InfoExpress products and services are protected by one or more of the following U.S.

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

www.infoexpress.com

www.easynac.com

V3.2.240329

Document Overview

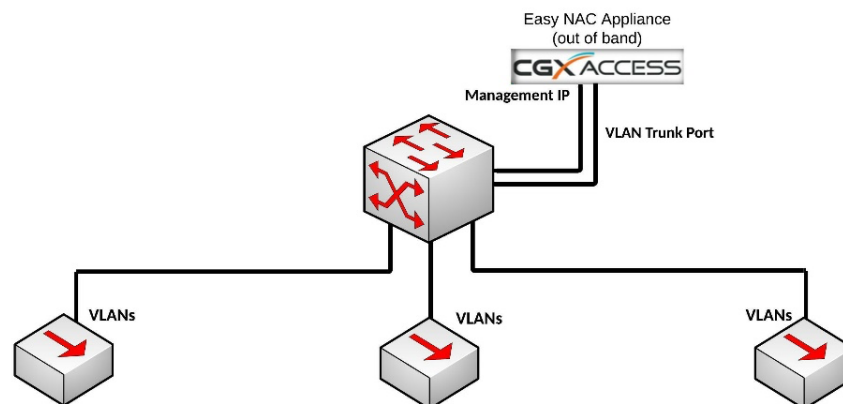
This document provides a getting started instructions for customers and partners on how to deploy the EasyNAC virtual appliance (CGX Access) on Microsoft Hyper-V Server for evaluation purposes.

For a full deployment guide covering more features, please refer to [EasyNAC 3.2 Deployment Guide](#).

Appliance Placement

The CGX Access appliance requires layer-2 visibility to provide protection and access control using ARP enforcement. The CGX Access appliance can protect up to 200 VLANs concurrently with the use of 802.1q trunk ports. The Management 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, endpoint security solutions, and e-mail via the Management IP.

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



Step 1. Installing on Microsoft 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, click Next to start the import process for the EasyNAC virtual appliance.
- Browse the location of the extracted EasyNAC virtual appliance image then click Next.
- Select the virtual machine for the EasyNAC virtual appliance then click Next.
- Select the option "Copy the virtual machine (create a new unique ID) then click Next.
- Modify the destination where the virtual machine will be stored if necessary. Click Next if using default virtual machine configuration.
- Specify the location for the virtual machine storage. Click Next once done.

- Verify the options on Summary page and click 'Finish' when ready to proceed.
- The Wizard will then proceed to deploy the image.
- The Virtual Machine will be listed in Hyper-V Manager.
- Select the virtual machine 'CGX-Access-3.2' and click 'Settings' from 'Action' menu.
- Select the Network Adapter #1 and assign a Virtual switch from the right-side drop-down box as highlighted below and Apply the setting.
- Select the CGX-Access-3.2 virtual machine and right click to Start to boot the appliance.

Step 2. 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.

- Open a console window and power on the VM.
- Login as admin/admin.

```
CGX Access Server
=== General Setup ===
1 Run Setup Wizard
10 Configure Networking
11 Set Date and Time
12 Manage Passwords
13 Configure Logging
14 Configure Services

=== Information ===
Version: CGX-ACCESS: 3.2.240223
Hardware: 1000-SWA 3.10.0
Managed IP: 10.160.0.100/255.255.255.0
Def gateway: 10.160.0.1
DNS Servers: 8.8.8.8 1.1.1.1
Server Mode: Standalone Appliance

=== Maintenance ===
91 Server Maintenance
99 Restart/Shutdown Server

Enter Option (0=Exit):
```

- From the main menu choose 1 (Run setup wizard) and follow the prompts to set the Time Zone, date and time, Managed IP address and netmask, the default gateway, and DNS servers.

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

- 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.

Captive Portal IP Address

When configured, new devices joining the network can be redirected to this page for guest or employee device registration. To configure this Captive Portal IP address:

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

The screenshot shows the 'Appliance Settings' interface for 'Networking'. It includes a table for network adapters, DNS & Domain Name settings, and Landing Pages. The IP addresses for the Captive Portal and Remediation Portal are highlighted with red boxes.

