MARTELLO | *Savision* is a subsidiary of Martello Technologies

VANTAGE DX ANALYTICS

INSTALLATION AND UPGRADE GUIDE

RELEASE 3.11

DOCUMENT DATE: JUNE 6, 2023

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.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Martello Technologies.

Trademarks

MarWatch™, Savision, Martello Technologies, GSX, and the Martello Technologies logo are trademarks of Martello Technologies Corporation.

Windows and Microsoft are trademarks of Microsoft Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

Installation and Upgrade Guide
Release 3.11 - June 6, 2023

Contents

CHAPTER 7

Introduction

Document Purpose and Intended Audience

This guide is intended to help you install Vantage DX Analytics or upgrade to Release 3.11. It contains information about the system requirements and the supported integrations.

Revision History

Document Date	Description
June 6, 2023	Vantage DX Analytics Installation and Upgrade Guide, Release 3.11

About Vantage DX Analytics

Vantage DX Analytics is a powerful IT Operations Analytics solution that integrates all your existing monitoring tools, cloud platforms and ITSM systems. VDX Analytics improves troubleshooting, decreases downtime and makes reporting easier. Using Elasticsearch, it can handle IT alerts in milliseconds, correlating them to help you understand the business impact and automate incident workflows. Straight out of the box, your teams can start to analyze data, streamline alerts and incident workflows and create business value dashboards.

Planning

The following sections provide information about the requirements that your system must meet before you can install or upgrade VDX Analytics.

- "Server Requirements" on page 8
- "IIS Roles and Features" on page 9
- "Java" on page 10
- "SQL Database" on page 10
- "Elasticsearch" on page 11
- "Active Directory" on page 12
- "Firewall Access" on page 13
- "Supported Upgrade Paths" on page 14

Server Requirements

You can install VDX Analytics on a Windows Server 2012 (or higher) running IIS 8.0 (or higher). We recommend that you use the latest available version of Windows Server. The server must be a member of an Active Directory domain, and VDX Analytics must be installed by a Domain user with local Admin rights.

We recommend that you install VDX Analytics on its own server. The following table lists the minimum requirements and recommendations for the server; however, the requirements depend on the number and size of your integrations. For deployments with more than 1 million components, please contact our IT-Ops Support Team at vdx-support@martellotech.com.

Table 1: Server Requirements and Recommendations

Component	Minimum Requirement	Recommended
Processor	2 GHz or faster 4 cores	2 GHz or faster 6 cores
Memory	16 GB or greater, but not greater than 64 GB	20 GB or greater, but not greater than 64 GB
Available Server Disk Space (Program Files Directory)	10 GB per integration	50 GB or greater per integration
Available SQL Server Disk Space	100 MB	200 MB
.NET Framework	4.7.2 or higher	4.7.2 or higher

Note: To determine how much memory to assign to Elasticsearch, see the formula listed in "Allocate Memory " on page 18.

IIS Roles and Features

The VDX Analytics installer can add the roles and features needed for VDX Analytics to function properly.

If you want to install the roles and features manually, add the roles and features listed in the table below to your Windows Server:

Table 2: Server Requirements and Recommendations

Web Server Components	Type
Roles	
Common	Default Document Static Content
Health and Diagnostics	HTTP Logging. Optional, but recommended for troubleshooting.
Security	Request Filtering Windows Authentication

Web Server Components	Type
Application Development	.NET Extensibility 4.5
	NET 4.5
	ISAPI Extensions
	ISAPI Filters
	WebSocket Protocol. Optional, but recommended.
Management Tools	IIS Management Console. We recommend that you install this on all IIS servers so you can manage them from a centralized Microsoft Management Console (MMC).
Features	
.NET Framework 4.6 Features	.NET Framework 4.6
	NET 4.5
	WCF Services:
	• HTTP Activation

In addition, ensure that you enable the following:

- Automatic start-up for the Windows Process Activation (WAS).
- World Wide Web Publishing (W3SVC) services.

> **Note:** VDX Analytics is installed as a new website with a self-signed certificate running on port 59212. You can change the port using the IIS Management Console under the bindings for the VDX Analytics website.

