



VANTAGE DX DIAGNOSTICS

ADMINISTRATION GUIDE - FOR SERVICE PROVIDERS

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.

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, GSX, Martello Technologies, 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.

© Copyright 2024, Martello Technologies Corporation
All rights reserved

Administration Guide - For Service Providers
Release 3.15 - February 26, 2024

Contents

CHAPTER 1

Introduction	5
Document Purpose and Intended Audience	5
Revision History	5

CHAPTER 2

About Vantage DX Diagnostics	6
------------------------------------	---

CHAPTER 3

Requirements	7
Machine	7
Network	7

CHAPTER 4

About the Interface	9
Home	9
Manage	10
Network Path Diagrams	10

CHAPTER 5

Getting Started	14
-----------------------	----

CHAPTER 6

Manage Sites	15
Add Target Endpoints	17
Create a Site Group	18
Configure the Vantage DX Analytics Integration	20
Create a Site	21
Manage Site Groups	22
Manage Sites	23

CHAPTER 7

Install the Probes	24
Install a Windows Probe	24

Install a Probe Using Deployment Software	25
Configure a Windows Probe	26
Configure a Software Deployed Probe	27

CHAPTER 8

View Network Path Data	29
View Data for a Site Group or Site	29



Introduction

Document Purpose and Intended Audience

This document provides information about how to configure and use Vantage DX Diagnostics to test the network paths between your physical office sites and target endpoints, such as Microsoft Teams.

This guide is intended for use by administrators.

Revision History

Document Date	Description
February 26, 2024	Vantage DX Diagnostics Administration Guide - For Service Providers Release 3.15



About Vantage DX Diagnostics

Vantage DX Diagnostics is an application that tests the network paths between physical office sites and target endpoints that you want to monitor, such as Microsoft Teams or SharePoint. It consists of a software probe and a web-based interface:

- **Probe:** The software probe installs on a Windows machine at each of your business sites, or on the machine of a remote user. The probe monitors and reports on the flow of data along the network path between the site where it is installed and the target endpoint. It uses My Traceroute (MTR)—which is a combination of traceroute and ping—to identify the segment of the network where errors occur. For example, if a user or a location is experiencing high round-trip time (RTT), jitter, or packet loss, you can deploy a probe to determine the source of the problem. The test results will show whether the issue is occurring in the corporate network, the user's home network, the ISP's network, or the Microsoft network.
- **Web-based interface:** The Vantage DX Diagnostics interface provides a visual representation of the quality of the connection at each hop in a network path. This information is shown on network path diagrams to help you quickly understand where issues are occurring along the network path, how your end users' experiences are affected, and which networks are responsible for the issues. The interface also provides information about packet loss rate, round-trip latency, and jitter average for each network path.



Requirements

The following section describes the system requirements for installing a Vantage DX Diagnostics probe.

- ["Machine" on page 7](#)
- ["Network" on page 7](#)

Machine

Ensure that the machine where you install the probe meets the following requirements:

- Windows 10 (64-bit) operating system
- Minimum 2 GB RAM
- 70 MB disk space

Network

Ensure that the firewall at the site where the probe is installed meets the following requirements:

- Port 443 is open; the probes need to connect to the Vantage DX Diagnostics endpoint on this port.

- The firewall must allow ICMP for outbound and inbound communications. Refer to the tables below for the inbound and outbound ICMP requirements.
- The `https://<instancename>.vantage-dx.com/npv-ui` endpoint must be accessible.

Table 1: Inbound ICMP Requirements

Response (Inbound to the Probe)	Source
Type: 0 (Echo Reply)	Any
Type: 11 (TTL Exceeded)	Any

Table 2: Outbound ICMP Requirements

Request	Source	Destination
Type: 8 (Echo Request)	Probe	Any

You may need to configure additional firewall rules for inbound ICMP if you have configured NAT.

We recommend that you run the following connectivity tests in PowerShell to ensure connectivity before you install and configure the probes:

- `Test-NetConnection -computername <company_name>.vantage-dx.com -port 443`
- `tracert world.tr.teams.microsoft.com`
- `ping <endpoint FQDN>`

About the Interface

The Vantage DX Diagnostics interface provides you with a global view of network path test results between your sites and target endpoints, such as Microsoft Teams. You can use the interface to see detailed information about each network path.

