

The background of the entire page is a photograph of an industrial facility, likely a refinery or chemical plant, at night. The scene is filled with tall distillation columns, complex piping, and scaffolding, all illuminated by various lights, creating a mix of yellow, white, and blue tones. A faint grid pattern is overlaid on the entire image. In the upper left quadrant, the 'CYBERX' logo is displayed in a large, white, sans-serif font, with the 'X' being a larger, yellow, stylized character. Below the logo, the tagline 'BATTLE-TESTED INDUSTRIAL CYBERSECURITY' is written in a smaller, yellow, sans-serif font.

CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY

CYBERX RELEASE NOTES

VERSION 2.6

Copyright © 2019, CyberX LTD.

This document contains proprietary and confidential information. All data submitted to the Customer is provided in reliance upon its consent not to use or disclose any information contained herein except in the context of its business dealings with CyberX Incorporated. The recipient of this document agrees to inform present and future employees of the Customer who view or have access to its content of its confidential nature.

The recipient also agrees not to duplicate or distribute or permit others to duplicate or distribute any material contained herein without CyberX express written consent.

CyberX retains all title, ownership and intellectual property rights to the material and trademarks contained herein, including all supporting documentation, files, marketing material, and multimedia.

Document version:

2.6(0)

Last revised:

July 11, 2019

Contents

1	About CyberX Version 2.6	2
	Getting More information	2
2	Scalability	3
	Enterprise Backup and Restore for Sensors	3
	About the Backup	3
	Receiving Backup Notifications	3
	Restoring Backups	4
	CLI Sensor Backup Naming Format Changed.....	4
	Enhanced Forwarding Rule Granularity.....	4
	Enhanced SSL Certificate Import Security	5
3	Visibility	6
	Display Multiple Controllers with Backplanes.....	6
	View SNMP and SMB Versions in Data Mining Reports	7
	Enhanced Asset Inventory Filtering	8
	Display Filtered Assets in the Map.....	8
	Enhanced Asset FQDN Resolution	9
	VLAN Tagging Widget Enhancement	10
4	Threat Detection	11
	Enhanced Detection and Alerting.....	11
	GE SRTP Protocol Detection Added.....	11
	Modbus Alerting Improved	12
5	Ease of Use	13
	NTLM Support for Email Server Authentication	13
	Subnet Definition Enhancement	13
	Improved Public Range Management	14
	Update Default Central Manager Name	15
6	Enterprise Integrations	16
	Aruba ClearPass Enhancement.....	16

1 About CyberX Version 2.6

Version 2.6 provides important new features and feature enhancements that improve:

- Scalability
- Visibility
- Threat Detection
- Ease of Use
- Enterprise Integrations

Users can upgrade to this version or install it as a first-time release.

Getting More information

For more information about customer facing features described in this document, customers will be referred to the CyberX Help Center at help.cyberx-labs.com. The user guides will be available at the Help Center.

For support and troubleshooting information, contact support@cyberx-labs.com.

2 Scalability

The following scalability enhancements are available:

- Enterprise Backup and Restore for Sensors
- Enhanced Forwarding Rule Granularity
- Enhanced SSL Certificate Import Security

Enterprise Backup and Restore for Sensors

You can schedule sensor backups and perform on-demand sensor backups from the Central Manager. This provides improved protection against hard drive failures and data loss.

The Sensor Backup Schedule feature lets you collect daily sensor backups and store them on the Central Manager or an external backup server. Copying files from sensors to the Central Manager is carried out over an encrypted channel.

The restore process from the sensors is the same regardless of where files are stored.

Sensor Backup Schedule

Configuration and data are backed up. PCAP files are not.

Sensors

CyberX Console
192.168.6.136

No backup found

[Back up Now](#)

Settings

Back up Off

Every days at in time zone

Maximum storage available GB

Retain last backups per sensor

Custom Path

[Download Log](#) CLOSE SAVE

About the Backup

Configurations and data are backed up. PCAP files and logs are not backed up. Backup and restore of PCAPs and logs can be done manually.