Java

VDX Analytics uses Elasticsearch to store the majority of its data. This allows it to retrieve information quickly. Elasticsearch requires Java, which is included in the Elasticsearch installation package. Ensure that you set the environment variable "ES_JAVA_HOME" to use the version of Java that is packed with Elasticsearch. You can set the variable at `%ProgramFiles%\Elasticsearch\elasticsearch\jdk`

SQL Database

VDX Analytics stores configuration information in a SQL database. We recommend that you use SQL Server 2012 or higher. The server can be a locally running instance

or an instance running in a cluster. VDX Analytics is also compatible with SQL Express.

If you are evaluating the software or wish to use SQL Express, you can download it using the following link: https://www.microsoft.com/en-us/download/details.aspx?id=55994.

During the installation, you are prompted to enter the SQL instance and user credentials that have permission to create a database. This same user account is used as the app pool account for VDX Analytics. After the installation is complete, you can adjust the account to a lower privilege level, as long as the account continues to have read/write permissions to the VDX Analytics database.

> **Note:** VDX Analytics requires the collation of your SQL instance to be case insensitive.

Elasticsearch

VDX Analytics requires Elasticsearch version 7.17.6. If Elasticsearch is not already installed, a single-node deployment is installed with VDX Analytics. This single-node deployment is suitable for evaluations; however, as a best practice, we recommend that you deploy an Elasticsearch cluster instead of a single node. You must deploy an Elasticsearch cluster when then the number of components from all your integrations exceeds 400,000.

Cluster Sizing

Follow the recommendations in the table below when you deploy VDX Analytics with an Elasticsearch cluster.

Table 3: Elasticsearch Cluster Sizing

Number of Components	Number of ES Nodes	VDX Analytics/ES Master Node	Date Node 1	Data Node 2
Less than 400,000	3	vCPU: 6 cores RAM: 24 GB	vCPU: 8 cores RAM: 24 GB SSD drives	vCPU: 8 cores RAM: 24 GB SSD drives
400,000 to 1 million	3	vCPU: 8 cores RAM: 32 GB	vCPU: 8 cores RAM: 32 GB SSD drives	vCPU: 8 cores RAM: 32 GB SSD drives
1 million to 3.5 million	3	vCPU: 8 cores RAM: 32 GB	vCPU: 10 cores RAM: 40 GB SSD drives	vCPU: 10 cores RAM: 40 GB SSD drives

For deployments with more than 3.5 million components, please contact our IT-Ops Support Team at vdx-support@martellotech.com.

Active Directory

By default, VDX Analytics queries the Global Catalog for available domain controllers and works with users and groups from all the domains in the forest.

To allow a user to target a specific Active Directory domain controller, you must edit the `Web.config` file. Add the following lines to the <appSettings> section:

```
<add key="ad.dc" value="" />
<add key="ad.user" value="" />
<add key="ad.password" value="" />
<add key="ad.domains" value="*" />

<add key="ad.scan_trusted_domains" value="false" />

<add key="ad.ignore_token_groups" value="true" />
```

If you use default values, the application reverts to the current Active Directory Forest settings.

```
<add key="ad.dc" value="<empty or Domain Controller>" />
<add key="ad.domains" value="<* or domains to query, separated by
comma>" />
```

The parameter `scan_trusted_domains` tells VDX Analytics to look for trusted domains in AD and is by default set to false.

The parameter `ignore_token_groups` tells VDX Analytics to ignore retrieving AD User groups by token groups. It is true by default.

These two parameters can make VDX Analytics slow if they are enabled.

Firewall Access

By default, VDX Analytics is installed as a website running under port 59212. You can change the port number if you wish.

Each integration has its own requirements for access. Your firewall rules for outbound traffic must allow VDX Analytics to communicate with the integrated system.

The following table lists the ports used by each monitoring system or ITSM that integrates with VDX Analytics. Some systems allow you to customize the port.

Table 4: Ports Required by Integrated Systems

Monitoring System or ITSM	Port
Amazon Web Services (AWS)	80 and 443
AppDynamics	443
Broadcom DX APM	8081
Cherwell	80 or 443
Cisco Prime	80 or 443
Derdack Enterprise Alert	80 (default) configurable by the VDX Analytics administrator using the following format: <server>:<port>
Ivanti Service Management (Powered by HEAT)	Service Management: 443 Cloud instance: 443 On-Premises: 80 or 443
Jira Software	443 (Default)
Microsoft Azure	443
Microsoft Office 365	443

Monitoring System or ITSM	Port
Nagios Core and XI	443 or configured in the URL
PowerShell	No ports are needed. The PowerShell integration runs on the VDX Analytics web server or on the Windows Server that a VDX Analytics Remote Agent is running on.
PRTG	Customizable port
ServiceNow	443
SolarWinds	17778
Splunk	8000 and 8089
System Center Operations Manager	5724
TopDesk	443
Vantage DX Monitoring	On-premises deployments: 80 (default but configurable) and 8080 (required for API access) Cloud-based deployments: 443 and 8443 (required for API access)
VMware vCenter	443
WhatsUp Gold	1433 (Default SQL server port)
Zabbix	80 (Default)

Supported Upgrade Paths

You can upgrade to VDX Analytics 3.11 from Release 3.7 or 3.9.

Installation Process

When you install VDX Analytics, the process that you follow depends on whether you are deploying VDX Analytics with an Elasticsearch cluster, or with a single Elasticsearch node. The following table lists the tasks for each type of deployment. Complete the tasks in the order listed for your deployment.

Task	Description
Deploy VDX Analytics with an Elasticsearch Cluster	
"Configure Elasticsearch " on page 17 • "Set up the Cluster" on page 17 • "Allocate Memory " on page 18 • "Test the Configuration" on page 19 • "Configure the Index Template" on page 20	Configure the Elasticsearch cluster on Windows servers. Complete all of the tasks in this chapter before you install VDX Analytics and connect it to the Elasticsearch cluster.
"Install VDX Analytics" on page 22	Install a new instance of VDX Analytics.
"Configure Connections" on page 25	Configure the connection strings in VDX Analytics with the IP addresses of the data nodes in the Elasticsearch cluster.
"Install Remote Agents" on page 26	Optional. Install a remote agent only if the source system is not accessible from the VDX Analytics web server.
"Add a License Key" on page 26	Activate the license.
Deploy VDX Analytics with a Single Elasticsearch Node	

Task	Description
"Install VDX Analytics" on page 22	Install a new instance of VDX Analytics.
"Install Remote Agents" on page 26	Optional. Install a remote agent only if the source system is not accessible from the VDX Analytics web server.
"Add a License Key" on page 26	Activate the license.
"Allocate Memory " on page 18	Assign additional memory in Elasticsearch.

Configure Elasticsearch

Complete the tasks in the table below to configure an Elasticsearch cluster on Windows servers. Ensure that you complete these tasks before you connect VDX Analytics to the Elasticsearch cluster.

If you are using Linux servers, contact our support team for more information.

Task	Description
"Set up the Cluster" on page 17	Install Elasticsearch and configure the names and IP addresses of the nodes.
"Allocate Memory " on page 18	Assign additional memory to Elasticsearch.
"Test the Configuration" on page 19	Verify that you can connect to each node in the cluster, and that the cluster is properly configured.
"Configure the Index Template" on page 20	Create a template for the Elasticsearch index.

> **Note:**
> In an Elasticsearch cluster, each node must be able to accept connections from the other nodes in the cluster. For this reason, we recommend that you enable authentication using X-Pack, which is pre-installed with Elasticsearch. For information about X-Pack, see the following URL:
>
> https://www.elastic.co/what-is/open-x-pack

Set up the Cluster

Use this procedure to install Elasticsearch and configure the names and IP addresses of the nodes. This procedure is for deploying Elasticsearch on

Windows servers. If you are using Linux servers, contact our support team for more information.

Before you Begin

Ensure that you have the following software available:

- **Elasticsearch 7.17.0**—The `Elasticsearch-7.17.0.exe` is included in the VDX Analytics installer file.
- **Notepad++**—To edit configuration files. You can also use Notepad running in administrator mode.

1. Run the `Elasticsearch-7.17.0.exe` on each node in the cluster. We recommend that you install the file on the SSD drive because all data will be stored in the installation location.
2. To create the cluster, edit the `Elasticsearch.yml` file on each node in the cluster.
   If this is a new installation, the default location of the file is
   `%programfiles%\Elasticsearch\elasticsearch\config\elasticsearch.yml`.

   If this is an upgrade, the default location of the file is
   `%programfiles%\Savision\Elasticsearch\elasticsearch\config\elasticsearch.yml`.

   Configure the following parameters:
   - `cluster.name`—This parameter is located in the Cluster section of the file. Assign a name for your cluster that will be used on all nodes.
   - `node.name`—This parameter is located in the Node section of the file. Assign a unique name for each node in the cluster.
   - `network.host`—This parameter needs to be set to bind the cluster to an external IP address. We recommend using 0.0.0.0 and enabling authentication using X-Pack security.
3. Optional. If you want to integrate more than 64 source systems with VDX Analytics, add the following parameter to the `Elasticsearch.yml` file on each node in the cluster, and then restart the service:
   - `http.max_initial_line_length: 128kb`

Next Steps

- "Allocate Memory " on page 18

Allocate Memory

The amount of memory allocated to Elasticsearch is set automatically when you install it. The memory allocation is set using heap space values. Use this procedure to adjust the heap space values to the recommended levels for VDX Analytics.

Before you Begin

Ensure that you have Notepad++ to edit configuration files. You can also use Notepad running in administrator mode.

Whether you are deploying a single node or an Elasticsearch cluster, you need to determine the amount of heap space to assign.

- **Single nodes or data nodes**—Use the following formula:
  Total (Total Windows memory - 4 GB for Windows processes) /2. Round down the total. For example, if the server has 40 GB of memory, the calculation is 40-4 =36. 36/2 = 18. The heap space required is 18 GB.
- **Master node**—No calculation is needed. This node requires 4 GB.

1. Open the `jvm.options` file on each node.
   The file is located where you installed Elasticsearch. The default location is:
   `Program Files\Elasticsearch\elasticsearch\config\jvm.options.d\jvm.options`.
2. Edit the following parameters on each node:
   - `XmsXXg`—This parameter represents the initial size of total heap space. For example, the default value is 2 GB and is represented as `# -Xms2g`.
   - `XmxXXg`—This parameter represents the maximum size of total heap space. For example, the default value is 2 GB and is represented as `# -Xmx2g`.
   Allocate 4GB to the master node, and allocate the amount you calculated for the data nodes. Ensure that you set the same value for both parameters.
3. After you have changed the values, save the file.
4. From **Services**, stop and restart the `Elasticsearch` service.

Next Steps

If you are deploying VDX Analytics with an Elasticsearch cluster, proceed to "Test the Configuration" on page 19.

If you are deploying VDX Analytics with a single Elasticsearch node, no further steps are needed.

Test the Configuration

Use this procedure to verify that you can connect to each node in the cluster, and that the cluster is properly configured.

1. Open a browser and ensure that you can connect to each node in the cluster at `http://<IP_Address>:9200/_nodes`.
   The first line of this file reports the number of nodes and cluster name.
2. Verify that the node name and the cluster name are set. For example:
   `{"_nodes":{"total":5,"successful":5,"failed":0},"cluster_name":"My-cluster","nodes":`

Next Steps

Configure the Index Template

Use this procedure to create a template for the Elasticsearch index.

Before you Begin

Ensure that you have Curl to run the scripts in this procedure. It is available at the following URL:
https://curl.haxx.se/download.html

1. Open up a Windows administrator command prompt and change the folder to `c:\curl\bin`.
2. Run the following four commands and ensure that after each one, you receive the acknowledgement: `true`.

```
curl -XPUT "localhost:9200/_template/template_async_
alerts_?pretty" -H "Content-Type: application/json" -d "{\"index_
patterns\":[\"savisioniq_alerts_*\"], \"settings\": {\"index\":{
\"number_of_shards\": 5, \"number_of_replicas\": 1,\"translog\":
{\"durability\": \"async\"}}}}"


curl -XPUT "localhost:9200/_template/template_async_
components_?pretty" -H "Content-Type: application/json" -d "
{\"index_patterns\":[\"savisioniq_components_*\"], \"settings\":
{\"index\":{ \"number_of_shards\": 5, \"number_of_replicas\":
1,\"translog\":{\"durability\": \"async\"}}}}"


curl -XPUT "localhost:9200/_template/template_async_
relationships_?pretty" -H "Content-Type: application/json" -d "
{\"index_patterns\":[\"savisioniq_component_relationships_*\"],
\"settings\": {\"index\":{ \"number_of_shards\": 5, \"number_of_
replicas\": 1,\"translog\":{\"durability\": \"async\"}}}}"


curl -XPUT "localhost:9200/_template/template_async_
incidents_?pretty" -H "Content-Type: application/json" -d "
{\"index_patterns\":[\"savisioniq_incidents_*\"], \"settings\":
{\"index\":{ \"number_of_shards\": 5, \"number_of_replicas\":
1,\"translog\":{\"durability\": \"async\"}}}}"
```

Next Steps

Install or Upgrade Vantage DX Analytics

Use the procedures in this section to install or upgrade VDX Analytics.

