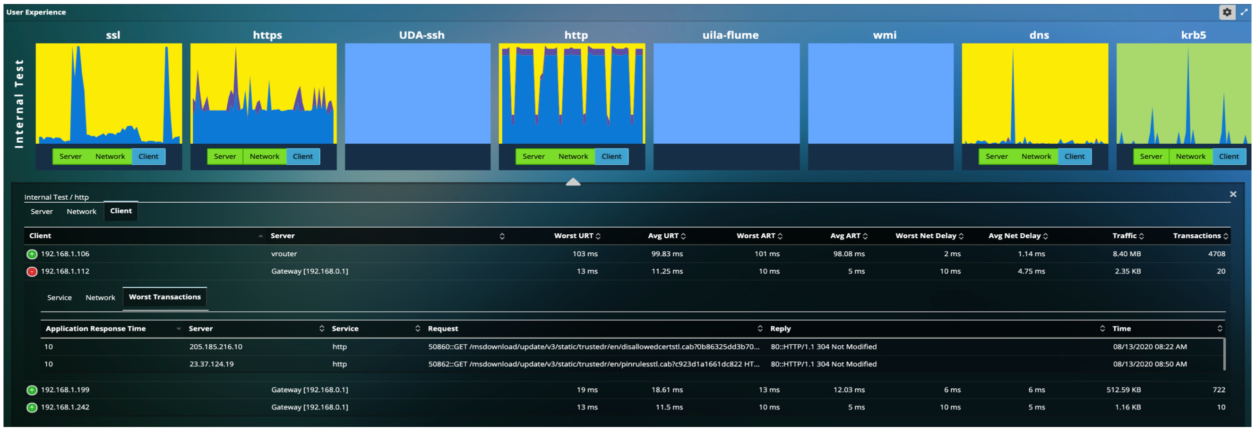
Version 3.6
Release Notes – 9/1/2020

Table of Contents

New Features

- **Tracking end-user experience down to the client**
  With remote working becoming the "new normal", being able to isolate and troubleshoot end-user performance challenges becomes very important. In this new release, with the end-user experience capability, you can now track down the challenges all the way to the client. By clicking on the individual application/protocol performance chart, you get a list of all the clients that are using that application/protocol and details on the service, network and the worst transactions for that end-user client.



Internal Test / http

Server | Network | **Client**

Client	Server	Worst URT	Avg URT	Worst ART	Avg ART	Worst Net Delay	Avg Net Delay	Traffic	Transactions
192.168.1.106	vrouter	103 ms	99.83 ms	101 ms	98.08 ms	2 ms	1.14 ms	8.40 MB	4708
192.168.1.112	Gateway [192.168.0.1]	13 ms	11.25 ms	10 ms	5 ms	10 ms	4.75 ms	2.35 KB	20

Service | Network | **Worst Transactions**

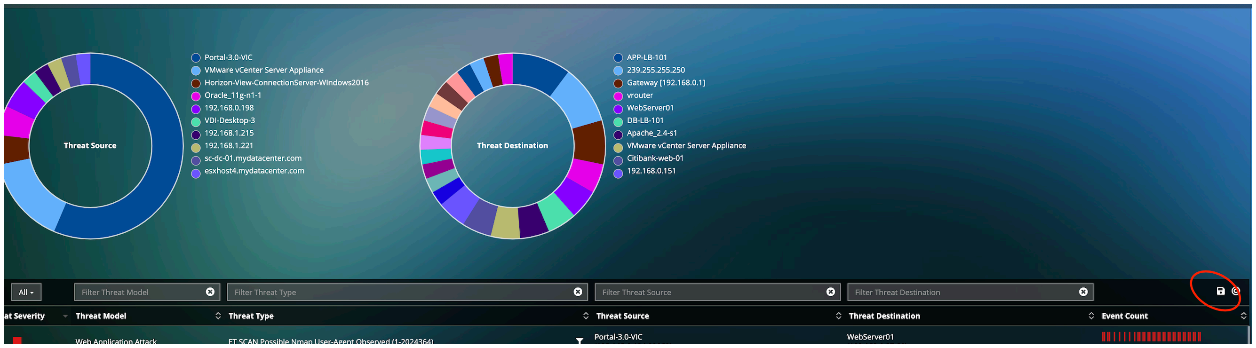
Application Response Time	Server	Service	Request	Reply	Time
10	205.185.216.10	http	50860::GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?0b86325dd3b70...	80::HTTP/1.1 304 Not Modified	08/13/2020 08:22 AM
10	23.37.124.19	http	50862::GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c923d1a1661dc822 HT...	80::HTTP/1.1 304 Not Modified	08/13/2020 08:50 AM

Client	Server	Worst URT	Avg URT	Worst ART	Avg ART	Worst Net Delay	Avg Net Delay	Traffic	Transactions
192.168.1.199	Gateway [192.168.0.1]	19 ms	18.61 ms	13 ms	12.03 ms	6 ms	6 ms	512.59 KB	722
192.168.1.242	Gateway [192.168.0.1]	13 ms	11.5 ms	10 ms	5 ms	10 ms	5 ms	1.16 KB	10

- **Visualization of clients behind a Load Balancer in Dependency Mapping**
  With this new capability, you can now visualize the dependency map between the real client IP address behind the Load Balancer that is using the X-Forwarded-Proto HTTP Protocol to the server they are connecting.