You can maintain up to 9 backups for each managed sensor, provided that the backed-up files do not exceed the maximum backup space allocated.

The default allocation is displayed in the Sensor Backup Schedule dialog box.

Receiving Backup Notifications

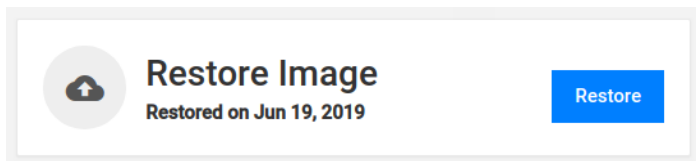
Information about backup successes and failures are automatically listed in the Sensor Backup Schedule dialog box and Backup log.

Sensors	
Sensor West 192.168.6.136	Backup on 24/06/2019 12:16 failed. Failed to access path. Verify location is accessible
Sensor East 192.168.27.117	Backup on 24/06/2019 14:58 succeeded
Sensor North 192.168.27.118	Backup on 24/06/2019 15:11 succeeded

Users can also create System Notification, Forwarding Rules which contain information about backup failures.

Restoring Backups

Restore backups from the Sensor System setting window.



CLI Sensor Backup Naming Format Changed

The CLI file format for backing up sensors has changed. The new format is: <sensor name>-backup-version-<version>-<date>.tar

Example: Sensor_1-backup-version-2.6.0.102-2019-06-24_09:24:55.tar.

The previous format was: cyberx-system-backup_2019-07-04_09-27-52.tar.gz

Enhanced Forwarding Rule Granularity

Forwarding rule granularity has been enhanced and now allows users to choose between:

- Sending only System Notifications, for example to **IT teams** responsible for CyberX sensors and Central Managers.
- Sending only alerts, for example to **security analysts**.
- Sending both System Notifications and alerts, for example to **SOC administrators**.

The screenshot shows the 'Create Forwarding Rule' configuration page. The 'Name' field is set to 'Warning'. Under 'Protocols', the 'All' radio button is selected. Under 'Engines', the 'Specific' radio button is selected, and the dropdown menu is empty, displaying 'No Engines selected'. In the 'System Notifications' section, the 'Report System Notifications' checkbox is checked. In the 'Alert Notifications' section, the 'Report Alert Notifications' checkbox is unchecked. The 'Actions' section has an 'Add' link. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

Previously only System Notifications could be enabled and disabled.

Component Support: Central Manager.

Enhanced SSL Certificate Import Security

Users working with their own trusted SSL certificates, rather than CyberX default self-signed certificates, can utilize a passphrase as part of the import process. This will be required when the private key is encrypted with a passphrase. Verify that you have your certificate passphrase before starting the certificate import process. This process should be carried out on all CyberX devices that use trusted certificates.

To work with this feature:

1. Copy the key and cer files to the Cyberx platform, using WinSCP or a similar application.
2. Run the following command:

```
sudo cyberx-xsense-certificate-import --crt <new_crt_file_name>.crt --key  
<new_key_file_name>.key --pass <'passphrase in apostrophe'>
```

Support users can work with this feature by running the certificate import command.

The passphrase is saved in `/var/cyberx/properties/phrases.properties`.