Adapters	IP / Netmask	Gateway	Metric	VLAN ID	Location
Adapter #1 MAC: 00:50:56:9a:04:bc Speed: 10 Gb/s	10.160.0.100/255.255.255.0	10.160.0.1	1		Cloud demo ▼
Adapter #2 MAC: 00:50:56:9a:28:97 Speed: 0 Gb/s	/		500		▼

Submit Network Changes

DNS & Domain Name:

DNS Servers: 8.8.8.8 1.1.1.1
Hostname: cgx-access
Domain Name: easynac.demo
Submit DNS & Domain Name

Landing Pages:

Support NAT'd:

Host Name for Captive Portal:

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

Host Name for Remediation Portal:

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

Submit Landing Pages

- Click “Submit Landing Pages” button.

Remediation Portal IP Address

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

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

Step 3. Protecting Additional Subnets

When protecting additional VLANs, each additional subnet protected will also use one IP on its respective subnet. These additional IP's can be a static IP or dynamically assigned by DHCP. 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 Hyper-V virtual appliance can support up to 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.

This guide will assume the use of an 802.1q trunk port.

Additional 802.1q configuration on Hyper-V server

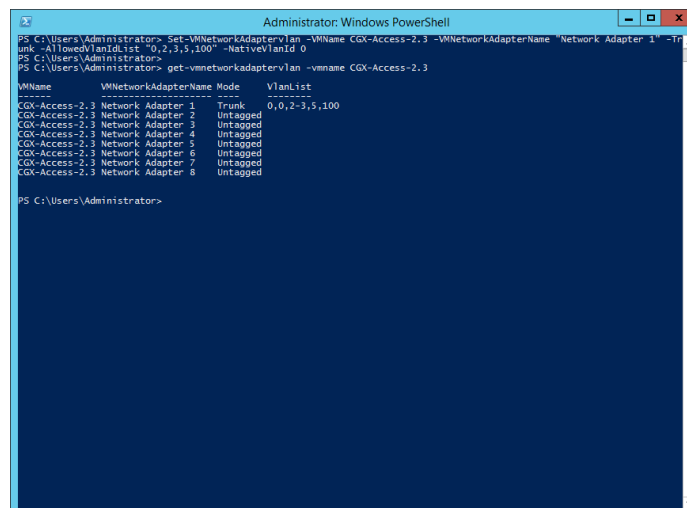
For CGX Access virtual appliances to support the 802.1q, Hyper-V's network adapters should be configured to tag frames. To enable trunking, some commands need to be entered from Windows PowerShell. The following screenshots show pre-requisite configuration.

- Hyper-V physical network adapter should support 802.1q tagging
- Switch port on which CGX Access trunk port is connected should support 802.1q tagging.
- From Virtual switch manager, configure virtual switch as "External Network"
- Select VM CGX-Access-3.2 (or vmname) and from right hand pane, click on settings. Assign virtual switch to the network adapter on CGX Access.
- Start Windows PowerShell and enter following command to configure "Network Adapter 1" as trunk port with allowed vlans 0,2,3,5,100 and Native Vlan as 0 (1 on cisco)

```
Set-VMNetworkAdaptervlan -VMName CGX-Access-3.2 -VMNetworkAdapterName "Network Adapter 1" -Trunk -AllowedVlanIdList "0,2,3,5,100" -NativeVlanId 0
```

- To verify enter following command.

```
Get-VMNetworkAdaptervlan -VMName CGX-Access-3.2
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Set-VMNetworkAdaptervlan -VMName CGX-Access-3.2 -VMNetworkAdapterName "Network Adapter 1" -Trunk -AllowedVlanIdList "0,2,3,5,100" -NativeVlanId 0
PS C:\Users\Administrator>
PS C:\Users\Administrator> get-vmnetworkadaptervlan -vmname CGX-Access-3.2
-----
VMName      VMNetworkAdapterName Mode      VlanList
-----
CGX-Access-2.3 Network Adapter 1   Trunk    0,0,2-3,5,100
CGX-Access-2.3 Network Adapter 2   Untagged
CGX-Access-2.3 Network Adapter 3   Untagged
CGX-Access-2.3 Network Adapter 4   Untagged
CGX-Access-2.3 Network Adapter 5   Untagged
CGX-Access-2.3 Network Adapter 6   Untagged
CGX-Access-2.3 Network Adapter 7   Untagged
CGX-Access-2.3 Network Adapter 8   Untagged
PS C:\Users\Administrator>
```

Configuring Network Adapters with 802.1q VLANs

Once Hyper-V has an adapter configured as a Trunk Port then adding additional VLANs is simple.

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

Networking:

Adapters	IP / Netmask	Gateway	Metric	VLAN ID	Location	Configuration	State	VLAN
Adapter #1 MAC: 00:15:56:01:10:00 Speed: 1 Gb/s	192.168.1.221/255.255.255.0	192.168.1.1	100			Managed IP	0	+
Adapter #2 MAC: 00:15:56:01:10:01 Speed: 0 Gb/s	/		500			Off		+
Adapter #3 MAC: 00:15:56:01:10:02 Speed: 0 Gb/s	/		1000			Off		+
Adapter #4 MAC: 00:15:56:01:10:03 Speed: 0 Gb/s	/		1500			Off		+

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

STATIC IP EXAMPLE

Add Vlan

VLAN ID (1-4094)
10

Static IP

IP / Netmask
192.168.10.221/255.255.255.0

Gateway
192.168.10.1

Cancel Save

DHCP IP EXAMPLE

Add Vlan

VLAN ID (1-4094)
20

DHCP

IP / Netmask

Gateway

Cancel Save

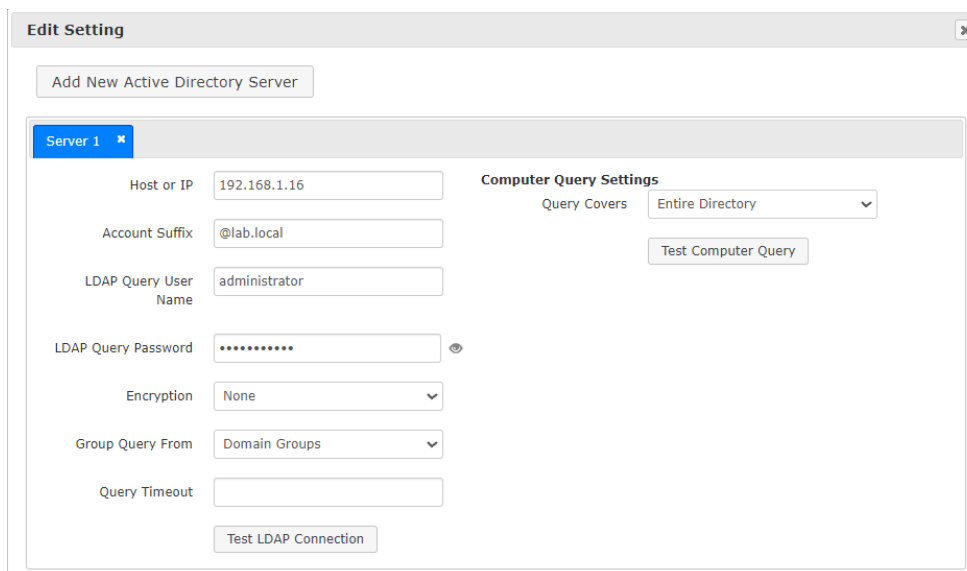
- Repeat above step for adding more VLANs.
- To confirm the network changes, click the “**Submit Network Changes**” button.

Note: If DHCP was configured, you should see IP address assignments to VLAN NICs after network changes were successfully submitted.

Step 4. Integration with Active Directory

Configure Active Directory server settings on CGX Access

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



The screenshot shows the 'Edit Setting' window for an Active Directory server. At the top, there is a button labeled 'Add New Active Directory Server'. Below this, a tab labeled 'Server 1' is selected. The configuration fields are as follows:

- Host or IP: 192.168.1.16
- Account Suffix: @lab.local
- LDAP Query User Name: administrator
- LDAP Query Password: [masked]
- Encryption: None
- Group Query From: Domain Groups
- Query Timeout: [empty]

On the right side, under 'Computer Query Settings', the 'Query Covers' dropdown is set to 'Entire Directory'. There are two buttons: 'Test Computer Query' and 'Test LDAP Connection'.

- 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

Enable Active Directory Integration

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

✕
Edit Action

Active Directory Integration

Enable Integration

Check the hostname inconsistency

Server Configuration

Query Interval (Seconds)

Policy

CONDITION	TAG
<input checked="" type="checkbox"/> Tag devices that are domain computers	<input style="width: 100px;" type="text" value="AD-managed"/>
Single AD Server <input type="checkbox"/> Tag devices with no user login in <input style="width: 30px;" type="text" value="3"/> days	<input style="width: 100px;" type="text" value="stale-login"/>
Multiple AD Servers <input type="checkbox"/> Tag device with no user login in <input style="width: 30px;" type="text" value="15"/> days	<input style="width: 100px;" type="text" value="stale-login"/>

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

- Check “Enable Integration”
- Check “Tag devices that are domain computers”
- 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. To use DNS enable, Configuration → Integration → Setting Shared by All the Integrations

Note: In some cases, AD directory database may be very large. In these cases, it may be necessary to adjust the OUs that need to be queried for AD computer objects. Custom OUs can be specified in the Active Directory Server section under Configuration → General Settings

Step 5. Configuring Email Server for Alerting

CGX Access can send notifications when certain events occur. These event triggers are configured with Auto Trust Policies, Monitoring rules, or with guest registration. To configure the email servers used by CGX Access:

- Go to Configuration → General Settings → E-mail Server

Edit Setting

Outbound Mail Server

Credential Type: SMTP

Host or IP: E.g. smtp.gmail.com or smtp.gmai

User Name: [Text Field]

Password: [Masked Password]

Encryption: MSA/STARTTLS (Port 587)

Ignore Certificate Validation

Send Email

Inbound Mail Server

Same as Outbound

Credential Type: SMTP

Host or IP: E.g. imap.gmail.com or imap.gmai

User Name: [Text Field]

Password: [Masked Password]

Encryption: IMAP (Port 143)

Test Inbound Server

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

Sender: webmaster@infoexpress.com

BCCed: a1234@infoexpress.com, b5678@infoexpress.com

Save Cancel Help

- The optional Inbound Mail Server is for use with Orchestration integrations with E-mail.
- Enter an email address used as sender address and optionally Bcc'd on guest registration emails.
- Go to Configuration → General Settings and click on the “Contact Information for Notifications” section.

Edit Setting

Recipients for Notifications

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

Prev 1 Next Pages: 1

For Email

Notification Subject Line: EasyNAC Notification

Syslog Notification

Destination Syslog Server: [Dropdown]

Log Format: [Dropdown]

