MARTELLO

Savision is a subsidiary
of Martello Technologies

VANTAGE DX ANALYTICS

INTEGRATION GUIDE

RELEASE 3.15

DOCUMENT DATE: FEBRUARY 26, 2024

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Martello Technologies Corporation. The information is subject to change without notice and should not be construed in any way as a commitment by Martello Technologies or any of its affiliates or subsidiaries. Martello Technologies and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

Integration Guide
Release 3.15 - February 26, 2024

Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 1

Introduction

Document Purpose and Intended Audience

This guide is intended to help you understand the type of information that Vantage DX Analytics retrieves from monitoring tools and ITSM systems. It also provides information to help you configure integrations between your monitoring tools and ITSM systems and VDX Analytics.

This guide is intended for administrators and IT support personnel.

Revision History

Document Date	Description
February 26, 2024	Vantage DX Analytics Integration Guide Release 3.15

CHAPTER 2

Integration Capabilities

Use the following sections to understand the information that VDX Analytics retrieves from each integrated source system, as well as the supported ITSM actions you can perform between VDX Analytics and the integrated source systems that support ITSM capabilities.

> **Note:** This information describes the maximum possible capabilities. However, these capabilities depend on your implementation of the integrated source system, including sufficient permission levels from the source system to allow VDX Analytics to access all required data and functionality.

- "Overview of Supported Integrations" on page 6
- "Detailed Integration Capabilities" on page 9

Overview of Supported Integrations

Use the following sections to understand the general capabilities of supported VDX Analytics integrations:

- "IT Monitoring Systems" on page 6
- "Virtualization and Cloud Solution Systems" on page 7
- "IT Service Management Systems" on page 8
- "Notification and Automation Systems" on page 9
- "Devices" on page 9

IT Monitoring Systems

The following table summarizes the general capabilities of the IT Monitoring tools that integrate with VDX Analytics:

Table 1: IT Monitoring Tools Summary

Source System	Retrieve Objects	Retrieve Health states	Retrieve Object Relationships	Retrieve Alarms, Alerts	Act on Alarms, Alerts	Retrieve Incidents
AppDynamics	✓	✓	✓	✓	—	—
Broadcom DX APM	✓	✓	✓	✓	—	—
Mitel Performance Analytics	✓	✓	✓	✓	✓	—
Nagios	✓	✓	✓	✓	✓	—
PRTG	✓	✓	✓	✓	✓	✓
SCOM	✓	✓	✓	✓	✓	—
SolarWinds (NPM, APM, VIM)	✓	✓	✓	✓	✓	—
Splunk	✓	✓	—	✓	—	—
Vantage DX Diagnostics	✓	✓	✓	✓	—	—
Vantage DX Monitoring	✓	✓	✓	✓	—	—
WhatsUp Gold	✓	✓	✓	✓	—	—
Zabbix	✓	✓	✓	✓	✓	—

For details on the capabilities of each of the IT Monitoring tools see "IT Monitoring Systems Capabilities" on page 9.

Virtualization and Cloud Solution Systems

The following table summarizes the general capabilities of the Virtualization and Cloud Solution tools that integrate with VDX Analytics:

Table 2: Virtualization and Cloud Solution Tools Summary

Source System	Retrieve Objects	Retrieve Health states	Retrieve Object Relationships	Retrieve Alarms, Alerts	Act on Alarms, Alerts	Retrieve Incidents
Amazon Web Services (AWS)	✓	✓	✓	✓	—	—
Azure	✓	✓	—	—	—	—
Azure Insights	✓	✓	✓	✓	—	—
Microsoft 365	✓	✓	✓	✓	—	—
Microsoft 365 Teams Call Quality Dashboard (CQD)	✓	✓	✓	✓	—	—
VMware vCenter	✓	✓	✓	✓	✓	—

For details on the capabilities of each of the Virtualization and Cloud Solution tools see "Virtualization and Cloud Solution Systems Capabilities" on page 15

IT Service Management Systems

The following table summarizes the general capabilities of the IT Service Management tools that integrate with VDX Analytics:

Table 3: IT Service Management Tools Summary

Source System	Retrieve Objects	Retrieve Health states	Retrieve Object Relationships	Retrieve Incidents	Act on Incidents
Cherwell	✓	—	✓	✓	✓
ServiceNow	✓	—	✓	✓	✓

For details on the capabilities of each of the IT Service Management tools see "IT Service Management Systems Capabilities" on page 20.

Notification and Automation Systems

The following table summarizes the general capabilities of the Notification and Automation tools that integrate with VDX Analytics:

Table 4: Notification and Automation Tools Summary

Source System	Act on Notifications
Derdack Enterprise Alert	✓
Email Notification	✓
PowerShell	✓

For details on the capabilities of each of the Notification and Automation tools see "Notification and Automation Systems Capabilities" on page 21.

Devices

The following table summarizes the general capabilities of the Device integration with VDX Analytics:

Table 5: Device Summary

Source System	Retrieve Objects	Retrieve Health states	Retrieve Alarms, Alerts	Retrieve Call Detail Record
AudioCodes SBC	✓	✓	✓	✓

For details on the capabilities of each of the Devices see "Devices Capabilities" on page 21.

Detailed Integration Capabilities

Use the following sections to understand the detailed capabilities of VDX Analytics integrations:

- "IT Monitoring Systems Capabilities" on page 9
- "Virtualization and Cloud Solution Systems Capabilities" on page 15
- "IT Service Management Systems Capabilities" on page 20
- "Notification and Automation Systems Capabilities" on page 21
- "Devices Capabilities" on page 21

IT Monitoring Systems Capabilities

The following table details the specific capabilities of the IT Monitoring tools that integrate with VDX Analytics:

Table 6: IT Monitoring Tools Details

Capability	Details
AppDynamics	
Retrieve objects (including all raw property information)	Retrieves computers, applications, tiers, nodes, business-transactions and application back-ends.
Retrieve health states	Retrieves health states based on application events and Health Rule violations.
Retrieve object relationships	Retrieves: • Business Application Contains Tier • Business Application References Backend • Tier Contains Node • Machine Hosts Node • Tier Contains Machine • Tier Contains Business Transaction.
Retrieve alerts and alarms	Retrieves alerts from application events.
Broadcom DX Application Performance Management (DX APM)	
Retrieve objects (including all raw property information)	Retrieves agent management module elements.
Retrieve health states	Retrieves health states of the agent management module elements.
Retrieve object relationships	Retrieves relationships between the agent and the managed modules.
Retrieve alerts and alarms	Retrieves alerts from the agent management modules.
Microsoft System Center Operations Manager (MS SCOM)	
Retrieve objects (including all raw property information)	Retrieves all entities including all property values. Component types are derived from the base classes of the entities.

Capability	Details
Retrieve health states	Retrieves health states, maintenance mode and availability information of the entities.
Retrieve object relationships	Retrieves all relationships between all entities.
Retrieve alerts and alarms	Retrieves all monitoring alerts.
Act on alerts and alarms	Set the resolution state of alerts to Acknowledged. Set the resolution state of alerts to Closed (255). Update the following alert properties: Owner, Ticket ID, Resolution State, and all custom fields.
Mitel Performance Analytics (MPA)	
Retrieve objects (including all raw property information)	Retrieves components (devices and containers).
Retrieve health states	Retrieves component health states.
Retrieve object relationships	Retrieves component relationships.
Retrieve alerts and alarms	Retrieves alerts (alarms).
Act on alerts and alarms	Set alert properties, acknowledge, resolve alerts.
Nagios Core and Nagios Xi	
Retrieve objects (including all raw property information)	Retrieves hosts, services and groups.
Retrieve health states	Retrieves health states of hosts and services.
Retrieve object relationships	Retrieves relationships between host and service groups with the containing hosts and services.

Capability	Details
Retrieve alerts and alarms	Retrieves alerts by translating unhealthy state changes of hosts and services into alerts.
Act on alerts and alarms	In Nagios, acknowledge alerts. You must configure the Nagios server for this capability. In Icinga2, acknowledge problems. No additional configuration required.
PRTG Network Monitor (PRTG)	
Retrieve objects (including all raw property information)	Retrieves sensors, devices and groups. The type of devices are derived from the group name the devices are related to.
Retrieve health states	Retrieves health states of sensors, devices and groups. Health states of devices and groups can be calculated based on the worst sensor state or the device or group status (configurable on the Settings > Integrations page).
Retrieve object relationships	Retrieves relationships between devices and sensors, and between groups and devices.
Retrieve alerts and alarms	Retrieves alerts for unhealthy sensors.
Act on alerts and alarms	Acknowledge unhealthy sensor alerts.
Retrieve incidents	Retrieves Incidents from PRTG.
SolarWinds Network Performance Monitor (NPM), Application Performance Monitor (APM), Virtual Infrastructure Monitor (VIM)	
Retrieve objects (including all raw property information)	Retrieves nodes, volumes, groups, virtual machines (VIM), applications (APM), network interfaces (NPM) and transactions (SUEM).

Capability	Details
Retrieve health states	Retrieves health states of all collected objects based on the Status property using the following logic: • Healthy status includes: Up, Dormant, Active, Inactive, Expired • Warning status includes: Warning, Mixed Availability, Misconfigured, Unconfirmed • Critical status includes: Down, Shutdown, Lower Layer Down, Unreachable, Critical • Not Monitored status includes: External, Monitoring Disabled • In Maintenance Mode status includes: Unmanaged • Unknown status includes: Unknown, Testing, Not Present, Unplugged, Could not Poll, Disabled, Not Licensed
Retrieve object relationships	Retrieves group member relationships and all relationships between components.
Retrieve alerts and alarms	Retrieves all alerts.
Act on alerts and alarms	Set Acknowledged field of alert to True. Set State field of alert to Reset.
Splunk	
Retrieve objects (including all raw property information)	Retrieves rules from services, alerts, fired_alerts.
Retrieve health states	Retrieves health states of the rules from services, alerts, fired_alerts details.
Retrieve alerts and alarms	Retrieves alerts from services, alerts, fired_alerts.
Vantage DX Diagnostics	
Retrieve objects	Retrieves site groups, sites, probes, service instances, and site services.
Retrieve health states	Retrieves health states of retrieved objects.

Capability	Details
Retrieve object relationships	Retrieves relationships between sites with probes and the related site services, and between service instances and related site services.
Retrieve alerts and alarms	Retrieves alerts.
Vantage DX Monitoring	
Retrieve objects	Retrieves robot managers, robots, and groups (based on the configured tags).
Retrieve health states	Retrieves health states of retrieved objects.
Retrieve object relationships	Retrieves relationships between robots and robot applications.
Retrieve alerts and alarms	Retrieves alerts.
VMware vCenter	
Retrieve objects (including all raw property information)	Retrieves all host systems and virtual machines.
Retrieve health states	Retrieves healthy, warning, critical states and maintenance mode information of host systems and virtual machines.
Retrieve object relationships	Retrieves relationships between the hosts and virtual machines.
Retrieve alerts and alarms	Retrieves active alarms from hosts and virtual machines and translate them into alerts.
Act on alerts and alarms	Acknowledge alarms from hosts and virtual machines.
WhatsUp Gold	
Retrieve objects (including all raw property information)	Retrieves devices and device groups.

Capability	Details
Retrieve health states	Retrieves health states based on the nInternalMonitorState field of the device or device group as follows: 1 is Critical, 2 is Maintenance Mode, 3 is Healthy, everything else is Unknown.
Retrieve object relationships	Retrieves relationships between device groups and between device group and devices.
Retrieve alerts and alarms	Retrieves alerts when devices go down.
Zabbix	
Retrieve objects (including all raw property information)	Retrieves hosts and host groups (shown in VDX Analytics as objects and groups).
Retrieve health states	Retrieves health states of the hosts, based on active problem events. A worst health state roll-up is performed for the host groups.
Retrieve object relationships	Retrieves all relationships between hosts and host groups.
Retrieve alerts and alarms	Retrieves events from triggers, items and discovery rules and displays as alerts.
Act on alerts and alarms	Zabbix problem events are acknowledged in VDX Analytics without closing the problem.

Virtualization and Cloud Solution Systems Capabilities

The following table details the specific capabilities of the Virtualization and Cloud Solution tools that integrate with VDX Analytics:

Table 7: Virtualization and Cloud Solution Tools Details

Capability	Details
Amazon Web Services (AWS)	

Capability	Details
Retrieve objects (including all raw property information)	Retrieves the following objects: • Auto Scaling Group • Availability Zone • Cloud Formation Stack • DB Cluster • DB Instance • EC2 Host • EC2 Instance • EC2 Volume • Elastic Beanstalk Application • Elastic Beanstalk Application Environment • Elastic Classic Load Balancer • Elastic Application Load Balancer • Elastic Load Balancing Target Group Can be extended with Lambda functions, CloudTrail, Resource Groups, and Route 53 objects.
Retrieve health states	Retrieves health states of all the above objects.
Retrieve object relationships	Retrieves the following relationships: • Availability Zone contains Objects (DB Clusters, DB Instances, EC2 Hosts EC2 Volumes, Load balancers) • Auto scaling group contains Load balancers, EC2 Instances hosts EC2 Volumes • Elastic Beanstalk Application Environment contains Elastic Beanstalk Application • DB Cluster contains DB instances • EC2 Host contains EC2 instances • Elastic Classic Load balancer contains instances • Resource Groups contain all above objects
Retrieve alerts and alarms	Retrieves alerts from CloudWatch metric alarms.
Azure	

Capability	Details
Retrieve objects (including all raw property information)	Retrieves virtual machines, virtual machines ARM, sites and databases.
Retrieve health states	Retrieves health states based on the following: • An online database is Healthy; an offline database is Critical • A running web site is Healthy; a web site that is not running is Critical • A VM Powerstate of Starting or Running is Healthy; all other Powerstates are Critical
Azure Monitor (Application Insights)	
Retrieve objects (including all raw property information)	Retrieves all configurations (relationships to Subscriptions). Within a tenant, per subscription or all subscriptions are converted to groups with no states.
Retrieve health states	Retrieves all resource groups, (shown as groups in VDX Analytics), such as virtual machines, storage accounts, virtual networks, web applications, databases and database servers, with their health states.
Retrieve object relationships	Retrieves all resource components with their health states (for example, application insight, application, virtual machine, or process).
Retrieve alerts and alarms	Retrieves all alerts that relate to resources.
Microsoft 365 Teams Call Quality Dashboard (CQD)	
Retrieve objects (including all raw property information)	Retrieves users and user devices, geographical locations, ISPs, conference calls, dynamic offices, TCP calls, Microsoft Data Center, and user call ratings.
Retrieve health states	Retrieves health states for user devices.

Capability	Details
Retrieve object relationships	Retrieves the following object relationships: • Country and user devices • City and user devices • ISPs and user devices • Users and user devices • Meetings and user devices • Dynamic offices and user devices • PSTN carriers and user devices • PSTN trunks and user devices
Retrieve alerts and alarms	Retrieves alerts for poor, failed and dropped calls.
Microsoft 365	
Retrieve objects (including all raw property information)	Retrieves the following objects: • Microsoft 365 services and service features • Microsoft 365 licenses (active and available) • Microsoft Teams meeting room and IP phone devices, including: • ipPhone • teamsRoom • surfaceHub • collaborationBar • teamsDisplay • touchConsole • lowCostPhone • teamsPanel • sip

Capability	Details
Retrieve health states	The health states of Microsoft 365 services and service features are displayed based on Status and FeatureServiceStatus values as follows: • Critical: ServiceDegradation and ServiceInterruption • Warning: ExtendedRecovery, FalsePositive, Investigating, and RestoringService • Healthy: ServiceOperational, ServiceRestored, and InformationAvailable • Not Monitored: InformationUnavailable The health states of Microsoft 365 licenses are calculated as follows: • Critical: 0 licenses are available • Warning: Fewer than 2 licenses are available, or if you have more than 20 pre-paid licenses, fewer than 5 are available. The health states of Microsoft Teams meeting room and IP phone devices are displayed based on the Teams device health status as follows: • Critical: Critical • Warning: Offline, Non-Urgent • Healthy: Healthy • Unknown: Unknown
Retrieve object relationships	Retrieves relationships between Microsoft 365 services and service features.
Retrieve alerts and alarms	Retrieves alerts from service incidents and related messages. These display as alerts in VDX Analytics. The health state and alert severity is based on the service incident status.
VMware vCenter	
Retrieve objects (including all raw property information)	Retrieves host systems and virtual machines.

Capability	Details
Retrieve health states	Retrieves health states of objects based on overall status as follows: • gray: unknown • green: healthy • yellow: warning • red: critical
Retrieve object relationships	Retrieves relationships between host systems and virtual machines.
Retrieve alerts and alarms	Retrieves active alarms from hosts and virtual machines and translates them into alerts.
Act on Alarms and Alerts	Acknowledge alarms.

IT Service Management Systems Capabilities

The following table details the specific capabilities of the IT Service Management tools that integrate with VDX Analytics:

Table 8: IT Service Management Tools Details

Capability	Details
Cherwell	
Retrieve objects (including all raw property information)	Retrieves all configuration items and services.
Retrieve object relationships	Retrieves all relationships between configuration items, and between services and configuration items
Retrieve Incidents	Retrieves all incidents.
Act on Incidents	Create and update incidents.
ServiceNow	
Retrieve objects (including all raw property information)	Retrieves all CIs.
Retrieve object relationships	Retrieves all relationships between the CIs.
Retrieve Incidents	Retrieves all incidents.
Act on Incidents	Create and update incidents.

Notification and Automation Systems Capabilities

The following table details the specific capabilities of the Notification and Automation tools that integrate with VDX Analytics:

Table 9: Notification and Automation Tools Details

Capability	Details
Derdack Enterprise Alert	
Act on Notifications	A notification from VDX Analytics is sent as an event into Derdack.
Email Notification	
Act on Notifications	A notification from VDX Analytics is sent as an email using an SMTP server.
Powershell (Applies only to standalone deployments of VDX Analytics.)	
Act on Notifications	A notification from VDX Analytics triggers the execution of a pre-configured PowerShell script.

Devices Capabilities

The following table details the specific capabilities of the device integration with VDX Analytics:

Table 10: Device Details

Capability	Details
AudioCodes SBC	

Capability	Details
Retrieve objects (including all raw property information)	Retrieves the SBC device components including: • Type • Version • IP • RAM • CPU type • Quality of experience (QOE) feature setup • Security protocol • Codec • Performance metrics, such as memory and CPU • Network effectiveness ratio (NER) • SIP transaction rate
Retrieve health states	Retrieves the component health states.
Retrieve alerts and alarms	Retrieves SBC alarms and displays as alerts including, but not limited to the following: • TLS certificate expiry or mismatch • Trunk issues, such as loss of signal and trunk stopped • High availability issues such as system failure and configuration and network issues • Device issues such device failure, DNS unavailability, loss of remote monitoring connection, configuration, temperature, upgrade, and proxy connection • Security issues • Performance threshold • Network issues related to ethernet, LDAP, IPv6, HTTP, connection, and configuration
Call detail record	Retrieves call detail record (CDR) data that is displayed in the Calls Dashboard*. For information, see the Calls Dashboard section in the *VDX Analytics User Guide*. *The Calls Dashboard only supports CDR data for AudioCodes SBC version 7.4.

CHAPTER 3

Configure Integrations

Use the information in this section to complete the following tasks:

- Collect the information that you need for your integrations; review "Required Information" on page 23
- "Add an Integration" on page 23

Add an Integration

Use this procedure to integrate a monitoring system with VDX Analytics.

Before you Begin

For a list of the information required by each integration, see "Required Information" on page 23.

1. From the main menu, select **Settings**.
   The Integrations tab displays the currently installed integrations.
2. Click the **Add** button at the bottom of the page.
3. Select a monitoring system from the dialog box.
4. Enter the information required for the monitoring system.
5. Click **Save**.

Required Information

Before you add an integration, ensure that you have all of the information required to access the monitoring system. The information required varies depending on the monitoring system that you are connecting to.

The user permissions in the source system are important, because those permissions determine the access that VDX Analytics has to the source system. If the user in the source system does not have sufficient permissions, some data may not be visible in VDX Analytics and some functionality—such as the ability to close an alert—may not work.

Use the links below to find a list of the information required for each integration.

- "Amazon Web Services " on page 24
- "AppDynamics" on page 25
- "AudioCodes SBC" on page 26
- "Azure" on page 28
- "Azure Application Insights" on page 29
- "Broadcom DX Application Performance Management" on page 30
- "Cherwell" on page 31
- "Derdack Enterprise Alert" on page 32
- "Email Notifications" on page 32
- "Microsoft Teams Call Quality Dashboard" on page 34
- "Microsoft 365" on page 39
- "Microsoft System Center Operations Manager " on page 41
- "Microsoft Teams Notifications" on page 42
- "Mitel Performance Analytics" on page 43
- "Nagios Core and Xi" on page 44
- "PowerShell" on page 47
- "PRTG Network Monitor" on page 48
- "ServiceNow" on page 49
- "SolarWinds" on page 52
- "Splunk" on page 53
- "VMware vCenter" on page 53
- "WhatsUp Gold" on page 54
- "Zabbix" on page 55

Amazon Web Services

You must configure permissions in Amazon Web Services (AWS) before you can integrate it with VDX Analytics. The permissions must be assigned to the account that is used to access VDX Analytics. To assign these permissions, Martello provides a permissions policy that you can copy into AWS. For instructions, see the following Knowledge Base article:

https://helpcenter.martellotech.com/s/article/Configure-Permissions-in-Amazon-Web-Services-AWS

Configure the following properties when you integrate AWS with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote Agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Region	The region determines the URL used.
Access Key	—
Secret Access Key	—
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

AppDynamics

Configure the following properties when you integrate AppDynamics with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
URL	Required.
Tenant Account Name	The AppDynamics tenant account name.
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the account.
Collect infrastructure events	Select the checkbox to enable.

Property	Description
Collect application events	Select the checkbox to enable.
Collect policy violation events	Select the checkbox to enable.
Calculate service availability health by worse case roll-up	Select the checkbox to enable.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Optional Event Types

In VDX Analytics, you can select which events are collected. To simplify the types of events in VDX Analytics, we define three types:

- Infrastructure
- Application
- Policy violation

You can read more details about event types on the AppDynamics Events Reference page.

AudioCodes SBC

When you configure an integration between AudioCodes SBC and Vantage DX Analytics, you must provide a user account that Vantage DX Analytics can use to log in and retrieve information. You can use a Security Administrator account or a Monitor account for this purpose. If you use a Monitor account, you need to provide the Call Detail Records (CDR) Format file; if the format changes after you configure the integration, you must update this information. If you use a Security Administrator account, you do not need to enter or update this information.

Integrations are supported for AudioCodes SBC devices version 7.2 and higher. The data that VDX Analytics retrieves depends on the device version.

Before you Begin

A Security Administrator must perform the following step, regardless of the type of account you are using:

- Enable CDR logging for the device and set the destination of the log file to local.

Prerequisites for Monitoring Accounts

If you are using a Monitor account, perform the following steps:

1. Connect to the AudioCodes SBC using SSH.
2. Log into the device as a Security Administrator and enter the following commands in order:
   - enable
   - [AdminPassword]
   - configure system
   - cdr
   - cdr-format show-title local-storage-sbc

   The CDR format file is output to the screen.
3. Copy the output. You will need to paste it into the **Call Detail Records (CDR) Format File Content** field, as described in the table below.

Configure the following properties when you integrate AudioCodes SBC with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
IP Address / FQDN	Enter the FQDN or IP address of the SBC.
Port	Enter the port to access the REST API. The default is port 80.
Secure Connection (HTTPS)	Optional. Select the checkbox to use HTTPS.
User Name	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	Enter the password for the user account.
SNMP Version	Select V1, V2c or V3. The default is V2c.
SNMP Port Number	Enter the SNMP port number to use. Port 161 is the default.
SNMP Read-Only Community String	Displays for SNMP V1 and V2c. The community string to access read-only data from the SBC. The default is public.

Property	Description
V3 Security Level	Displays for SNMP V3. Select the permitted level of access. The default is ReadOnly.
V3 UserName	Displays for SNMP V3. Enter the user name.
V3 Auth Type	Displays for SNMP V3. Select the authentication method. The default is MD5.
V3 Password	Displays for SNMP V3. Enter the authentication password.
V3 Privacy Type	Displays for SNMP V3 when Security Level is set to ReadWrite. Select the privacy protocol type.
V3 Privacy Password	Displays for SNMP V3 when Security Level is set to ReadWrite. Enter the privacy password.
Call Detail Records (CDR) Format File Content:	If you are using an account with a Monitor role, paste the content of the CDR format file in the text area.
Auto Collect Call Detail Records (CDR) Format	Select this option only if you are using an account with an Administrator role.
SSH Server Port	Displays only when you select the option to Auto Collect Call Details Records (CDR) Format. Enter the port number to use when connecting to an AudioCodes SBC. The default port is 22.
Discovery Interval	Enter how often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	Enter how often health states and alerts are collected. The default is 120 seconds.

Azure

Before you Begin

Before VDX Analytics can integrate with Microsoft Azure, you must complete setup tasks in Azure. For more information, see the following Martello Knowledge Base article:

https://helpcenter.martellotech.com/s/article/Set-up-the-Azure-Connector

Configure the following properties when you integrate Microsoft Azure with VDX Analytics:

Property	Description
Azure Environment	Port 443
Tenant ID	Use the information provided in the Tenant ID properties in Microsoft Azure.
Subscription ID	Use the information provided in the enterprise application in Microsoft Azure. If you have multiple subscriptions, you can enter all of the IDs in this field, separated by commas. If you want to integrate all of your Azure subscriptions, you can leave this field blank and VDX Analytics will automatically integrate all of the subscriptions that are available in your tenant at the time of the integration.
Client ID	Use the information provided in the application registration in Microsoft Azure.
Client Secret	This information is part of the application registration in Microsoft Azure.
Agents	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Azure Application Insights

You must complete setup tasks in Azure Monitor before you can integrate Azure Application Insights with VDX Analytics. For more information, see the following Martello Knowledge Base article:

https://helpcenter.martellotech.com/s/article/Setup-Azure-Insights-Connector

Configure the following properties in Azure Monitor when you integrate Azure Application Insights with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Tenant ID	Use the information provided in the Tenant ID properties in Azure Monitor.
Client ID	Use the information provided in the application registration in Azure Monitor.
Client Secret Key	This information is part of the application registration in Azure Monitor.
Subscription IDs	Use the information provided in the enterprise application in Azure Monitor. If you have multiple subscriptions, you can enter all of the IDs in this field, separated by commas. If you want to integrate all of your Azure subscriptions, you can leave this field blank and VDX Analytics will automatically integrate all of the subscriptions that are available in your tenant at the time of the integration.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Broadcom DX Application Performance Management

Configure the following properties when you integrate Broadcom DX Application Performance Management (DX AMP) with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server that will communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.

Property	Description
URL	The URL to the rest API endpoint. Port 8081 is the default.
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the account.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Cherwell

Configure the following properties when you integrate Cherwell with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agents	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
URL	Default ports are 80 for HTTP or 443 HTTPS.
Authentication Mode	OAuth2 authentication is not currently available.
Client ID	Refer to the Cherwell website to obtain a Client ID for VDX Analytics. https://cherwellsupport.com/
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the account.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often incidents are collected. The default is 120 seconds.

Note: Due to a limitation of the Cherwell API, the timezone of the VDX Analytics Server/Agent must be the same as the Cherwell server.

Derdack Enterprise Alert

Configure the following properties when you integrate Derdack Enterprise Alert with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Server	The hostname, FQDN or IP address of the Derdack server.
Use SSL	Optional.
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the user.
Response URL	URL that can be used to navigate from Derdack Enterprise Alert to VDX Analytics.

Email Notifications

Vantage DX Analytics provides an SMTP server that is preconfigured for email notifications by default. No additional configuration is required unless you want to change the name of the configuration.

You can also configure your own SMTP server for email notifications by enabling the **Use My Own SMTP** option.

Configure the following properties when you integrate Email Notifications with VDX Analytics:

Property	Description
Integration Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server (Local Agent) or a machine that has a VDX Analytics Remote agent installed on it.
Use My Own SMTP	By default, this option is disabled and VDX Analytics uses a preconfigured SMTP server to send email notifications. If you prefer to use your own SMTP server, enable this option and provide the following settings: • From Email—The sending email address. • SMTP Server—The address of the SMTP server. • Port—The port to access the server. • Username—The username for the email account. • Password—The password for the account.
Send emails as HTML	Optional. Enabled by default.

Martello Vantage DX Diagnostics

This integration is available only for cloud-based deployments of Vantage DX.

You must configure an integration between Vantage DX Diagnostics and VDX Analytics for each site group that you monitor. Ensure that you have access to the Vantage DX Diagnostics interface before you begin to configure an integration. The Vantage DX Diagnostics interface provides information that you need to configure the integration for each site group. To find the required information, complete the following steps:

1. Click **Manage > Site Groups** and select a site group.
2. Next to Vantage DX Diagnostics Integration Configuration, click **Show**.

Configure the following properties when you integrate Vantage DX Diagnostics with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Vantage DX Diagnostics URL	URL of the Vantage DX Diagnostics site group. Copy and paste the URL provided on the Vantage DX Diagnostics interface.
Site Group GUI	Site group identifier. Copy and paste the URL provided on the Vantage DX Diagnostics interface.
Username	User name for the site group. Copy and paste the URL provided on the Vantage DX Diagnostics interface.
Password	The password for the integration. Copy and paste the URL provided on the Vantage DX Diagnostics interface.
Number of Alerts for Service to be Critical	The number of alerts reported by Vantage DX Diagnostics before the status of an endpoint is shown as Critical in VDX Analytics.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Microsoft Teams Call Quality Dashboard

Use the information in this section to configure the integration between VDX Analytics and your Microsoft Call Quality Dashboard (CQD).

Before you Begin

Before you configure the integration, ensure that you meet the requirements listed in "Requirements" on page 1.

Configure the following properties when you integrate the Microsoft Teams CQD with VDX Analytics to monitor remote users:

Property	Description
Set-up	

Property	Description
Integration Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Credentials	
Azure Login Name	The Microsoft 365 account that VDX Analytics can use to access the CQD.
Azure Login Password	The password for the Microsoft 365 account.
MFA Shared Secret (Optional)	The optional shared secret is used for multi-factor authentication for Azure Active Directory. To use this option, the account that VDX Analytics uses to connect to your Microsoft CQD must use Azure MFA with a passive authentication flow. In addition, the account must be cloud-native. To generate the password for this field, see the following Knowledge Base article: https://helpcenter.martellotech.com/s/article/000001082
Leverage Martello VDX Enterprise App	This option is enabled by default. We recommend that you do not change the setting. It allows the integration to use the permissions that you granted to the Martello VDX App when you first registered it.
Data Processing	
Tenant Size	Select the tenant size based on the number of users, or select Custom to provide an alternate value. The selected tenant size sets the defaults for the rest of the data processing values.
Data Retrieval Period	The number of days of data from the CQD to display in VDX Analytics. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Max Data Query Time (minutes)	The maximum time in minutes allowed for a single CQD query. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.

Property	Description
Data Window Incremental (minutes)	The amount of time in minutes that the CQD query will look back from the last call that was loaded into the database. The default value is 120 minutes; however, if you select a custom tenant size, you must enter a value.
Use Incremental Sync Start	When enabled, this option retrieves data beginning from the day of the integration, as opposed to VDX Analytics also retrieving historical data. This default value for this option changes, depending on the selected tenant size. If you selected a custom tenant size, you can enable or disable this option.
Split Properties over Multiple Queries	This option is disabled by default and cannot be enabled unless you selected a custom tenant size. Enable this option only if you are advised to do so by a Martello support engineer.
Add Good Calls as Information Events	Select this option if you want each call to display as a separate component in VDX Analytics. This option is disabled by default and cannot be enabled unless you selected a custom tenant size. ⚠ **Warning:** This option significantly increases the amount of data that VDX Analytics retrieves and stores. If you select this option, it may impact the performance of VDX Analytics.
Discovery Interval (minutes)	The interval for collecting components and relationships from the integrated system. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Operation Interval (minutes)	The interval for collecting alerts, incidents, and component health states. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Thresholds	

Property	Description
Poor Call Warning Ratio (%)	The threshold used by VDX Analytics to trigger a warning about the health status of a user device. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the Hours to Look Back for Health Status field. By default, the call warning ratio is 20%.
Poor Call Critical Ratio (%)	The threshold used by VDX Analytics to trigger a critical alert about the health status of a user device. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the Hours to Look Back for Health Status field. By default, the call critical ratio is 30%.
Jitter (ms)	Set the jitter threshold to use. Jitter indicates the size of the buffer that is needed to store packets before they are reconstructed in the correct order. Jitter can cause delays in calls and is an indicator of congestion of the network. Jitter is averaged over 15-second intervals for the duration of the call. Microsoft classifies call quality as poor when the average exceeds 30 ms. By default, VDX Analytics raises an alert when jitter exceeds the 30 ms threshold, but you can use this field to change the threshold that triggers an alert.
Round Trip Time (ms)	Set the round trip time (RTT) threshold to use. RTT is the time in milliseconds that it takes a data packet to travel from point A to B and return. It is determined by the physical distance between the two points, the speed of transmission, and the overhead taken by the routers in between. RTT is averaged over 15-second intervals for the duration of the call. A value over 500 ms can cause poor call quality. By default, VDX Analytics raises an alert when RTT exceeds the 500 ms threshold, but you can use this field to change the threshold that triggers an alert.

Property	Description
Packet Loss (%)	Set the packet loss threshold to use. The number of packets lost in a 15-second interval. Packet loss is calculated as a percentage. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%. By default, VDX Analytics raises an alert when packet loss exceeds the 10% threshold, but you can use this field to change the threshold that triggers an alert.
Localization	
Timezone	Data collected by the Microsoft CQD is stored in UTC. You can use this setting to have VDX Analytics convert from UTC to another time zone.
Localize Call Times	Select this option to show calls in the local timezone of the participant. When you select this option, the local time is shown for each endpoint in the call. VDX Analytics uses the geolocation to determine the local timezone. If geolocation information is not available, the timezone defaults to UTC.
Office Display Names	Optional. Use this field if you want to customize the office names that are displayed in the dashboards. To use this feature, complete the following steps: **1.** Create a .CSV file that lists the office names you wish to display. Enter one line for each office, using the following format: `<ipaddress>,<officename>,add` **2.** Upload the file to OneDrive. Ensure that the file is shared with the Microsoft 365 account that is assigned to the integration and that the file is downloadable. **3.** Click the main menu and select **Settings**. **4.** On the Integrations tab, locate the Microsoft CQD integration and clicking the **Edit** icon. **5.** In the **Office Display Names** field, enter the OneDrive link to the .CSV file that you shared with the Microsoft 365 account in Step 2. **6.** Click **Save**. If you do not use this option, offices are identified by their IP addresses only.
Privacy Protection	

Property	Description
Anonymize Data	Select this check box if you do not want to show identifiable information for your users, such as names, email addresses, and IP addresses. User information displays as number strings.
Disable Caller Resolution	Select this check box if you do not want to show identifiable information about call recipients. When you choose this option, VDX Analytics displays the name of the user who placed a call, but does not show the name of the call recipient
External Users	
Track External Users	Select this check box to include external users in the number of attendees who participated in Teams meetings. Vantage DX Analytics displays objects for external users and devices and provides a link to the meeting in which they participated.
Track External Users in Location Groups	Select this check box if you want to include external users in the groups that Vantage DX Analytics creates for cities and countries.
Options	
Health Status Period (hours)	The number of hours used to calculate the health status of objects. By default, this field is set to 48 hours; however, you can edit this value if you want to calculate the health status over a different period of time.
Disable Dashboard Data Retrieval	Select this check box if you do not want VDX Analytics to retrieve and store data for the dashboarding feature. If you select this option, ensure that you also disable the dashboarding feature using the options on the **Settings > General Settings** page.

Microsoft 365

Use the information in this section to configure an integration with Microsoft 365.

Before you Begin

You must register the Vantage DX application in the Azure Active Directory so that VDX Analytics can connect with the Microsoft Graph API and collect data from it.

There are two ways to automatically register the application and grant consent:

- Click the following URL and click **Accept** to grant consent when prompted: https://login.microsoftonline.com/common/adminconsent?client_id=0d75f118-91b7-4a02-8c52-25d8a1590a7c

- Use the Vantage DX Validation Tool and click **Accept** to grant consent when prompted: https://vdxvalidation.vantage-dx.com/

We recommend that you perform these steps before you configure the integration. When you configure the integration, select **Leverage Martello VDX Enterprise App** in the integration settings.

If you prefer to register the application and grant consent manually, refer to the following Knowledge Base article:

https://helpcenter.martellotech.com/s/article/Microsoft-365-Integration-VDX-A-Requirements

If you follow the manual process, ensure that the Microsoft Graph API has the following permissions:

- Organization.Read.All
- Reports.Read.All
- ServiceHealth.Read.All
- TeamworkDevice.Read.All (optional, for data collection from Teams meeting room devices)
- Place.Read.All

The tenant administrator needs to consent to the application permissions.

Configure the following properties when you integrate Microsoft 365 with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Leverage Martello VDX Enterprise App	Select this checkbox if you have used the automated option to register the application in Azure AD. When you select this option, you need to provide your Tenant ID only; you do not need to enter a Client ID or a Client Secret Key.
Tenant ID	Required. For information about how to find your Microsoft tenant GUID, see https://docs.microsoft.com/en-us/onedrive/find-your-office-365-tenant-id.

Property	Description
Client ID	The Application (Client) ID from the above Azure Application registration. This information is required only if you are registering the application and granting consent manually.
Client Secret Key	The Client Secret associated with the Azure Application registration. The Client Secret can have an expiry date configured; if your Client Secret has an expiry date, you will need to regenerate it and update the integration when it expires. This information is required only if you are registering the application and granting consent manually.
Collect Teams Devices	Optional. Select this checkbox to collect information about the following Teams meeting room devices: • Teams Room devices • Surface Hub devices • Teams Panel devices • Collaboration Bar devices • Teams Display devices • Touch Console devices
Collect IP Phones	Optional. Select this checkbox to collect information about the following Teams meeting room IP Phone devices: • IP Phone devices • Low-Cost Phone devices • SIP devices
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Microsoft System Center Operations Manager

Configure the following properties when you integrate Microsoft System Center Operations Manager (SCOM) with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Management Server	Port 5724.
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the SCOM account.
Operations Manager URL	Enter the URL of the SCOM Web Console.
Source System Navigation	Choose one of the following options: • Navigate to the SCOM web console for the source system—This is the default option and allows you to connect to the SCOM Console without the use of LiveMaps. • Navigate to LiveMaps for the source system—This option is available for customers who wish to use existing deployments of LiveMaps.
Load component states directly from SQL Server?	Select the checkbox to enable this function.
Load relationships per object?	Select the checkbox to enable this function.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Microsoft Teams Notifications

Configure the following properties when you integrate Microsoft Teams Notifications with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Integration Name	Provide a name for the integration; this name displays on the VDX Analytics interface. **Tip:** Include the name of the teams channel in the integration name. This will be useful when configuring the notification for a board or business service., as it will be obvious to which channel you are sending the notification.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server (Local Agent) or a machine that has a VDX Analytics Remote agent installed on it.
Webhook URL	Create a webhook in Microsoft Teams. This will allow you to send notification messages to a specific Teams channel. Perform the steps provided in the following article: https://docs.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook Copy the webhook URL and paste it here.

Note: A separate Teams integration is required for each Teams channel to which you want to send notifications.

Mitel Performance Analytics

Configure the following properties when you integrate Mitel Performance Analytics (MPA) with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
MPA URL	The URL of the MPA instance.
Login	The email address used to access the account.
Password	The password for the account.
Container GUID	Optional. The GUID of the container in MPA.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Nagios Core and Xi

Before you Begin

The Nagios integration supports two modes. Select one of the following modes and complete the prerequisites before you add the integration in VDX Analytics:

- "Nagios Core API Mode" on page 45: VDX Analytics pulls data from Nagios using the JSON API shipped with Nagios since release 4.0.7.
- "Martello API Mode" on page 46: VDX Analytics communicates with Nagios using the custom CGI endpoint shipped with VDX Analytics.

The Nagios integration allows VDX Analytics to interface with the majority of the current Nagios distributions, such as Nagios Core, Nagios XI, Icinga, Check_MK, Shinken.

Tip: For Nagios Core and Xi, you must install the CGI script if you want to use the Acknowledge Alerts feature. For the other Nagios forks, like Shinken or Check_MK, the Martello API Mode—including the installation of the CGI scripts—is required. The CGI scripts require the LiveStatus module to be installed.

Configure the following properties when you integrate Nagios Core and Xi with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Nagios API	Choose one of the APIs.
Server	The server Nagios is installed on.
Port	The port to access the server.
Secure Connection (HTTPS)	Optional.
Username	The username used to authenticate with Nagios.
Password	Password used to authenticate with Nagios.
VDX Analytics Endpoint URL	URL used to retrieve the data when you choose the Martello API mode.
Base URL	The URL used to open the Nagios web console from VDX Analytics.
Host URL	URL used to retrieve the data when you choose the Martello API mode.
Service URL	URL that is used to navigate from VDX Analytics to Nagios from a service component.
Host Group URL	URL that is used to navigate from VDX Analytics to Nagios from a host component.
Service Group URL	URL that is used to navigate from VDX Analytics to Nagios from a service group component.
Discovery Interval	Required. How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	Required. How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Nagios Core API Mode

Core API mode has the following requirements:

- Nagios Core 4.0.7 and up
- Python 2.7+ with modules cgi, cgitb, JSON installed
- Nagios must be configured to allow external commands. In your `nagios.cfg`, ensure the following settings have the required values:
  - `check_external_commands = 1` to enabled external commands.
  - `command_check_interval = -1` to check for external commands as often as possible.
- Restart Nagios after you make the changes listed above.

CGI Script Installation

Copy the `savisioniq.cgi` script located in the VDX Analytics installation folder. If this is a new installation, the directory is `%programfiles%\Martello iQ\Integrations\Nagios\Core Api\savisioniq.cgi`. If this is an upgrade, the directory is `%programfiles%\Savision iQ\Integrations\Nagios\Core Api\savisioniq.cgi`. Copy the script into the `Nagios cgi-bin` folder. On Nagios Core 4 and up the folder is `/usr/local/nagios/sbin`. Other Nagios installations maybe different.

Make sure that the `savisioniq.cgi` CGI Script is executable and associated with the user and group that is allowed to run Nagios. On Nagios Core 4 the user and group are **nagios**.

```
sudo chmod +x /usr/local/nagios/sbin/savisioniq.cgi
```

```
sudo chown nagios:nagios /usr/local/nagios/sbin/savisioniq.cgi
```

Configuration

Open the `savisioniq.cgi` script with an editor and change the following parameters to match your current Nagios configuration:

- **command_file** has to be set to the same value as **command_file** in your `nagios.cfg` (by default `/usr/local/nagios/var/rw/nagios.cmd`).
- **status_file** has to be set to the same value as **status_file** in your `nagios.cfg`.

Martello API Mode

Martello API mode has the following requirements:

- Python 2.7+ with modules cgi, cgitb, JSON installed.
- Any Nagios distribution that supports MK_LiveStatus.

If MK_Livestatus is not installed, you can install it manually. Refer to this article for more information: http://mathias-kettner.com/checkmk_livestatus.html.

The recommended MK_LiveStatus version is 1.4.0p34

CGI Script Installation

Copy the `savisioniq.cgi` script and the `livestatus.py` module from the VDX Analytics installation folder. If this is a new installation, the directory is `%programfiles%\Martello iQ\Integrations\Nagios\Savision Api`. If this is an upgrade, the directory is `%programfiles%\Savision iQ\Integrations\Nagios\Savision Api`. Copy the script and the module into the Nagios `cgi-bin` folder. On Nagios Core 4 and up the folder is `/usr/local/nagios/sbin`. Other Nagios installations may be different.

Make sure that the `savisioniq.cgi` CGI Script is executable and associated to the user and group that is allowed to run Nagios. On Nagios Core 4 the user and group are **nagios**.

```
sudo chmod +x /usr/local/nagios/sbin/savisioniq.cgi
```

```
sudo chown nagios:nagios /usr/local/nagios/sbin/savisioniq.cgi
```

Configuration

Enable the LiveStatus TCP Unix socket. By default, it is set to localhost, port 6557.

Open the `savisioniq.cgi` script with an editor and find the LiveStatus connection properties and change them to match your current LiveStatus configuration:

```
cmk_livestatus_nagios_server = "localhost"
```

```
cmk_livestatus_tcp_port = 6557
```

PowerShell

Configure the following properties when you integrate PowerShell with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics remote agent installed on it. If you are using a cloud deployment of VDX Analytics, you must choose the machine where the remote agent is installed.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Username	The username for the account that is authorized to run the PowerShell script as required.
Password	The password for the account that is authorized to run the PowerShell script as required.

Property	Description
Script	Enter the full name of the PowerShell script, including the file extension. The script is available in Vantage DX Analytics after you copy it to the **PSScripts** folder of the machine where the remote agent is installed.

PRTG Network Monitor

Configure the following properties when you integrate PRTG Network Monitor with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
URL	Default ports are 80 or 443.
Probe Id	Optional. Enter the probe ID only if you want to configure an integration with a specific probe. When you use this option, Vantage DX Analytics retrieves data from the specified probe only; it does not retrieve data from other probes in the same instance.
Username	The login name of a PRTG administrator user.
Password	The password for a PRTG administrator user.
Roll-up worst sensor state to components and groups	Optional. By default, PRTG does not roll-up the worst sensor state. When you enable this option, VDX Analytics calculates the states of the devices and groups based on the worst state of the related sensors.

Property	Description
Minimum number of items per request	This field controls the requests that VDX Analytics sends to PRTG. The default value is 2000 items per request. You can set the value higher to have the PRTG server send larger, less frequent responses to VDX Analytics. If the request times out before the PRTG server can respond with the number of requested items, you can lower the value.
Request delay in milliseconds	The interval between requests sent from VDX Analytics to the PRTG server. The default value is 1000 milliseconds.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

ServiceNow

Before you Begin

Configure your ServiceNow instance to work with VDX Analytics:

- Install the Vantage DX ServiceNow app in your instance of ServiceNow. You can find the application in the ServiceNow app store at https://store.servicenow.com/.
- Create a user with the x_savis_iq.Vantage DX role and check the Access Control List (ACL) settings. See "Vantage DX ServiceNow Roles and Permissions" on page 50 for more information.
- Specify port 443 for Port Access to the Instance.

Configure the following properties in VDX Analytics when you add the ServiceNow integration:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Instance Address	Use port 443 to connect to your ServiceNow instance.

Property	Description
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the user.
Fields for incident creation	Enable or disable retrieval of the following data: • Assignment Group • Assigned To • Category • Service • Service Offering • Impact • Urgency When these options are enabled, VDX Analytics retrieves this data from ServiceNow and includes it in new incidents and automatic notifications. When these options are disabled, the data is not retrieved. Both of these options are enabled by default.
Configuration Items Optional Data Retrieval	Enable or disable retrieval of the following data: • Component Types • Component Relationships When these options are enabled, VDX Analytics retrieves this data from ServiceNow and includes it in new incidents and automatic notifications. When these options are disabled, the data is not retrieved. Both of these options are enabled by default.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often incidents are collected. The default is 120 seconds.

Vantage DX ServiceNow Roles and Permissions

The x_savis_iq.Vantage DX role includes the following ServiceNow base system roles:

- personalize
- itil
- import_set_loader
- import_transformer

For information on what each of these roles can do, refer to the ServiceNow documentation: https://docs.servicenow.com/bundle/tokyo-platform-administration/page/administer/roles/reference/r_BaseSystemRoles.html

The following ServiceNow Access Control List settings should be configured by default. However, if you have configured ServiceNow to be more restrictive, you need to ensure that the following system table permissions are configured as outlined below.

System Table	Permission	Description
incident	read create (not active) write (not active)	Used to discover incidents.
cmdb_ci	read	Used to discover all configuration items
cmdb_rel_ci	read	Used to discover the relationships between the configuration items
cmdb_rel_type	read (only the sys_name and sys_id fields)	Used to discover the relationship type between configuration items
sys_user	read (only the sys_id, name, sys_updated_on, and sys_created_on fields) Note: A condition can be added to only show the VDX user.	Used to show a list with users to which an incident can be assigned
sys_user_grmember	read (only the group, user, sys_updated_on, and sys_created_on fields) Note: A condition can be added to only show the VDX user.	Used for showing the list of groups an incident can be assigned to and lookup the users per group
sys_db_object	read (only the sys_id, name, and super_class fields)	Used for discovering the types of the configuration items

System Table	Permission	Description
sys_choice	read (only the value and label fields) Note: We only need records with name=incident and element=state	Used to show all the possible states for an incident

SolarWinds

Configure the following properties when you integrate SolarWinds with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Server Name	Port 17778 access to the SolarWinds Server.
Connection Type	Possible values are HTTPS or NET TCP. If you choose NET TCP, set the FQDN of the SolarWinds server in the web.config file or in the Savision.UnityiQ.Agent.exe.config file in the case the integration is hosted by a remote agent.
Username	Enter an administrative account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the account.
URL	URL to Orion.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Note: We use the SolarWinds Information Service (SWIS) to load data from SolarWinds Orion: (https://github.com/solarwinds/OrionSDK/wiki/About-SWIS)

Splunk

Configure the following properties when you integrate Splunk with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Management URL with a port	Default Port: 8089
Web URL with a port	Default Port: 8000
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the account.
To add default Splunk alert rules	Check to enable.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

VMware vCenter

Configure the following properties when you integrate VMware vCenter with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
vCenter Server	Port 443 access to your vCenter Server.
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the account.
Use Single Sign-on (SSO)	Optional.
SSO Endpoint override	Configure the URL to the SSO endpoint.
vSphere Client Type	Select which web client is used to navigate from VDX Analytics to VMware vCenter.
vSphere Client URL	The URL to the VMware vCenter web client.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

WhatsUp Gold

Configure the following properties when you integrate WhatsUp Gold with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
SQL Server	SQL Server instance the WhatsUp database is on.

Property	Description
Use SQL Authentication	Optional.
User	Enter a user that has read permissions to access the WhatsUp database.
Password	The password for the user account.
Console URL	URL to the web console of WhatsUp Gold. This URL is used to navigate from VDX Analytics to WhatsUp Gold.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Zabbix

Configure the following properties when you integrate Zabbix with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
URL	URL to the endpoint where `api_jsonrpc.php` is located.
Username	Enter a user account that Vantage DX Analytics can use to log in and retrieve information.
Password	The password for the account.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

MARTELLO