3 Visibility

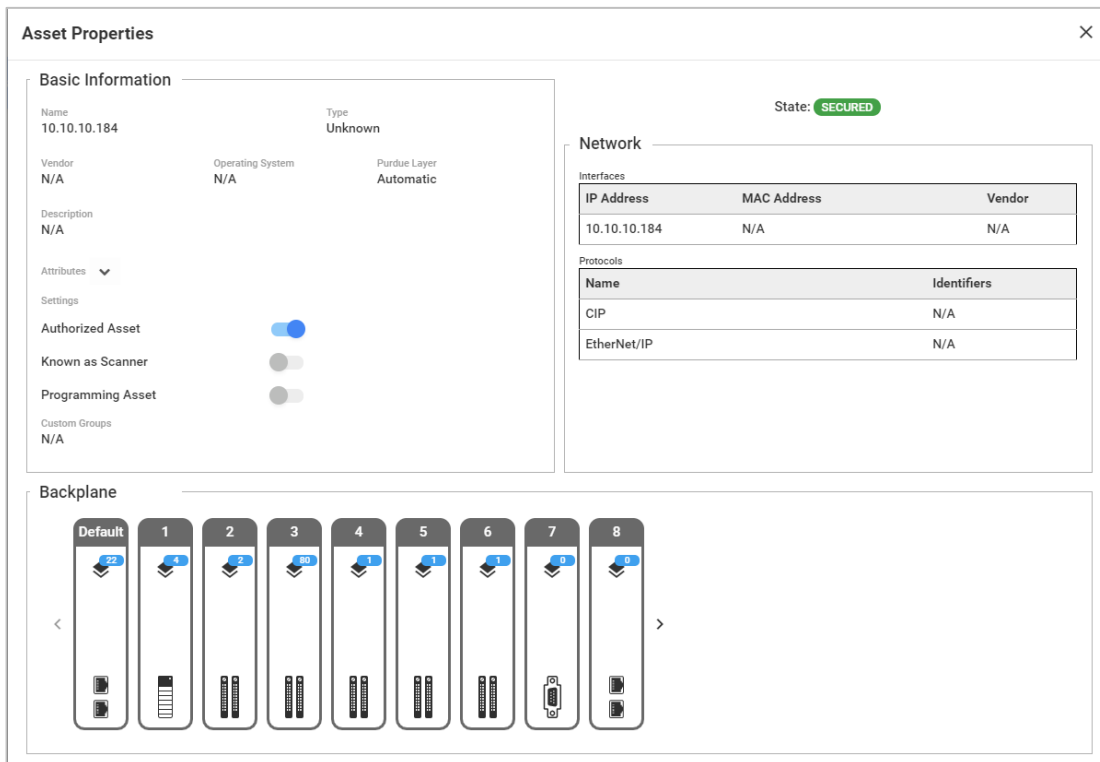
The following visibility enhancements are available:

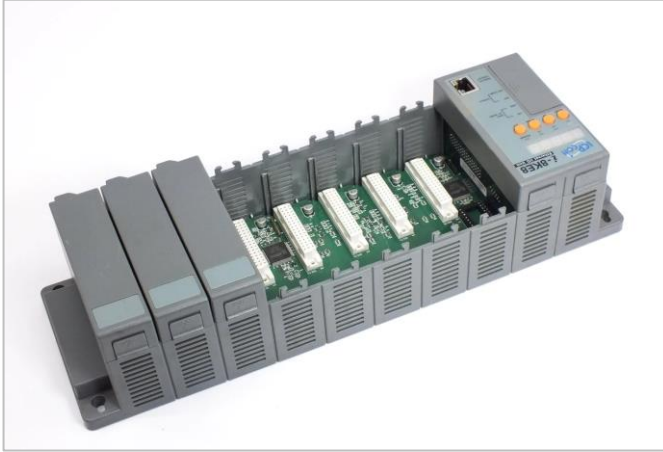
- Display Multiple Controllers with Backplanes
- View SNMP and SMB Versions in Data Mining Reports
- Enhanced Asset Inventory Filtering
- Enhanced Asset FQDN Resolution
- VLAN Tagging Widget Enhancement

Display Multiple Controllers with Backplanes

If a PLC contains multiple modules separated into racks and slots, the characteristics might vary between the module cards. For example, if the IP and the MAC are the same, the firmware might be different.