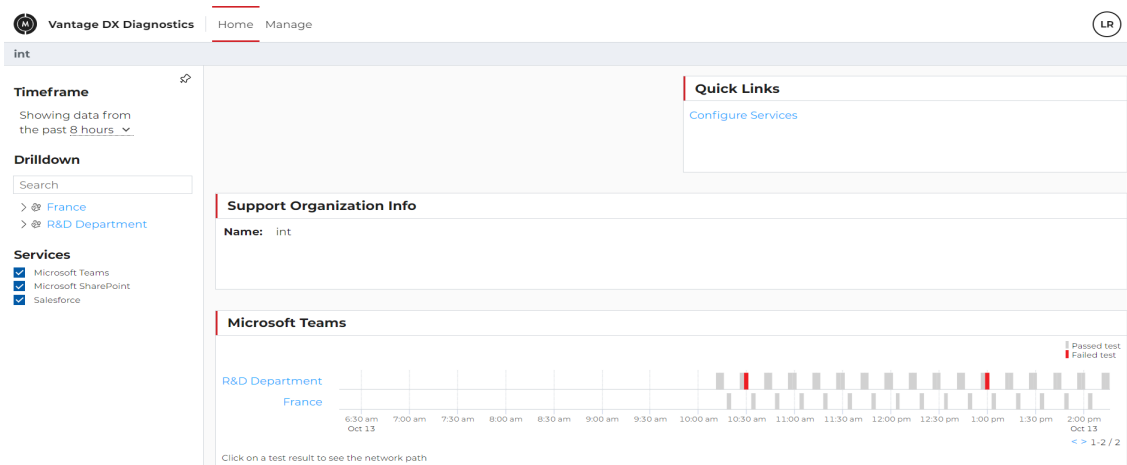
The following sections describe the pages in the interface and the functionality that each one provides:

- ["Home" on page 9](#)
- ["Manage" on page 10](#)
- ["Network Path Diagrams" on page 10](#)

Home

The Home page is displayed when you log into Vantage DX Diagnostics. The following image shows an example of the Home page.

Figure 1: Home Page Example



The **Network Testing Summary** panel consists of a bar graph that illustrates the network path test results between the target endpoint and the sites contained within each site group. Each configured endpoint has its own corresponding

Network Testing Summary panel. From the panel you can access more detailed data about the tests by doing the following:

- Select a site group link to display the test results for each site within that group.
- Click on a specific test result bar to display a visualization of the network path test for the site group or site. See ["View Data for a Site Group or Site" on page 29](#).

Use the following options to filter the data displayed in the Network Testing Summary panel:

- **Timeframe**—Display data from the past 8 hours, 24 hours, 3 days, or 7 days.
- **Drilldown**—Click on a site group to display the test summary for all of the sites within the group. Click on a site to display the test summary for only the selected site. The selected site or site group is displayed in the Network Testing Summary panel. You can also find a site or a site group by typing its name directly in the search bar.
- **Services**—Select the endpoints that you want to display on the Home page. Each configured endpoint has a corresponding Network Testing Summary panel.