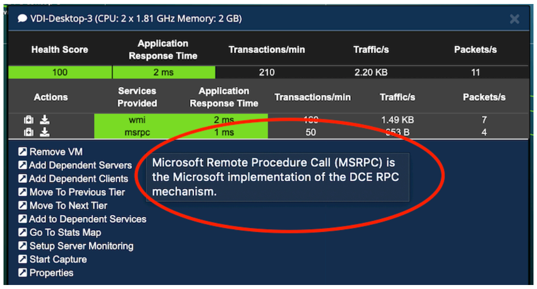
Enhancements

- **Export Identified Threat list**
  Uila Cyber Threat Monitoring module users can now export the list of threats that have been identified in their deployment to a CSV file with a single click.



at Severity	Threat Model	Threat Type	Threat Source	Threat Destination	Event Count
	Web Application Attack	ET SCAN Possible Nmap User-Agent Observed (1-2024364)	Portal-3.0-VIC	WebServer01	

- **Tooltip description for classified built-in applications/protocols**
  Users can now visualize a brief description on the classified built-in applications/protocols via a tooltip.



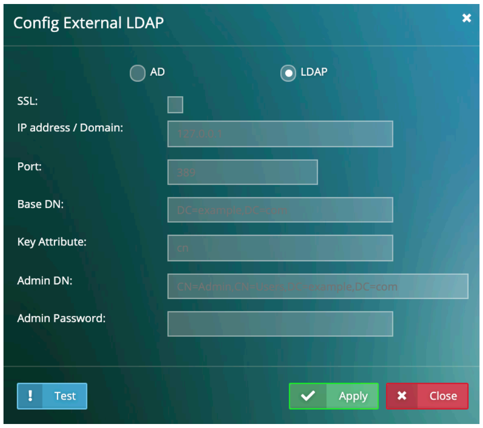
VDI-Desktop-3 (CPU: 2 x 1.81 GHz Memory: 2 GB)

Health Score	Application Response Time	Transactions/min	Traffic/s	Packets/s
100	2 ms	210	2.20 KB	11

Actions	Services Provided	Application Response Time	Transactions/min	Traffic/s	Packets/s
	wmi	2 ms	100	1.49 KB	7
	msrpc	1 ms	50	653 B	4

Microsoft Remote Procedure Call (MSRPC) is the Microsoft implementation of the DCE RPC mechanism.

- **Importing group of LDAP users**
  Since many releases, Uila has supported importing of LDAP users to create Uila user accounts. With this release we have further enhanced it to import groups of LDAP users.



Config External LDAP

○ AD ● LDAP

SSL: □

IP address / Domain: 127.0.0.1

Port: 389

Base DN: DC=example,DC=com

Key Attribute: cn

Admin DN: CN=Admin,CN=Users,DC=example,DC=com

Admin Password:

- **New Application and Protocol Supported**
  This release includes support for over 30 new application and protocol classification including Rockwell API, Direct Internet Message Encapsulation (DIME), Moxa, Microsoft SQL Server Analysis Services (MS-SSAS), Distributed File System Replication (DFSR), etc. Access the supported list from: https://www.uila.com/resources/documentation

Bug Fixes

- Sometimes, the URL to download a Uila report doesn’t contain a valid UMAS IP Address.
- Traffic dropped under special circumstances in NSX-T environment.
- Cannot display worst transactions for VMs with Chinese symbols in name.
- Wrong DNS names for external devices.
- Show negative values for some port stats.
- Missing storage stats on storage dashboard widget
- Cyber Threat Monitoring license warning messages even though module is not activated.
- Failed to pick up performance counters for Horizon virtual desktops when they are continuously removed and spawned.
- Filter by location does not work for Data exfiltration traffic.

Known Issues

- In certain situations, some VMware hosts may randomly drop out of topology.
- Users don’t see empty virtual switch on vST configuration page.
- A large amount of Uila rescheduled reports may lead the UMAS disk to get full.
- Certain Internet services may generate too many alerts.
- Cannot hold threshold adjustments for non-persistent Horizon Virtual Desktop VMs.

Contact Uila Support

Uila software solutions are designed with ease of installation and simplified maintenance in mind. The Uila team is dedicated to exceeding your expectations and knows that any downtime is too much in today's competitive world. Our goal is to keep your applications running 24 X 7. We offer a simple and effective support program to meet your needs.
Customers who purchased Uila products and under support contract will receive the following benefits:

- 24 X 7 support
- Unlimited support via email or phone call
- Free software minor release update
- Free software major release upgrade

Email: support@uila.com
Phone: (408) 819-0775

About Uila

Uila provides Performance and Cyber Threat Analytics in a single pane of glass for the Hybrid Enterprise. With Uila, IT Operations teams can visualize application workload dependencies across cloud platforms, right-size resources and investments for their workloads and plan workload migration strategies for Hybrid and Multi-Cloud deployments. Uila allows security teams to combat advanced cyber threats by providing immediate and comprehensive application-centric insight into lateral movement-based threats for the Hybrid Enterprise. Businesses use Uila to align themselves with their IT teams and cut time to resolution from days to minutes, keep their application at peak performance and secure at all times and ensure end-user satisfaction to the fullest across cloud boundaries.