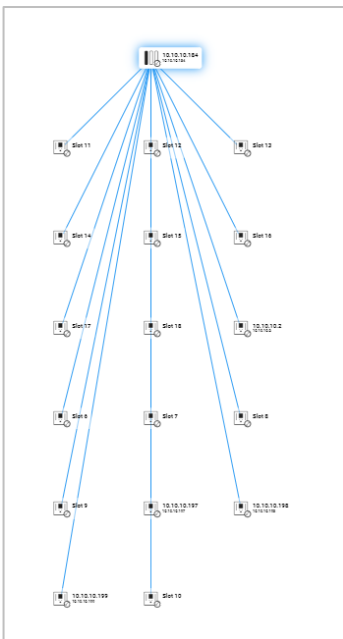
The CyberX Backplane capability lets users display multiple controllers/cards and their nested assets as one entity with a variety of definitions. Each slot in the Backplane view represents the underlying assets – the assets that were discovered behind it.





The Backplane pane is an integral part of the Asset properties window and it is shown only when such configurations exist. Each slot appears with the number of underlying assets and the icon that shows the module type.

The slot is presented in the Asset map with all the underlying modules and assets connected to it.



Component Support: CyberX Platform

View SNMP and SMB Versions in Data Mining Reports

Starting with version 2.6, users can view SNMP and SMB versions in the Protocol Versions report in Data Mining reports.

Data Mining LEARNING

Protocol Report 1

Protocol Versions

Client	Server	Protocol	Revision	Version	Last Seen
10.10.10.13	10.10.10.30	SNMP	N/A	SNMPv1	09/07/2019 11:33:20
10.10.10.16	10.10.10.30	SNMP	N/A	SNMPv1	09/07/2019 11:31:44
10.10.10.17	10.10.10.13	SNMP	N/A	SNMPv1	09/07/2019 11:31:31
10.10.10.17	10.10.10.16	SNMP	N/A	SNMPv1	09/07/2019 11:31:19
10.10.10.17	10.10.10.18	SNMP	N/A	SNMPv1	09/07/2019 11:31:19

Component Support: CyberX Platform

Enhanced Asset Inventory Filtering

Users can save a filter or a combination of filters in the Asset Inventory and re-apply them when needed.

You can create broad filters, for example based on a certain asset type; or create more narrow filters, for example based on an asset type and a specific protocol.

Assets LEARNING

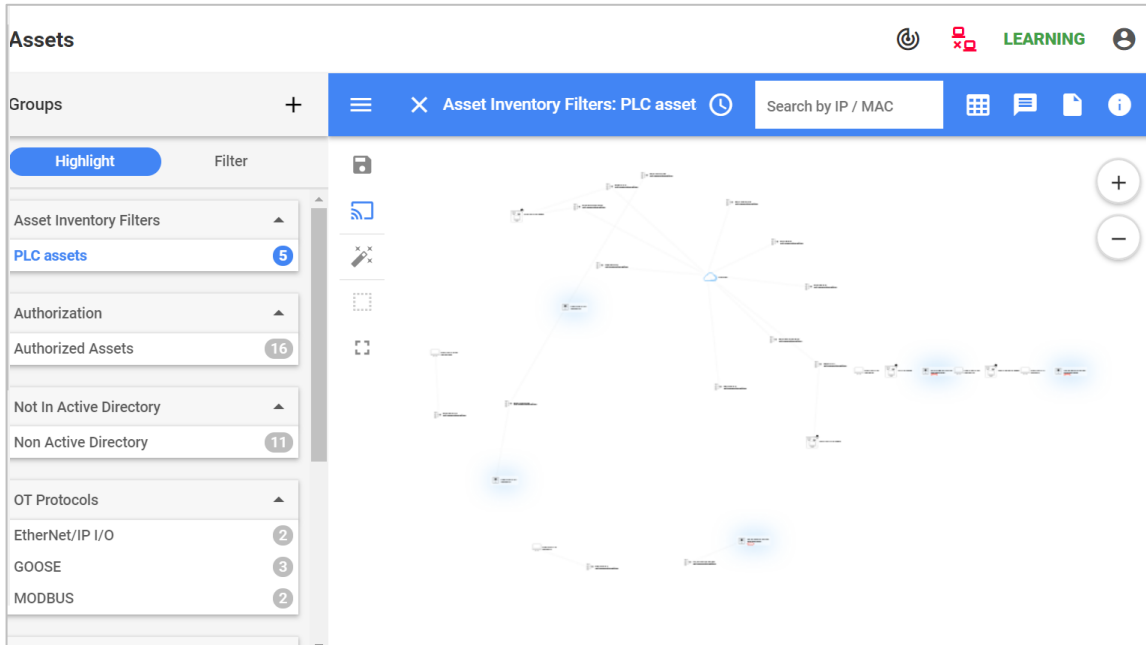
Asset Inventory

Filter by (clear all): Type: Contains 'plc' X Save Changes

Name	Type	Operating System	IP Address
192.168.1.11	PLC		192.168.1.11
192.168.1.10	PLC		192.168.1.10
00:01:4a:01:00:02	PLC		
00:01:4a:01:00:00	PLC		
00:01:4a:01:00:03	PLC		

Display Filtered Assets in the Map

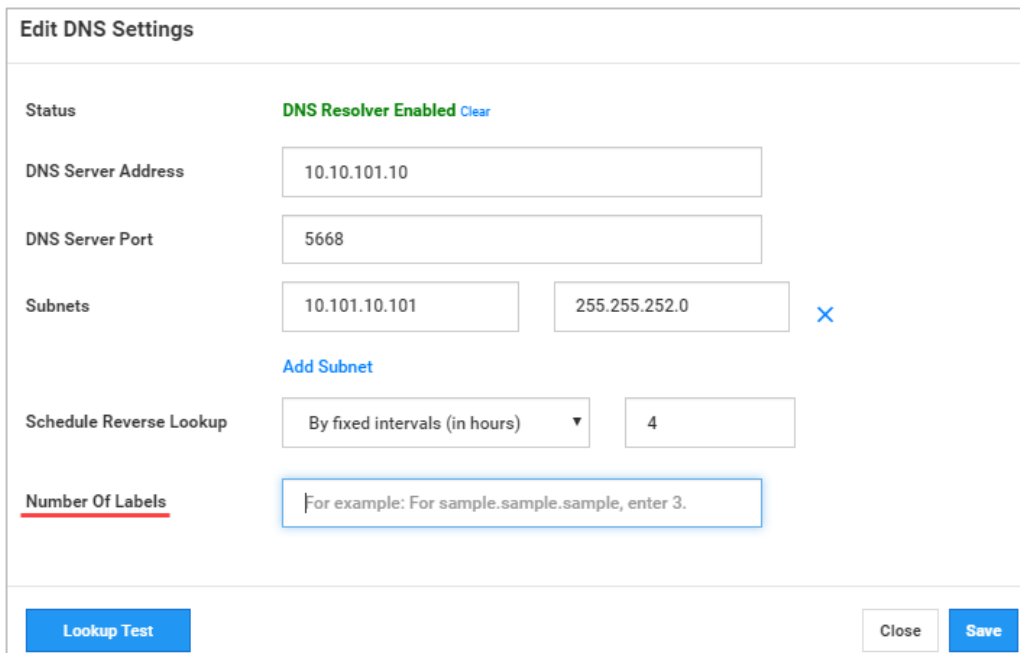
In the Map view, the saved filter can be used to highlight assets in the filtered group. The side menu under the *Asset Inventory Filters* group displays the filter you saved.



Component Support: Central Manager and CyberX Platform

Enhanced Asset FQDN Resolution

You can instruct CyberX to automatically resolve network IP addresses to asset FQDNs. To configure DNS FQDN resolution, add the number of domain labels to display. Up to 30 characters are displayed from left to right.



The FQDN previously appeared as an additional attribute in the Properties windows, rather than an asset name.

