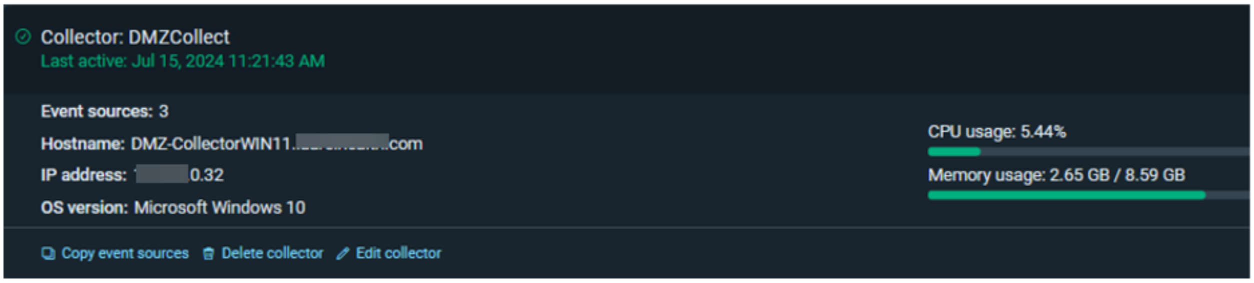
# DMZCollect Collector on InsightIDR

DMZ-Collect Collector in InsightIDR is hosting on a xx.x.8.78 (https://xx.x.8.78/ui/#/login)

Service account name: dmzcollect. The password is in Bitwarden.

Public IP address: xxx.xxx.149.111

Private IP address: xx.255.0.32

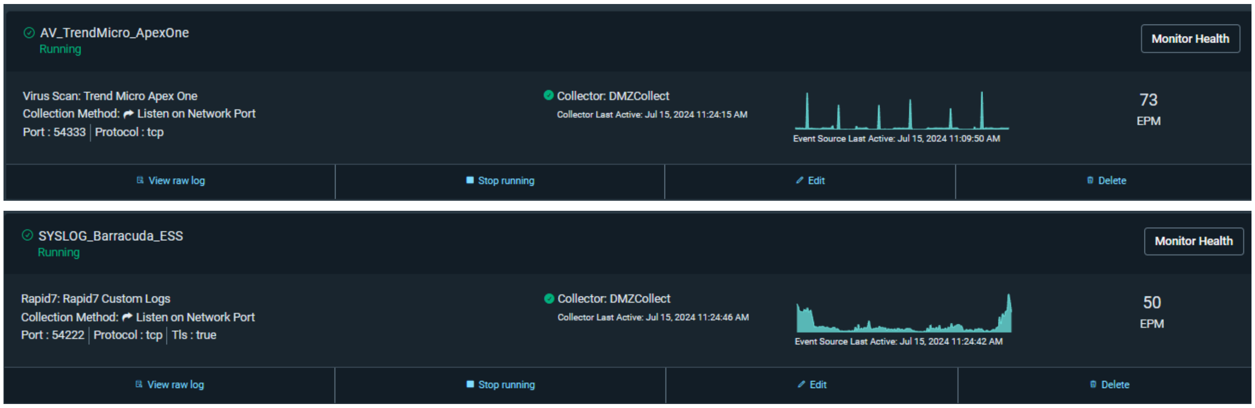


Collector: DMZCollect
Last active: Jul 15, 2024 11:21:43 AM

Event sources: 3
Hostname: DMZ-CollectorWIN11.[redacted].com
IP address: [redacted]0.32
OS version: Microsoft Windows 10

CPU usage: 5.44%
Memory usage: 2.65 GB / 8.59 GB

This DMZ-Collect collector contains event sources from AV_TrendMicro_ApexOne (Trend Micro Apex One Service) and SYSLOG_Barracuda_ESS (Barracuda Email Security Gateway).



AV_TrendMicro_ApexOne
Running

Virus Scan: Trend Micro Apex One
Collection Method: Listen on Network Port
Port : 54333 | Protocol : tcp

Collector: DMZCollect
Collector Last Active: Jul 15, 2024 11:24:15 AM
Event Source Last Active: Jul 15, 2024 11:09:50 AM