Manage

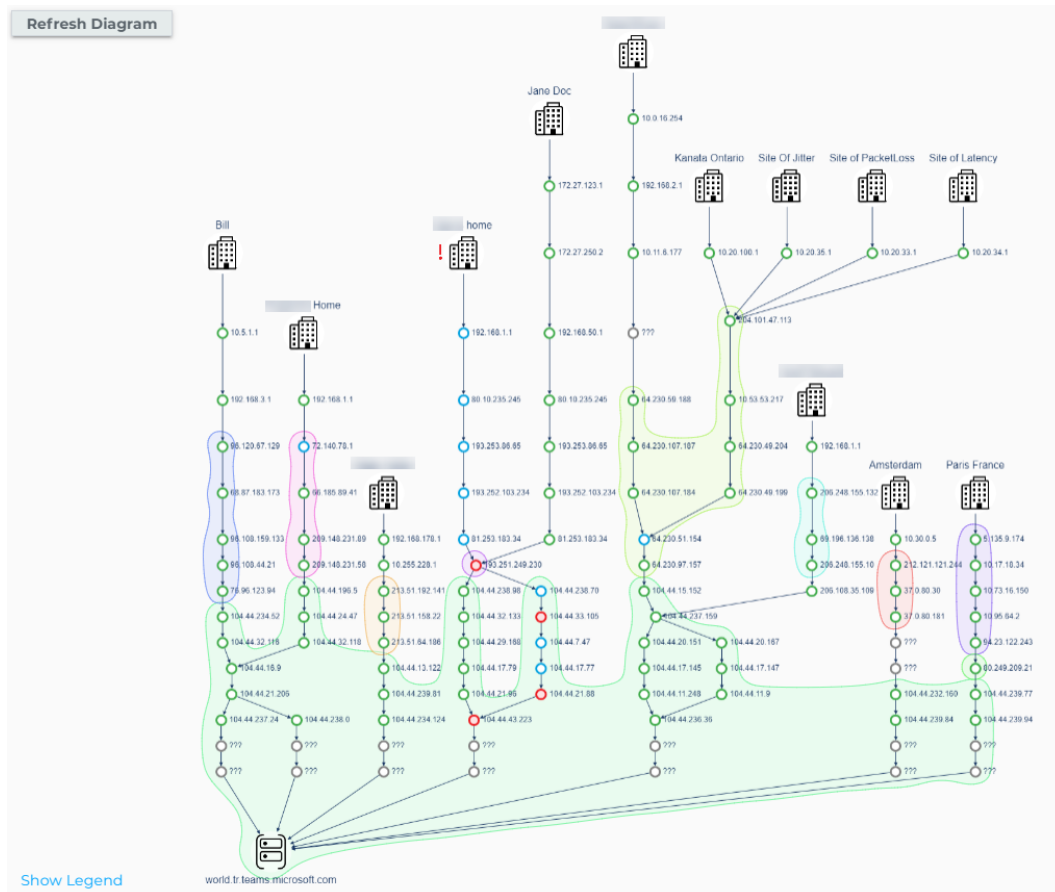
The Manage menu provides access to the Application Management page. From this page you can perform the following tasks:

- Add target endpoints
 - Configure the default endpoints to monitor. See ["Add Target Endpoints" on page 17](#).
- Create and manage site groups
 - Create site groups to represent the customers that your organization provides supports. See ["Create a Site Group" on page 18](#).
 - View and edit the details of the site groups in your organization. See ["Manage Site Groups" on page 22](#).
- Create and manage sites
 - Create individual sites to represent the physical office locations within each customer site group that need to be monitored. See ["Create a Site" on page 21](#).
 - View and edit the details of the sites contained within your site groups. See ["Manage Sites" on page 23](#).

Network Path Diagrams

The Network Path view provides a visualization of the network paths from each site to the Microsoft Teams endpoint or custom target endpoint. These visualizations are diagrams that identify each hop in the network path and use color-coding to indicate the health status of each hop.

The following diagram shows an example of network paths for multiple sites.

Figure 2: Network Path Diagram Example

In addition to the status, the diagram also shows the owner of each hop in the network. Click the **Show Legend** link to display the statuses in the diagram. The hop statuses are:

- Grey—Hop is not responding to network testing. This occurs when a server refuses to recognize ICMP requests.
- Green—Good hop. The network test results do not exceed the established thresholds.
- Blue—Hop is responding poorly to network testing. This can occur for a couple of reasons. Some servers deprioritize ICMP packets, so the server response time exceeds the threshold. A blue status may also be displayed for a hop when a threshold is exceeded but the subsequent hops have a green status.
- Red—Hop at which bad test results may have started. The threshold was exceeded for at least one of the following tests:
 - packet loss (5%)
 - round trip time (200 milliseconds)
 - jitter (40 milliseconds)

The hops thereafter may have poor test results, but may appear with a green status because they are not considered to be the problem hops.

Using the following example, we demonstrate how hop statuses are determined.

Figure 3: Hop Status Example

- The packet loss thresholds for the first two hops are exceeded, but the third to the ninth hop are good. As a result, the statuses for the first two hops are blue. This indicates that there may be a problem at these hops, but subsequent hops appear to be unaffected, so it is assumed that the problem is likely packet loss due to the servers at these hop de-prioritizing the ICMP requests.
- The packet loss for the 10th hop is 10%, and every hop after, including the smtp.office365.com has packet loss equal to or greater than 5%. As a result, this hop is considered to be the problem hop and is given a status of red.

- Although the subsequent hops (hops 11, 12 and 13), do experience packet loss, they are still given a status of green because they are not considered to be the problem hop.
- The grey hops have packet loss 100%. The servers at these hops refuse to recognize the network test ICMP requests.



Note: Keep in mind that what the algorithm considers a problem hop, versus what might actually be a problem hop, can be different. When investigating hops for issues, also refer to the Hop Breakdown section of the Path Analysis panel for more details.

The **Path Analysis** panel to the right of the diagram provides a map of MS server entry points (for MS Teams service only), plus detailed information about each network path that appears in the diagram. See ["View Data for a Site Group or Site" on page 29](#).

You can filter and group the elements on the diagram using the options in the sidebar to the left of the diagram. The options include:

- **Test Type**—Displays site-to-service network paths by service. This option allows you switch between service endpoints to easily determine which sites are having issues with a specific service. Alternatively, you can view all service endpoints to view all of the site-to-service network paths, and all of the correlations between those network paths.
- **Date**—Display results for a selected date. The default is the current date.
- **Time of day**—Display results for a selected time, in 15-minute increments.
- **Site**—Display results for selected sites. The top 10 sites with recent test results are displayed by default. These sites are organized in the following order: sites with failed tests, sites with passed tests, and sites without test results. If you have many sites, or the site you want to view is not in the top 10 sites, type the site name in the search bar to find the specific site.

You can also click **Select All**, to display the path visualization for all sites. Use the **Deselect All** button to remove any selected sites from the path visualization.

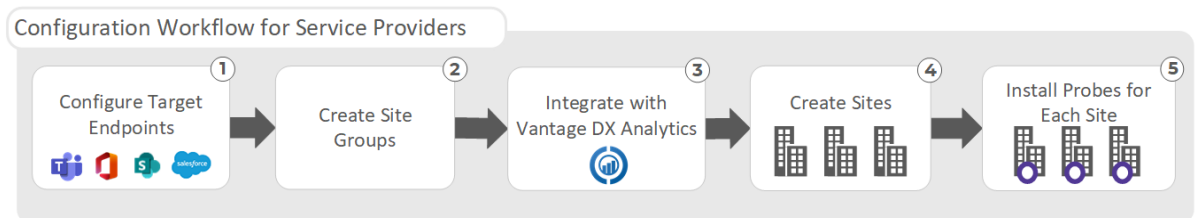
Optionally, you can set the **Auto-select sites with results** option to **On** to only display the sites that have network path test results in the diagram.

- **Grouping**—Click the **Grouping** link to display the grouping options:
 - **Group by network hop**—Select one of none, by network, or by network owner.
 - **Show network owner**—Set to **On** to highlight each network owner in the diagram in a different color. You can also select which networks to highlight in the diagram.

Getting Started

Vantage DX Diagnostics is configured in the following order.

Figure 4: Configuration Workflow for Service Providers



1. Add any required target endpoints to monitor for the Support Organization. See ["Add Target Endpoints" on page 17](#).
2. Create site groups that represent each of the companies you support.
 - To understand the site configuration within a service provider scenario, see ["Manage Sites" on page 15](#).
 - To add a site group to your service provider organization, see ["Create a Site Group" on page 18](#).
3. For each site group an integration is configured for Vantage DX Analytics. This integration allows the Vantage DX Diagnostics components and alerts to be viewed and reported on in VDX Analytics. See ["Configure the Vantage DX Analytics Integration" on page 20](#).
4. Within each site group, add sites that represent the customer's physical office locations. See ["Create a Site" on page 21](#).
5. For each site that you create in Vantage DX Diagnostics, you need to install and configure probe software. See ["Install the Probes" on page 24](#).

After your sites are configured and collecting data, you can view the network path data. See ["View Network Path Data" on page 29](#).