Component Support: CyberX Platform

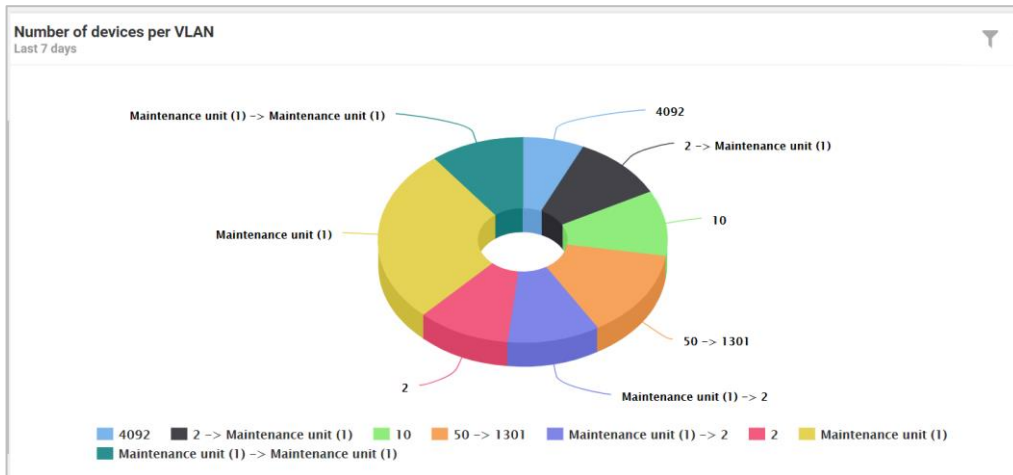
VLAN Tagging Widget Enhancement

This version provides two new Investigation widgets:

■ Number of Assets per VLAN Widget

This pie chart shows the number of discovered assets per VLAN. The size of each slice of the pie is proportional to the amount of discovered assets relative to the other slices.

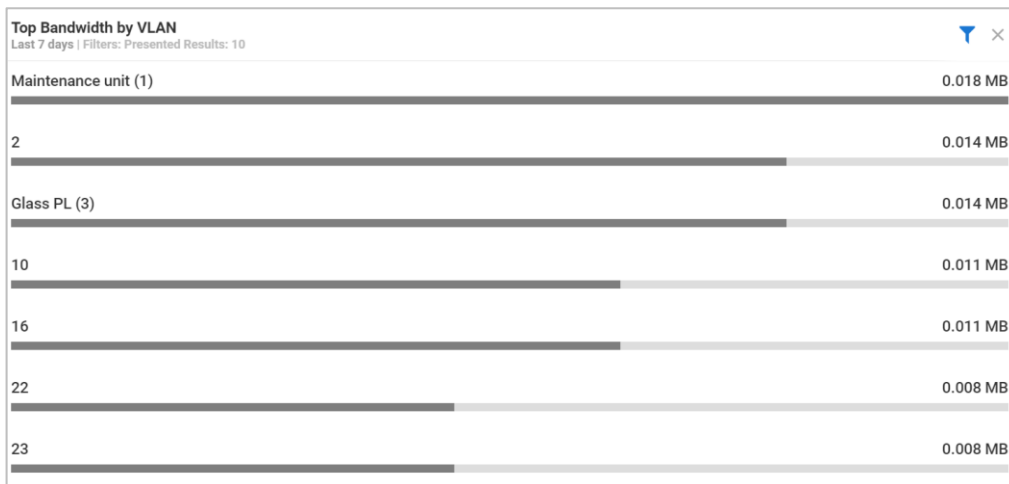
Each VLAN appears with the VLAN tag assigned by the sensor or name that the users have manually added.



■ Top Bandwidth by VLAN Widget

This widget displays the bandwidth consumption by VLAN. By default, the widget shows five VLANs with biggest bandwidth usage.

Users can filter the data by the period presented in the widget.



Component Support: CyberX Platform

4 Threat Detection

This section describes detection and alerting improvements.

Enhanced Detection and Alerting

- [GE SRTP Protocol Detection Added](#)
- [Modbus Alerting Improved](#)

GE SRTP Protocol Detection Added

CyberX now detects GE SRTP Protocol traffic. The following information is detected between assets.

- Service (Read or Write Smem)
- Packet Type
- Memory Type traffic


This information is available at the Console, for example in Data Mining reports. Deviations in learned traffic will trigger Alerts.

ID: 17 📄 🖨️ 📌 ✕

Unauthorized GE SRTP System Memory Operation

Policy Violation | Jul 14, 2019 1:41:32 PM (3 minutes ago)

The sensor detected network traffic that has not been learned by the Policy Engine. The following traffic was detected between asset 192.168.90.148 and asset 192.168.90.61: Protocol GE SRTP, Service Read Smem, Packet Type Mailbox Request, Memory Type %M (76).



192.168.90.148

Mitigation

- Verify that the traffic between these assets is valid.
- If it is, select Learn to approve the traffic.
- Select Handle to hide the alert.

Learn Handle

Modbus Alerting Improved

The Modbus Address Range violation alert has been added. The alert detects deviations regarding access to slave memory addresses.

The screenshot shows an alert window titled "Modbus Address Range Violation" with ID: 8. The alert is categorized as a "Policy Violation" and occurred on Jul 10, 2019 at 2:38:00 PM. The description states: "The master requested access to a new slave memory address. Master: 192.168.110.131, Slave: 192.168.110.138, Unit: 1, Function: Write Single Coil (5), Operation: Write". A diagram below the text shows two computer icons representing the master and slave devices, with a double-headed arrow between them. The master IP is 192.168.110.131 and the slave IP is 192.168.110.138. The "Mitigation" section includes three steps: 1. Verify that the request made by the master is valid. 2. If the request is valid, select Learn. 3. Select Handle to hide the alert. The "Additional Information" section shows "New Parameters : Discrete Output Coil 1". At the bottom right, there are "Learn" and "Handle" buttons.

The Modbus Exception alert has been improved to specify which Modbus addresses returned the exception.

The screenshot shows an alert window titled "Modbus Exception" with ID: 3. The alert is categorized as a "Protocol Violation" and occurred on Jul 10, 2019 at 2:25:57 PM (2 minutes ago). The description states: "Modbus slave device 192.168.110.138 returned an exception to master 192.168.110.131 with exception code 2 (Illegal Data Address). It is recommended to verify if a recent programming, configuration change or a firmware upgrade was performed on slave or master device, and notify the system engineer of the incident." The "Mitigation" section includes one step: 1. Verify if a recent programming, configuration change or a firmware update was performed on Slave or Master device. The "Additional Information" section shows "Parameters : Discrete Output Coil 1" and "Analog Output Holding Registers 1-5". At the bottom right, there is a "Handle" button.

5 Ease of Use

The following usability enhancements are available:

- NTLM Support for Email Server Authentication
- Subnet Definition Enhancement
- Improved Public Range Management
- Update Default Central Manager Name

NTLM Support for Email Server Authentication

Users can now choose to authenticate to SMTP email servers using NTLM. This provides a higher level of password encryption when clients authenticate.

Sensor NTLM Authentication

To work with NTLM on the sensor, select System Settings>Mail Server. Enable Authentication and then enable NTLM.