Save Cancel Help

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

Step 6. Integration with Anti-Virtus/EPP/XDR Solutions

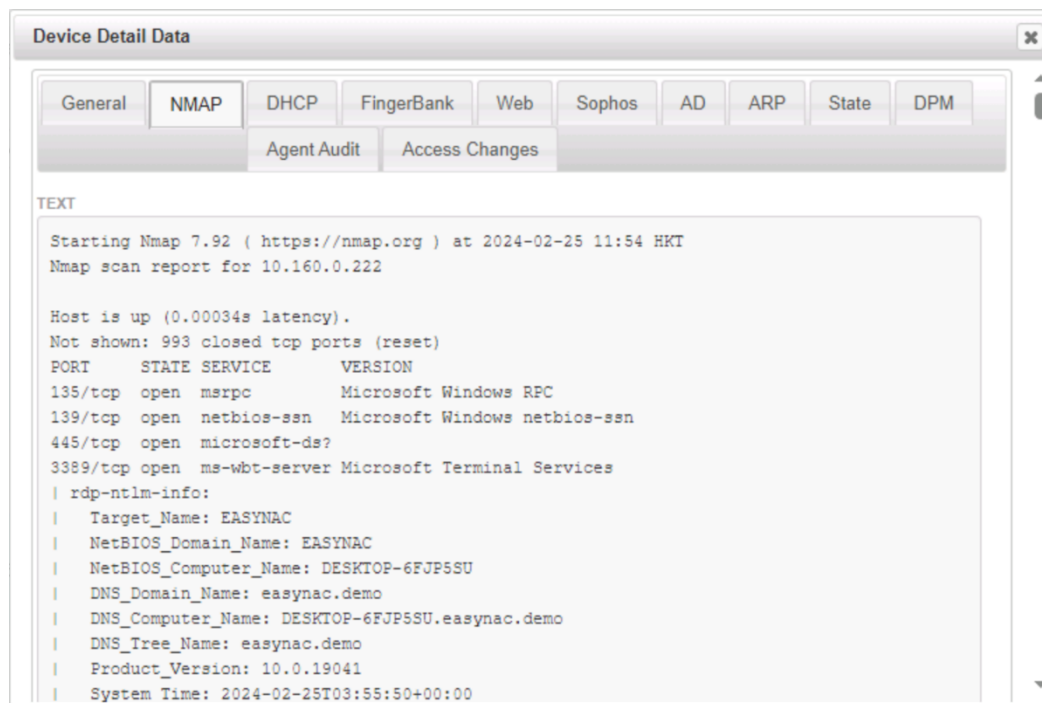
Easy NAC supports integration with various endpoint security solutions to provide additional context on the organization's managed endpoints. This can be enabled to identify all AV-Managed devices and provide details on outdated signatures or real-time protection is disabled as examples and quarantine the device accordingly.

- In CGX Access GUI go to Configuration → Integration
- Refer to page 86 in the [EasyNAC 3.2 Deployment Guide](#) for instructions on setting up the following integrations:
 - Bitdefender GalaxyZone
 - Carbon Black Cb Response
 - Carbon Black Cloud
 - CrowdStrike Falcon
 - Cybereason
 - Elastic XDR
 - ESET Antivirus
 - FireEye HX Integration
 - HCL BigFix
 - Ivanti Security Controls
 - Kasaya VSA
 - Kaspersky Antivirus
 - Managed Engine Desktop Central
 - Managed Engine Patch Manager
 - Microsoft Intune
 - Microsoft SCCM \ WSUS – 4.x +
 - Microsoft Windows Management Instrumentation (WMI)
 - Moscii StarCat 2013 and StarCat 10
 - OKTA Verify
 - Sophos Enterprise Console - 5.x +
 - Sophos Central (cloud)
 - Symantec Endpoint Protection Manager - 14.x
 - Symantec Endpoint Protection Cloud
 - Trend Micro OfficeScan - XG+
 - Trend Micro Apex Central (cloud)
 - Trellix ePO
 - Webroot (cloud)

Step 7. Use Device Profiling for Tagging / Allowlist

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

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



The information seen in these tabs can be used to create custom device profiling policies.

Customized Device Profiling Policies

In CGX Access GUI:

- Go to Policies → Device Profiler

CGX Access has a few of preconfigured Device Profiling Policies. It also allows custom device profiling policies can be created:

- Click [Add Rule](#) to create a custom profiling rule
- Click [Add](#) to create one or more conditions. Multiple conditions use “and” logic.
- Click [Add](#) to create one or more Actions. Setting Tags is a common profiling action
- Click “Activate Policies”

Note: Adjust the Auto Trust Policy accordingly to assign access to the devices tagged with the device profiling policy created.

Allowlist

CGX Access also supports a quick method to add device(s) to a manual allowlist or blocklist.

- Allowlist – Device will always have Full Access and be protected, regardless of policy.
- Blocklist – Device will always be Restricted, regardless of policy

The examples below will assume Allowlist, but blocklist works the same way.