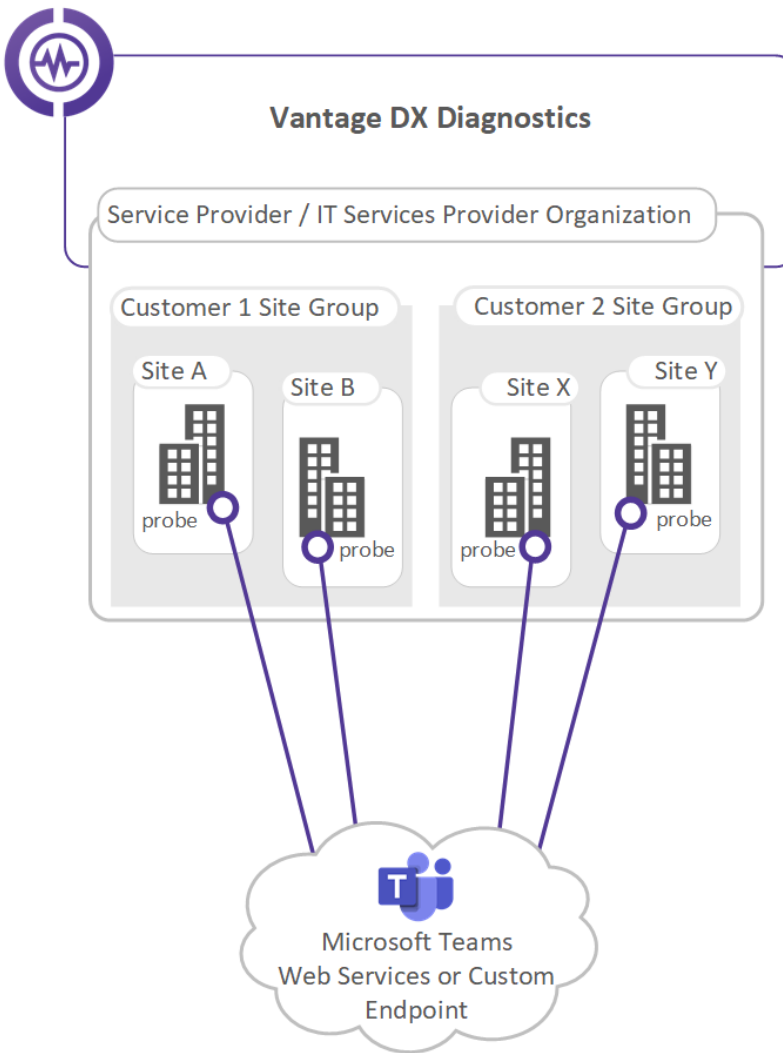


Manage Sites

Vantage DX Diagnostics deployments include the following concepts:

- **Support Organization**—The top level entity, which is the service provider or IT services organization. From the support organization, the target endpoints to monitor are configured. The endpoints are enabled and further configured for each site group.
- **Site Group**—Site groups function as theoretical containers for sites. A site group is comparable to a customer.
- **Site**—A site represents a physical office location. Each site must have probe software installed on a computer at the physical location in order to test the connection to the target endpoints and collect data. Vantage DX Diagnostics supports up to 400 sites (probes). Sites are created within a site group.

The following diagram demonstrates the site configuration for a service provider deployment. The service provider is at the support organization level, and each customer is represented by a site group. Within each customer site group are sites that represent the customer's office locations. At each site location, probe software is installed that communicates with target endpoints to gather network path data between the site and the monitored endpoints.

Figure 5: Service Provider Deployments

Use the tasks listed in the table below to manage the support organization, site groups, and sites..

Task	Description
"Add Target Endpoints" on page 17	Complete this task to configure the target endpoints to monitor.
"Create a Site Group" on page 18	Complete this task to create a site group.
"Configure the Vantage DX Analytics Integration" on page 20	Complete this task to create an integration between the site group in Vantage DX Diagnostics and Vantage DX Analytics.
"Create a Site" on page 21	Complete this task to create a site.

Task	Description
"Manage Site Groups" on page 22	Search for, sort and filter site groups within a service provider deployment. View site group details and edit site group information, or delete a site group.
"Manage Sites" on page 23	Search for, sort and filter sites. View site details and edit site information, install probe software for the site, or delete a site.

Add Target Endpoints

At the support organization level, add the target endpoints that you want to monitor.

The Microsoft Teams endpoint is included by default for your support organization. You can also monitor custom endpoints, such as Microsoft 365 SharePoint, O365 Outlook Exchange Server, or Salesforce. When you configure a custom endpoint, it is available to all of the site groups within your support organization. You can further customize it for each site group.

To add custom endpoints to your support organization, perform the following steps:

Before you Begin

- You must know the target endpoint URL or IP address.
- The provided FQDN or IP address must be able to respond to ICMP ping requests.

1. Click **Manage** to access the Application Management page, then click **Support Organization**.
2. On the Manage Support Organization page, beside the Services heading, click the **Add** link and set the following options.
 - **Name**—Type a descriptive name for the target endpoint.
 - **Default Target**—The URL/FQDN or IP address for the endpoint. This default target can be further customized per site group.
 - **Frequency**—Specify how often to check the network path for the endpoint. Select one of:
 - Every 5 minutes
 - Every 15 minutes
 - Every 30 minutes
3. Click **Save**.