The screenshot shows a configuration window titled "Edit Mail Server Configuration". It includes the following elements:

- SMTP Server Address:** A text input field with the placeholder "IP / Domain address".
- SMTP Server Port:** A text input field containing the value "25".
- Outgoing Mail Account:** A text input field with the placeholder "e.g. noreply@site.com".
- SSL:** A checked checkbox.
- Authentication:** A checked checkbox followed by two text input fields. The first contains "dasdsad" and the second contains ".....".
- Use NTLM:** A checked checkbox.
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

Central Manager NTLM Authentication

To work with on the Central Manager

1. Log in to the Central Manger and access:

```
vim /var/cyberx/properties/remote-interfaces.properties
```

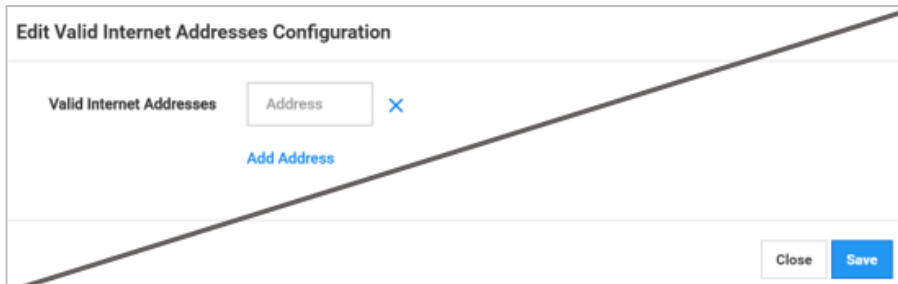
2. Change the mail.use_authentication and mail.use_ntlm_auth to **True**.

Component Support: Central Manager and CyberX Platform

Subnet Definition Enhancement

Subnets that were configured in the Valid Internet Addresses dialog box should now configured in the Subnet Configuration dialog box, enabling one dialog box for all subnet configurations.

The Valid Internet Addresses feature was removed from the product. Valid internet address ranges already defined will be automatically migrated and displayed as subnets in the Subnet Configuration dialog box.



About the Migration

This section describes the migration samples:

External IP address -> subnet IP, subnet mask

x.y.z.* -> x.y.z.0, 255.255.255.0

x.y.*.* -> x.y.0.0, 255.255.0.0

x.*.*.* -> x.0.0.0, 255.0.0.0

If there is a wildcard * in the middle of the IP, the migration is as follows

x.y.z.w -> same as x.y.z.*

x.*.y.*, x.*.*.y -> same as x.*.*.*

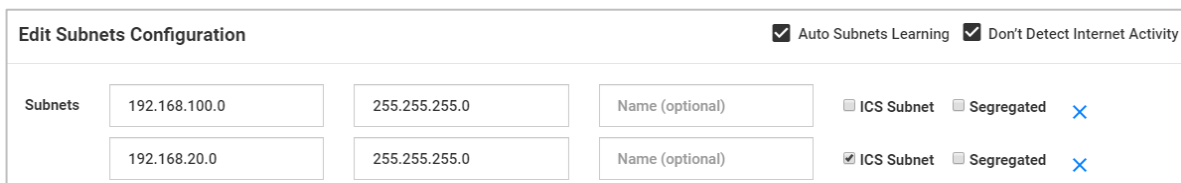
*.x.y.z, *.*.x.y -> same as *.*.*.*

If you want to validate the migration was carried out as expected, you can export subnets before the update. Export subnets after the update and compare.

Component Support: CyberX Platform

Improved Public Range Management

A new subnet configuration allows users to instruct CyberX to resolve all subnets as internal subnets. This may be required in environments that use public ranges as internal ranges, for example large organizations that work with segregated networks. Using this option reduces notifications and alerts received on external addresses.



To resolve all addresses as internal addresses, select the **Do Not Detect Internet Activity** check box. When you use select this option, you will not receive alerts, notifications, Risk Assessment and Attack Vector reports regarding internet connections.

Update Default Central Manager Name

You can change the default name of Central Manager to a customized name. This name appears at the bottom of the Console main screen and CyberX Central Manager browser tab.

Change the name from the System Setting, Edit CyberX Platform Configuration dialog box.

6 Enterprise Integrations

Aruba ClearPass Enhancement

Starting with version 2.6, the data discovered by CyberX and forwarded to ClearPass will be enriched with subnet information, which is sent to ClearPass during the sync process.