73 EPM

SYSLOG_Barracuda_ESS
Running

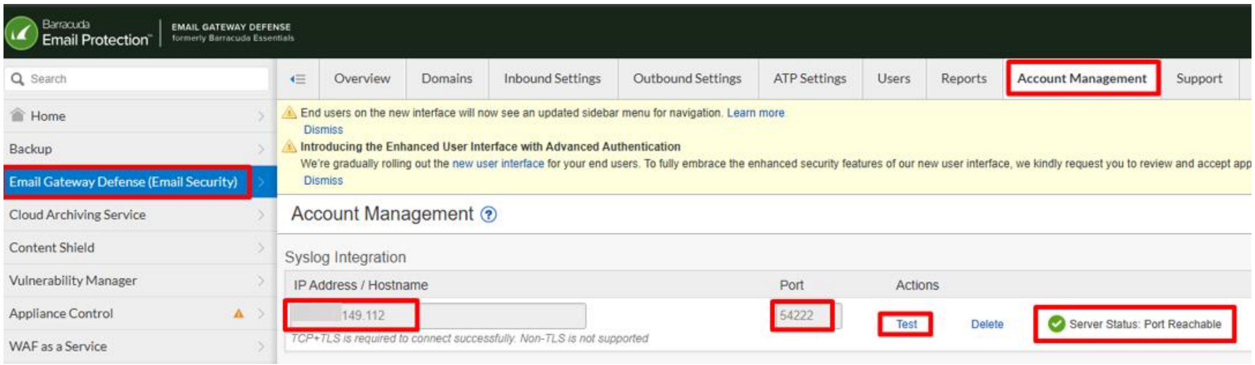
Rapid7: Rapid7 Custom Logs
Collection Method: Listen on Network Port
Port : 54222 | Protocol : tcp | Tls : true

Collector: DMZCollect
Collector Last Active: Jul 15, 2024 11:24:46 AM
Event Source Last Active: Jul 15, 2024 11:24:42 AM

50 EPM

In Barracuda, go to Email Gateway Defense (Email Security) > Account Management

- ➢ Add the public IP of the DMZ-Collect here.
- ➢ Test the connection under action to ensure that the port is reachable.



End users on the new interface will now see an updated sidebar menu for navigation. Learn more
Dismiss

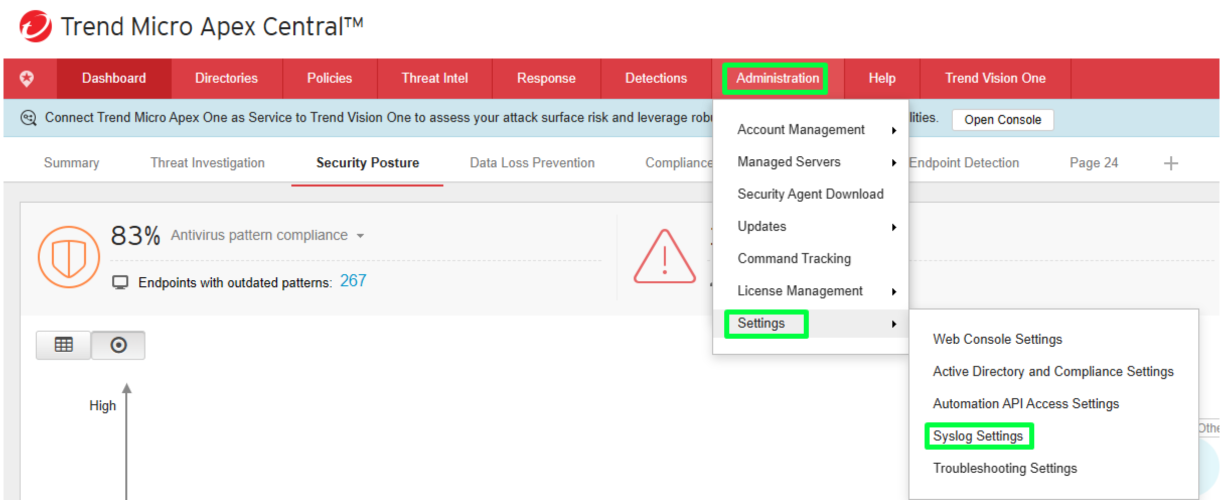
Introducing the Enhanced User Interface with Advanced Authentication
We're gradually rolling out the new user interface for your end users. To fully embrace the enhanced security features of our new user interface, we kindly request you to review and accept app
Dismiss