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

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

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

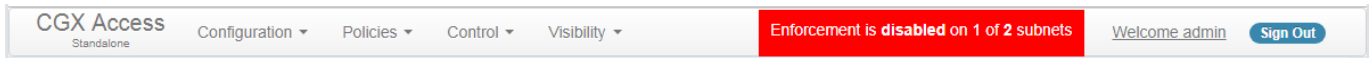
The screenshot shows the 'Device Manager' interface. At the top, it says 'All Unique Devices Identified by CGX Access' and 'Updated at Wed Dec 13 2023 11:20:32'. Below this, there are filters for 'Cover Devices Active in: Past 24 Hours' and a 'Show Report Filter' link. The main action area has a dropdown menu for 'Add to list' (labeled 2), a dropdown for 'allowlist' (labeled 3), a dropdown for 'Permanent' (labeled 3), and a button 'Apply to selected devices' (labeled 4). Below this, it says 'Total # of Devices: 4' (labeled 1). A table of devices is shown with columns: MAC, Hostname, Access Group, Roles, OS, Vendor, Tags / Lists, IP Address / IPv6, Last Seen, Comment, Access Status, Grant Access, and an icon. Three devices are selected with checkboxes. The table data is as follows:

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

NOTE: for more information, please refer to [EasyNAC 3.2 Deployment Guide](#).

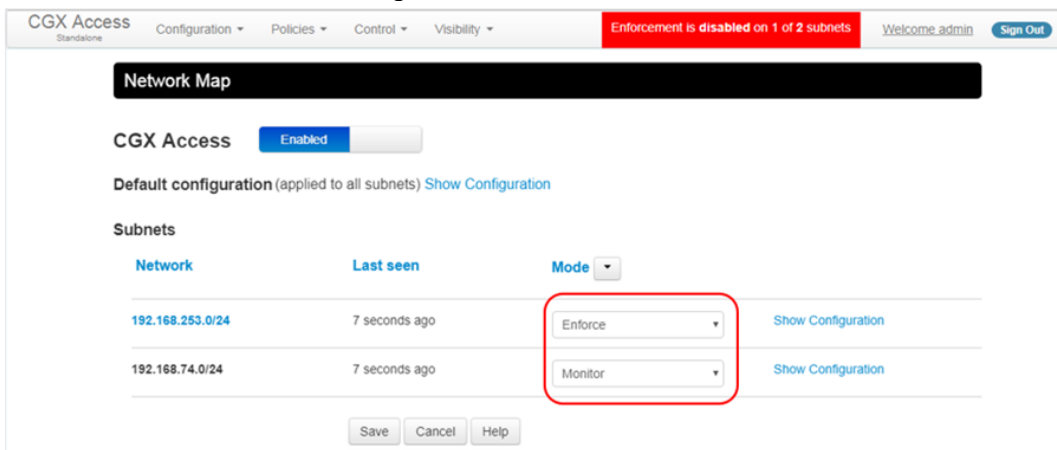
Step 8. Enable and Test Enforcement

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



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

- Go to Control → Network Map



Testing enforcement

- Verify from the Device Manager the access role assigned to managed devices is full-access.
- Make sure full-access devices have the right access to resources via connectivity testing.
- Blocklisted devices should not be able to communicate with other devices in the network and if captive portal is configured, should be redirected to the EasyNAC landing page when opening a web browser.

Step 9. Test Guest Access

CGX Access supports multiple login methods for guest registration. Typical options include self-service registration, sponsor registration, or registration with sponsor approval. Guest Access is a standard feature that is enabled by default, but a few steps are recommended to customize or enhance the guest experience.

Customize Captive Portal

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

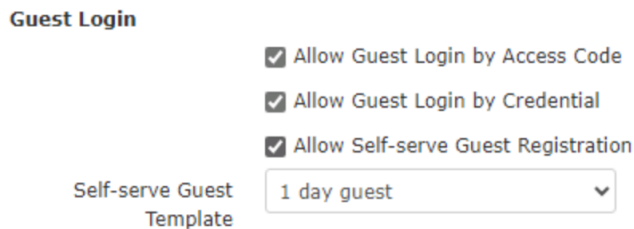
- Adjust the Company Title, Welcome Page Title, and any other details as desired.
- Upload a corporate image* and adjust the header and footer colors

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

Customize Guest Portal

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

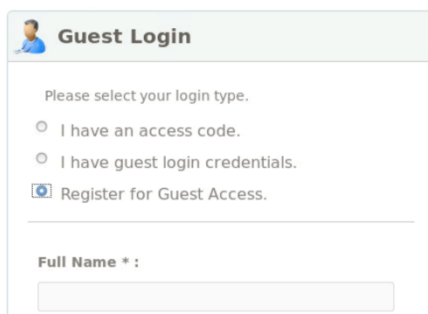
- Edit the title and message boxes as desired.
- Scroll down to enable your organizations preferred login methods



The screenshot shows the 'Guest Login' configuration section. It includes three checked checkboxes: 'Allow Guest Login by Access Code', 'Allow Guest Login by Credential', and 'Allow Self-serve Guest Registration'. Below these is a dropdown menu for 'Self-serve Guest Template' currently set to '1 day guest'.

Customizing Self-Registration Templates for Guests

- Go to Configuration → Device Registration Templates → Guest Registration Templates
- Select and edit the existing “1 day guest” template
- Configure the template according to the expected behavior when a guest self-registers a device.
- For initial testing, use the Self-registration functionality



The screenshot shows the 'Guest Login' user interface. It features a header with a user icon and the title 'Guest Login'. Below the header, there is a prompt 'Please select your login type.' followed by three radio button options: 'I have an access code.', 'I have guest login credentials.', and 'Register for Guest Access.' (which is selected). At the bottom, there is a text input field labeled 'Full Name *'.

NOTE: For more advance Guest portal options please refer to [EasyNAC 3.2 Deployment Guide](#).

Step 10. Enable Deception Feature

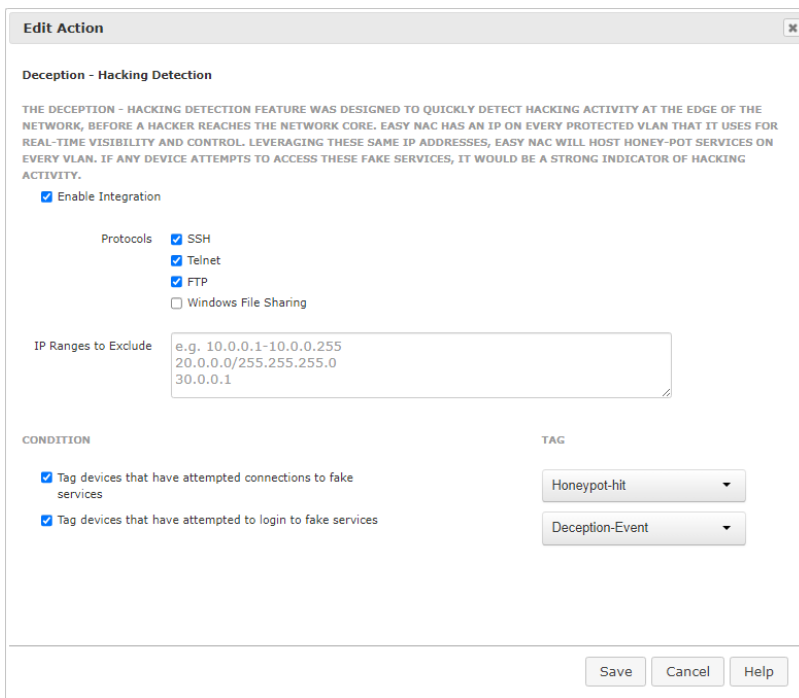
Advanced Security – Deception – Hacking Detection

This feature was developed to quickly detect hacking activity using the EasyNAC IP on every protected VLAN. EasyNAC will host honey-pot services on every VLAN and will detect and tag attempts to these fake services which suggests a strong indication of malicious activity.

- In CGX Access GUI go to Policies → Advance Security → Deception – Hacking Detection



- Enable Integration and specify the protocols/services to be impersonated by EasyNAC. Click Save once done.



- Once enabled, use a SSH, FTP, or Telnet client to access an IP address being used by the appliance. For example: Captive Portal, Remediation Portal, or any of the IP addresses on the Trunk port. Note: The Manage IP doesn't host any honeypot services.

End of Document