Before you Begin

- Ensure that your system meets all the prerequisites listed in "Planning " on page 8.
- Download the installation package from our website at: https://www.martellotech.com/downloads

The installation package contains the following installers:

- Vantage DX Analytics-3.11.exe
- Vantage DX Analytics Agent-3.11.exe
- Elasticsearch-7.17.0.exe

After you download the installation package, complete the following tasks:

Task	Description
Choose one of the following options: • "Install VDX Analytics" on page 22 • "Upgrade VDX Analytics" on page 23	Install a new instance of VDX Analytics, or upgrade an existing instance.
"Configure Connections" on page 25	Use this procedure only if you are deploying VDX Analytics in an Elasticsearch cluster. This procedure sets the connection strings in VDX Analytics with the IP addresses of the data nodes in the Elasticsearch cluster.

Task	Description
"Install Remote Agents" on page 26	Optional. Install a remote agent only if the source system is not accessible from the VDX Analytics web server.
"Add a License Key" on page 26	Activate the license.

Install VDX Analytics

Use the following procedure to install VDX Analytics. You must be a domain user with local administration privileges to complete this procedure.

If you are deploying VDX Analytics with an Elasticsearch cluster, perform this procedure on the master node.

Before you Begin

VDX Analytics needs to access information that is stored on the SQL server. You can use a full SQL server, or you can use SQL Server Express. Before you begin, ensure that you have the server instance and the credentials for the SQL server that is used to store this metadata.

- For an SQL server, the default instance name is `<SQL Server host name or IP Address>`. The non-default instance name is `<SQL Server host name or IP Address>\<instance name>`.
- For SQL Server Express, the default instance name is `<SQL Server host name or IP Address>\SQLExpress`. The non-default instance name is `<SQL Server host name or IP Address>\<instance name>`.

If you do not have a full SQL server, the VDX Analytics installer provides a link to SQL Server Express. If you are using this option, ensure that you record the connection string that SQL Express generates; you will need this connection string during the installation process. The connection string uses the following format: `<machine_name>\SQLExpress`. Ensure that Windows updates are installed and there are no pending reboots.

1. Right-click the `Vantage DX Analytics-3.11.0.exe` file and select **Run As Administrator**.
2. Click **Next** at the welcome screen.
3. Click on **I accept the agreement** and then click **Next**.
4. Optional. Select **Enable Google Analytics** to help us understand how we can improve the application. Click **Next**.
5. On the **Connect to SQL Server** page, enter the SQL server instance as well as the credentials of a user that has rights to create the database.

> **Note:**
> If you do not have a SQL Server, you can click on **Install SQL**

Server Express to install the express version of SQL Server. This option is useful if you have a small environment or would like to use VDX Analytics for demonstration or evaluation purposes. When you choose this option, you can de-select the following features: SQL Server Replication and SQL Client Connectivity SDK.

6. Click **Verify**. When the credentials are verified, click **Next**.

7. Select the destination where you want to install VDX Analytics and click **Next**.

8. Optional. Click on **Create a desktop shortcut** and click **Next**.

9. If Elasticsearch is not already installed on this server, the Elasticsearch installer launches. When the Welcome to the Elasticsearch Setup Wizard displays, click **Next** .

10. Click **I accept the agreement** and click **Next**.

11. Select the destination where you want to install Elasticsearch and click **Next**.

12. When the Elasticsearch installation is complete, click **Finish**.
VDX Analytics continues its installation. It verifies the IIS Roles and Features and adds any requirements that are missing.

13. When the installation is complete, click **Finish**.
VDX Analytics launches.

Next Steps

To complete the installation, perform the following procedures:

- Optional. Perform the procedure "Install Remote Agents" on page 26 only if the source system is not accessible from the VDX Analytics web server.
- To activate the installation, perform the procedure "Add a License Key" on page 26

Upgrade VDX Analytics

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

- "Understand the Upgrade Process" on page 23
- "Upgrade the Software" on page 24

Understand the Upgrade Process

The VDX Analytics installer supports an in-place upgrade. If you made manual changes to the `web.config` file, those changes are preserved during an in-place upgrade. If you choose to uninstall and reinstall the software, instead of performing an in-place upgrade, any manual changes that you made in the `web.config` file are lost when you install the new version. In addition, uninstalling and reinstalling the software will not remove any data from the SQL server and Elasticsearch data stores.

This release of VDX Analytics requires Elasticsearch version 7.17.0. The VDX Analytics installer package contains an installer for Elasticsearch that upgrades an Elasticsearch node. If Elasticsearch is installed on the same machine as VDX Analytics, the VDX Analytics installer executes the Elasticsearch installer automatically. In the case of an Elasticsearch cluster, you must execute the Elasticsearch installer on all Elasticsearch nodes before you install VDX Analytics.

When you are upgrading to release 3.11, VDX Analytics re-indexes all savisioniq_* indices in Elasticsearch after the installation. This process can take several hours. During that time, the indices being processed are not accessible and no data from those indices is visible in VDX Analytics.

Upgrade the Software

Use the following procedure to upgrade VDX Analytics.

Before you Begin

- Backup any PowerShell scripts from the PSScripts folder.
- Stop the app pool. The app pool automatically restarts after the upgrade is complete.
- View the current binding information on the VDX Analytics website, making note of ports, SSL certificates, and host name information. You may need to restore some of these settings after the upgrade.
- Ensure that you have upgraded the .NET version to 4.7.2.

1. Right-click the `Vantage DX Analytics-3.11.exe` file and select **Run As Administrator**.
2. Click **Next** at the welcome screen.
3. Click on **I accept the agreement** and then click **Next**.
4. Optional. Select **Enable Google Analytics** to help us understand how we can improve the application. Click **Next**.
5. Select the destination where you want to install VDX Analytics and click **Next**.
6. Optional. Click on **Create a desktop shortcut** and click **Next**.
   VDX Analytics continues its installation. It verifies the IIS Roles and Features and adds any requirements that are missing.
7. When the installation is complete, click **Finish**.
   VDX Analytics launches.

Next Steps

To complete the upgrade, perform the following procedures:

- Optional. Perform the procedure "Install Remote Agents" on page 26 only if the source system is not accessible from the VDX Analytics web server.
- To activate the installation, perform the procedure "Add a License Key" on page 26
- If you previously configured an integration with Microsoft Teams CQD, select **Settings > Integrations** and re-save the integration.

Configure Connections

Perform this procedure only if you are deploying VDX Analytics with an Elasticsearch cluster. This procedure explains how to configure the connections between nodes in the cluster. Perform this procedure on the server where VDX Analytics is installed.

Before you Begin

Ensure that you have Notepad++ to edit configuration files. You can also use Notepad running in administrator mode.

1. Open the `web.config` file.
   If this is a new installation, the default location for this file is
   `%programfiles%/Martello/Martello iQ/web.config`

   If this is an upgrade, the default location depends on the version you installed initially. For upgrades from release 2.10, the default location is
   `%programfiles%/Savision/Savision iQ/web.config`. For upgrades from release 2.11, the default location is `%programfiles%/Martello/Martello iQ/web.config`.

2. In the `connectionStrings` section, edit the "defaultElasticSearchConnection" settings to include the IP addresses of the data nodes as shown in the following example:

   ```
   <connectionStrings>
   <clear />
   <add name="defaultSqlConnection" connectionString="Data Source=SV-
   IQ-LG\SQLEXPRESS; Initial Catalog=Savision_iQ; Integrated
   Security=true; Connection Timeout=30"
   providerName="System.Data.SqlClient" />
   <add name="defaultElasticSearchConnection"
   connectionString=
   "Nodes=http://10.20.6.31:9200,http://10.20.6.33:9200" />
   <add name="elmah" connectionString="data
   source=~/Logs/ErrorLog.db" />
   </connectionStrings>
   ```

   If you have enabled authentication using X-Pack, ensure that you include the username and password when you edit the connection strings, as shown in the following example:

   ```
   <add name="defaultElasticSearchConnection"
   connectionString=
   "Nodes=http://10.20.6.31:9200,http://10.20.6.33:9200;
   Username=username; Password=secret" />
   ```

Install Remote Agents

When you install VDX Analytics, it will install an agent locally on the server. For most installations the local agent is all that is needed. In some cases, you may need to install a remote agent to access certain systems you want VDX Analytics to integrate with. For example, you need to install a remote agent when the source system is not accessible from the VDX Analytics web server.

The remote agent installs as a Windows service.

1. From the remote computer, open your browser and log into VDX Analytics.
2. From the main menu, select **Settings >Agents**.
3. Click the **Download Agent** icon in the bottom corner of the page.
   The AgentInstaller.zip file downloads.
4. Extract the files.
   There are two files: `Martello Vantage DX Analytics Agent-<version>.exe` and `Setup.cmd`.
5. Choose one of the following options:
   - Double-click the `Setup.cmd` to launch the installer with the VDX Analytics web server URL pre-populated.
   - Right-click on `Martello Vantage DX Analytics Agent-<version>.exe` and select **Run As Administrator**.
6. Click **Next** on the welcome screen.
7. Select **I accept the agreement** and click **Next**.
8. If you did not use the `Setup.cmd` file, enter the URL of the VDX Analytics web server.
9. Enter your VDX Analytics Administrator credentials and click **Verify**.
10. Enter the destination where you want to install the agent and click **Next**.
11. Click **Finish** when the installation is complete.
    After a few moments, the remote agent is listed as an available agent in VDX Analytics.

Add a License Key

After you purchase a license, the support team sends you an email with the license key attached in a text file. Use this procedure to activate the license.

1. From the main menu, select **Settings**.
2. Click the **Licensing** tab.
3. Click the **Add License** button.
4. Paste your license key in the dialog box and click **Activate**.

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 27
- "Add an Integration" on page 27

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 27.

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

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://support.martellotech.com/knowledgeBase/9521026

Configure the following properties when you integrate AWS 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.
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	A user in the account
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.

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://support.martellotech.com/knowledgeBase/9443244

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.

Property	Description
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://support.martellotech.com/knowledgeBase/9362697

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.
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.

Property	Description
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.

BMC Remedy IT Service Management Suite

Configure the following properties when you integrate BMC Remedy 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 to Mid-Tier Server	The server that facilitates the web console and the REST API.

Property	Description
URL to Action Request (AR) System API	The server that facilitates the web services. You must enable the API in your BMC Remedy environment.
AR Server Name	Find the name using the registry key `HKLM\SOFTWARE\Remedy\ARServer\ServerNameList`
Dataset ID	The BMC Remedy environment includes multiple datasets. To collect information from more than one dataset, enter the IDs separated by a comma.
Username	A user in the account
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.

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.
URL	The URL to the rest API endpoint. Port 8081 is the default.
Username	A user in the account
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	A user in the account
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.

Cisco Prime

Configure the following properties when you integrate Cisco Prime 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.
URL	—
Username	A user in the account
Password	The password for the account.
API Version	Use the highest version available for your Cisco Prime version.
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.

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	A user in the account.
Password	The password for the user.
Response URL	URL that can be used to navigate from Derdack Enterprise Alert to VDX Analytics.

Email Notifications

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.
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.

Icinga2

Configure the following properties when you integrate Icinga2 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 server Icinga2 is installed on.
Port	The port to access the server.
Secure Connection (HTTPS)	Select the checkbox to use HTTPS.
Username	A user in the account
Password	The password for the account.

Property	Description
Base URL	The URL used to open the Icinga2 web console from VDX Analytics.
Host URL	URL used to retrieve the data.
Service URL	URL that is used to navigate from VDX Analytics to Icinga2 from a service component.
Host Group URL	URL that is used to navigate from VDX Analytics to Icinga2 from a host component.
Service Group URL	URL that is used to navigate from VDX Analytics to Icinga2 from a service group component.
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.

Ivanti Service Management

Configure the following properties when you integrate Ivanti Service Management 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	Include the port access to the instance, typically 80 or 443.
Username	A user in the account.
Password	The password for the account.
On-Premises	Optional.
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.

Jira Software

Configure the following properties when you integrate Jira Software 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	The default port is 8080.
Type	VDX Analytics supports Jira on-premises.
Username	A user in the account
Password	The password for the account.
Operation Interval	How often incidents are collected. The default is 120 seconds.

Martello API

This entry is not an active integration. It uses an API endpoint on the Elasticsearch server to push data into VDX Analytics. This approach allows you to use the same filters that are used for the data from other integrations.

Configure the following properties when you integrate the Martello API with VDX Analytics:

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.
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.

For more information about the API, refer to the *Vantage DX Analytics REST API Guide*, available on the Martello documentation site at the following URL:

https://martellotech.com/documentation/vantage-dx/

> **Note:** This is not an active integration. This approach uses an API endpoint on the Elasticsearch server to push data into VDX Analytics.

Martello Vantage DX Monitoring

If you are integrating Martello Vantage DX Monitoring 2.1 with VDX Analytics, ensure that you enable the Vantage DX Monitoring API using the instructions provided in the following Knowledge Base article:

https://help.gizmo.gsx.com/knowledge-base/how-to/how-to-enable-the-gizmo-api/

If you are using Martello Vantage DX Monitoring 2.2 or higher, you do not need to enable the API; it is enabled by default.

Configure the following properties when you integrate Vantage DX Monitoring 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 URL	URL of the Vantage DX Monitoring instance API. For Vantage DX Monitoring 2.1 integrations, an example URL is `http://<servername>:8080/api/v1/robotmanager`. For Vantage DX Monitoring 2.2 and higher, an example URL is `http://<servername>/api/v1/robotmanager`.
<Domain\>User Name	Administrative credentials for the account.
Password	The password for the account.
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.

Property	Description
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Microsoft Teams Call Quality Dashboard

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

Property	Description
Set-up	
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
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.

Property	Description
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.
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. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide 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.
Privacy Protection	
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.

Property	Description
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.

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.
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	A SCOM username.
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.

Property	Description
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 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.

After you register the application, you must grant consent for 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. For information about how to perform these steps, see the following Knowledge Base article:

https://support.martellotech.com/knowledgeBase/15513875

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.

Property	Description
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.
Client ID	The Application (Client) ID from the above Azure Application registration.
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.
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.

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 48: VDX Analytics pulls data from Nagios using the JSON API shipped with Nagios since release 4.0.7.
- "Martello API Mode" on page 49: 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	Select a PowerShell script from the drop-down menu. Scripts are available in the menu after you copy them to the **VDX Analytics > PSScripts** folder.

Provance

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

https://support.martellotech.com/knowledgeBase/15220588

Configure the following properties when you integrate Provance 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	The URL of the Provance instance.
Tenant ID	The Azure AD tenant where the Provance application is registered. Registering the application allows it to connect to Dynamics 365.
Application ID	Also known as the client ID, this is the ID of the Dynamics 365 application.
Application Secret	The secret of the Dynamics 365 application.
Operation Interval	How often incidents are collected. The default is 120 seconds.

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.

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.
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.
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 Martello iQ 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.Martello iQ role and check the Access Control List (ACL) settings. See "Martello iQ ServiceNow Roles and Permissions" on page 1 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.
Username	Enter the credentials for the user you created.
Password	The password for the user.
Fields for incident creation	Enable or disable retrieval of the following data: - Assignment Group - Assigned To 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.

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	Administrative credentials for the account.
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.

Property	Description
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	The user of the account.
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.

TOPdesk

Configure the following properties when you integrate TOPdesk 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.
Username	Choose one of the following options for authentication: • Use an operator account that has privileges to access the API. The account cannot be an administrator account. • Use an application password. Martello recommends that you use an application password for better performance.

Property	Description
Password	The password for the Operator account or the application password. If you are using an application password, ensure that you select **Using application-based authentication**.
Mandatory Fields for Incident Creation	Use the drop-down list to select the mandatory fields to include when VDX Analytics creates an incident in TOPdesk.
Using application-based authentication	Select the checkbox if you are using an application password instead of an operator account.
Load asset data	Select the checkbox to enable.
Cache asset data	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.

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.
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	A user in the account
Password	The password for the account.
Use Single Sign-on (SSO)	Optional.
SSO Endpoint override	Configure the URL to the SSO endpoint.

Property	Description
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.
Use SQL Authentication	Optional.
User	Enter a user that has read permissions on 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	A user in the account
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