Account Management

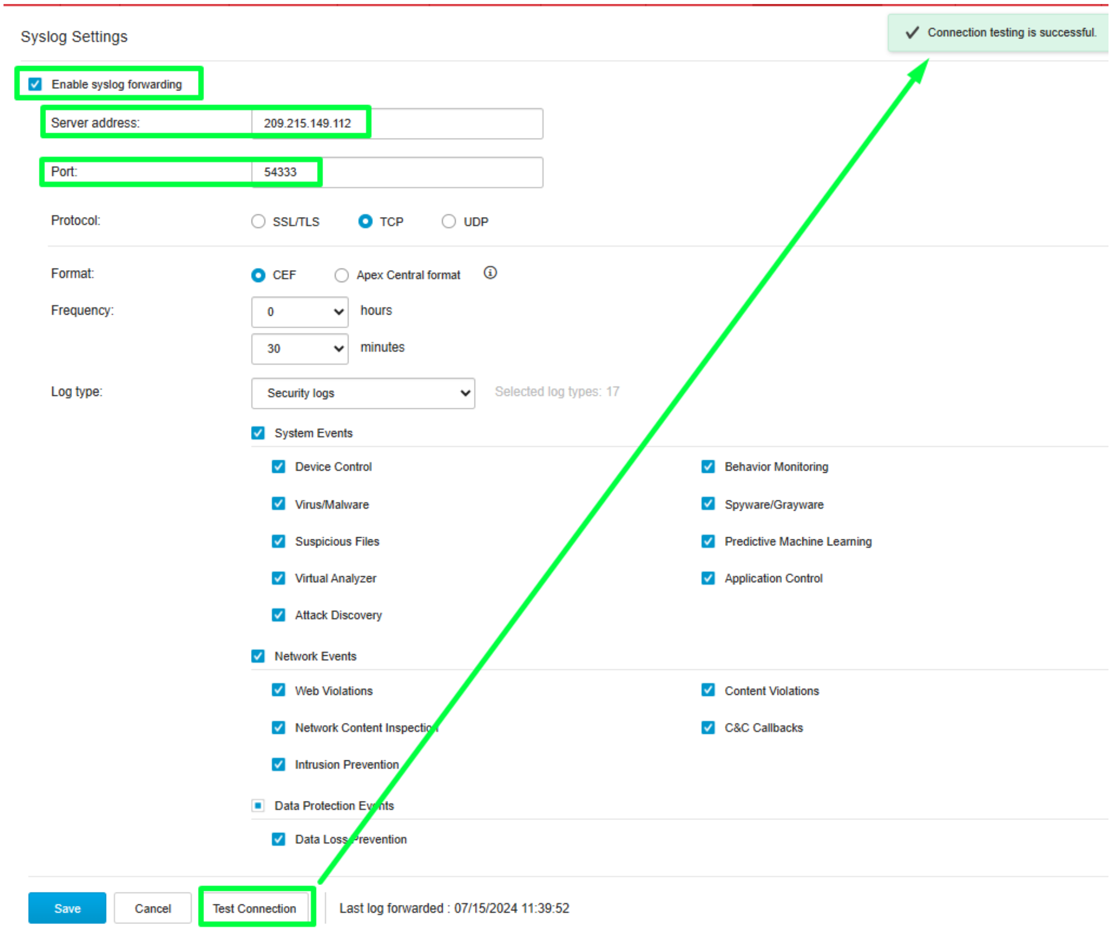
Syslog Integration

| IP Address / Hostname | Port | Actions | |
|---|---|---|---|
| [redacted]149.112<br>TCP+TLS is required to connect successfully. Non-TLS is not supported | 54222 | Test Delete | Server Status: Port Reachable |

In Trend Micro Apex Central, go to Administration> Settings > Syslog Settings



- ➢ Ensure that “syslog forwarding” is **Enable**.
- ➢ The Server IP address will be the DMZ-Collect public IP address, port **54333**, protocol **TCP.**



Syslog Settings

✓ Connection testing is successful.

☑ Enable syslog forwarding

Server address: 209.215.149.112

Port: 54333

Protocol: ○ SSL/TLS ● TCP ○ UDP

Format: ● CEF ○ Apex Central format

Frequency: 0 hours

30 minutes

Log type: Security logs Selected log types: 17

☑ System Events

☑ Device Control ☑ Behavior Monitoring

☑ Virus/Malware ☑ Spyware/Grayware

☑ Suspicious Files ☑ Predictive Machine Learning

☑ Virtual Analyzer ☑ Application Control

☑ Attack Discovery

☑ Network Events

☑ Web Violations ☑ Content Violations

☑ Network Content Inspection ☑ C&C Callbacks

☑ Intrusion Prevention

▪ Data Protection Events

☑ Data Loss Prevention

Last log forwarded : 07/15/2024 11:39:52

| Version | Date | Author | Status | Notes |
|---|---|---|---|---|
| 1.0 | 07/15/2024 | Soklim Seang | Draft | Initial document creation. |
| 1.1 | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |