



What's New in Easy NAC 3.2

March 2024 Release

Disclaimer

This document is provided for your use to help understand the InfoExpress short-term development priorities. Features may get delayed, changed, canceled, or not added to the official release(s).

The information in this document is subject to change without notice. The statements, configurations, technical data in this document are believed to be accurate and reliable but are represented without express or implied warranty.

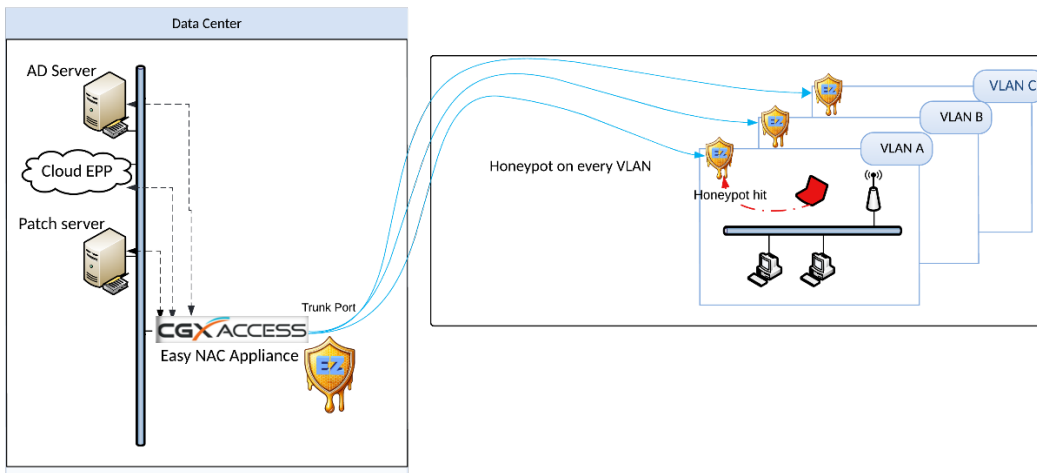
Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners.

The information in this document is proprietary to InfoExpress Inc.

Updated March 2024

Deception – Hacking Detection

We added a distributed Honey Pot feature that can detect hacking activities on the entire network and take immediate protective actions. The Easy NAC appliance has an IP address on every VLAN. This IP address provides layer-2 visibility. Leveraging this same IP address, the Easy NAC solution will offer fake honey services like SSH, telnet and FTP. If any device tries to access these honey services, we can be certain it's a hacking activity, and can immediately block the device and report the credentials used for the attempted breach. With this new feature, Easy NAC will provide both proactive security and active hacking protection with near-zero false positives.



Edit Action

Deception - Hacking Detection

THE DECEPTION - HACKING DETECTION FEATURE WAS DESIGNED TO QUICKLY DETECT HACKING ACTIVITY AT THE EDGE OF THE NETWORK, BEFORE A HACKER REACHES THE NETWORK CORE. EASY NAC HAS AN IP ON EVERY PROTECTED VLAN THAT IT USES FOR REAL-TIME VISIBILITY AND CONTROL. LEVERAGING THESE SAME IP ADDRESSES, EASY NAC WILL HOST HONEY-POT SERVICES ON EVERY VLAN. IF ANY DEVICE ATTEMPTS TO ACCESS THESE FAKE SERVICES, IT WOULD BE A STRONG INDICATOR OF HACKING ACTIVITY.

Enable Integration

Protocols SSH
 Telnet
 FTP
 Windows File Sharing

IP Ranges to Exclude

CONDITION Tag devices that have attempted connections to fake services
 Tag devices that have attempted to login to fake services

TAG

Edge Protection – Layer-2 Security

With its layer-2 visibility, the Easy NAC solution added the ability to detect configuration issues (IP conflicts and ARP storms) or security risks (ARP spoofing) occurring at the edge of the network.

Edit Action

Edge Protection - Layer 2 Security

CONDITION	TAG EVENT
<input checked="" type="checkbox"/> Tag devices with IP-conflicts Devices to exclude	ip-conflict
<input checked="" type="checkbox"/> Tag devices detected as ARP Poisoning Sensitivity Level: <input type="radio"/> Low <input checked="" type="radio"/> Medium <input type="radio"/> High <input type="radio"/> Custom	arp-poisoner
<input checked="" type="checkbox"/> Tag devices sending excessive Gratuitous ARP Sensitivity Level: <input type="radio"/> Low <input checked="" type="radio"/> Medium <input type="radio"/> High <input type="radio"/> Custom	arp-storm

Save Cancel Help

Enhanced Notifications

Building on Easy NAC's extensive notification capabilities, version 3.2 adds API support so notifications can also be sent via business messaging apps such as Slack and Microsoft Teams.

In addition, existing e-mail based notifications can include the option for Action Buttons, so quick actions can be taken from within e-mail itself.

Edit Action

Send Notification

Method Email
 SMS
 WhatsApp
 Syslog
 Slack
 Microsoft Teams

Check All Applicable Recipients EasyNAC Admin
 EasyNAC Admin2

Message

E-mail Action Button Yes
 No

Tag the device Add Tag
 Remove Tag

Save Cancel Help

Enhanced Permission Management and 2FA

In version 3.2, Easy NAC adds additional granularity in the Permission Manager. Organizations will not only be able to control who has Read/Write authority over policies, it will also provide control over the length of time their policies changes have effect. For example, a help-desk staff member could be given the ability to allow temporary access for only 1 hour or 4 hours.

The screenshot shows a 'Reports' section with a table of permissions for 'Device Manager'. The table has three rows: 'Device Manager', 'Allow Add to Lists', and 'Expiration time'. The 'Device Manager' row has radio buttons for 'No access', 'Readonly', and 'R/W', with 'R/W' selected. The 'Allow Add to Lists' row has radio buttons for 'No' and 'Yes', with 'Yes' selected. The 'Expiration time' row has a dropdown menu with options: 'All Durations', 'Permanent', '1-hour', '4-hours', '8-hours', '1-day', '2-days', '7-days', and '30-days'. The '1-hour' and '4-hours' options are checked.

Permission	Options
Device Manager	<input type="radio"/> No access <input type="radio"/> Readonly <input checked="" type="radio"/> R/W
Allow Add to Lists	<input type="radio"/> No <input checked="" type="radio"/> Yes
Expiration time	<input type="checkbox"/> All Durations <input type="checkbox"/> Permanent <input checked="" type="checkbox"/> 1-hour <input checked="" type="checkbox"/> 4-hours <input type="checkbox"/> 8-hours <input type="checkbox"/> 1-day <input type="checkbox"/> 2-days <input type="checkbox"/> 7-days <input type="checkbox"/> 30-days

In addition, 2FA for management accounts is now supported.

The screenshot shows a dialog box titled 'Authentication App (TOTP) Setup'. It contains a QR code and a dropdown menu for selecting the 2FA app. The dropdown menu is open, showing options: 'Google Authenticator', 'Duo Mobile (Cisco)', 'Microsoft Authenticator', and 'Other'. Below the QR code, there is a text input field for the six-digit code and a password input field. At the bottom, there are 'Cancel' and 'Continue' buttons.

Authentication App (TOTP) Setup

Scan this QR code with your app

Scan the QR code below with the two-factor authentication app on your phone.

Provide the used 2FA app's name to remind yourself.

Google Authenticator

Google Authenticator

Duo Mobile (Cisco)

Microsoft Authenticator

Other

If you can't use QR code, enter the six-digit code

Enter the six-digit code

After scanning the QR code, the app will display a six-digit code that you can enter below.

Please enter your password to continue

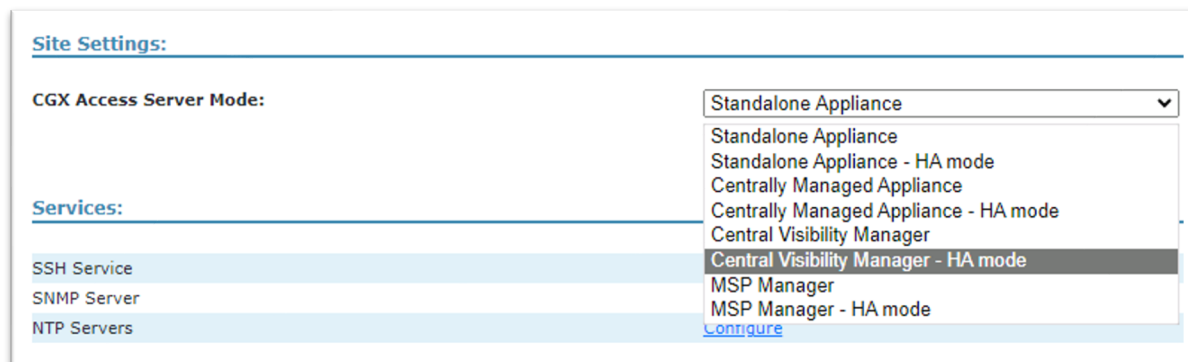
.....

Cancel Continue

Central Management Options

In version 3.2, Easy NAC introduced additional options for the Central Management of appliances.

- 1) High-Availability support will be added to the Central Visibility Manager.
- 2) An MSP version of the Central Visibility Manager will be introduced to allow Managed Service Providers to better manage multiple customers.



Additional Enhancements in 3.2

In addition, the following enhancements are included in Easy NAC 3.2

- Enhanced MAC spoofing protection to detect static IP addresses in a DHCP scope.
- Linux-based Enforcer Sensor to cost effectively extend protection to remote sites.
- Elastic XDR integration
- Other usability enhancements

End of Document