Next Step

- ["Create a Site Group" on page 18.](#)



Create a Site Group

Use this procedure to create site groups. Each site group represents a customer; use site groups to organize one or more sites under the same customer. Site groups allow you to monitor and have a global view of your customer sites.

To create a site group, complete the following steps.

Before you Begin

- The endpoints to be monitored must already be configured at the Support Organization level.
1. Click **Manage** to access the Application Management page, then click **Site Groups**.
 2. On the **Manage Site Groups** page, click **Create Site Group**.
 3. Provide a **Name** for the site group in the **Create New Site Group** section.
 4. In the **Monitor Services** section toggle the applicable endpoints options to **On**.
 5. Configure the following options for each of the enabled endpoints, then click **Save**:

Option	Description
Target	<p>The monitored endpoint.</p> <p>For Microsoft Teams, select one of the following:</p> <ul style="list-style-type: none"> • Discover Microsoft Teams Server (recommended). This option presents an exact server IP address to which a Microsoft Teams Server can connect. • General Microsoft Teams Server • Custom—Supply the URL <div data-bbox="716 579 1458 989">  <p>Warning: Unless you have been specifically directed by Martello, do not change the Microsoft Teams settings. If you have changed these settings prior to reading this warning, you can reset the values for Target back to "Discover Microsoft Teams Server" and the ToS value to 184.</p> </div> <p>For the other custom endpoints, you can use the default target value configured for the Support Organization, or you can provide a custom endpoint as a URL or IP address. Any changes to the target are applicable to this site group only.</p>
Packet ToS	<p>Use the Priority slider to specify a Type of Service value to define the traffic classification for network data and the associated DSCP value. Alternatively, you can type the ToS value into the text box. The default value is 184.</p>
Protocol	<p>Select the protocol to use:</p> <ul style="list-style-type: none"> • ICMP • TCP • UDP <div data-bbox="716 1545 1458 1749">  <p>Note: Only ICMP is supported for this release of Vantage DX Diagnostics.</p> </div>

Option	Description
Port	Specify the port to use if the protocol is set to TCP or UDP.
Packet Size	Specify the packet size in bytes for data transmission.
Packet Count	The number of pings per hop. Select one of: <ul style="list-style-type: none">• 10• 30• 50

Next Steps

- ["Configure the Vantage DX Analytics Integration" on page 20](#)

Configure the Vantage DX Analytics Integration

Use this procedure to integrate Vantage DX Diagnostics with Vantage DX Analytics.

Every site group in Vantage DX Diagnostics must have an integration configured in Vantage DX Analytics. This integration allow you to view the Vantage DX Diagnostics components and alerts in VDX Analytics.

To configure the integration, complete the following steps.

Before you Begin

- The site group in Vantage DX Diagnostics must already exist.
- A license for the site group in VDX Analytics must be in place.

1. Click **Manage** to access the Application Management page, then click **Site Groups**.
2. On the **Manage Site Groups** page, select the site group for the integration.
3. Next to the Vantage DX Diagnostics Configuration Integration, click **Show**.
4. Make note of the following information, as you will need it to configure the integration in VDX Analytics:
 - Vantage DX Diagnostics URL
 - Site Group GUID
 - Username
 - Password
5. Navigate to VDX Analytics.
6. From the main menu in VDX Analytics select **Settings**.
7. On the **Integrations** tab, click the **Add** button at the bottom of the page.
8. Select **Vantage DX Diagnostics** from the list of integration options.
9. Enter the following information.

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.
Vantage DX Diagnostics URL	The URL for the Vantage DX Diagnostics environment. Copy and paste the URL from the Vantage DX Diagnostics Site Group page.
Site Group GUID	The site group specific GUID. Copy and paste the GUID from the Vantage DX Diagnostics Site Group page.
Username	The generated username for the Vantage DX Diagnostics site group. Copy and paste the username from the Vantage DX Diagnostics Site Group page.
Password	The generated password for the Vantage DX Diagnostics site group. Copy and paste the password from the Vantage DX Diagnostics Site Group page.
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.

10. Click **Save**.

Next Steps

- ["Create a Site" on page 21.](#)

Create a Site

Use this procedure to create a site that represents the physical location of your customer's office, or that represents a remote user.

1. Click **Manage** to access the Application Management page, then click **Sites**.

2. On the **Manage Sites** page, click **Create Site**.
3. On the **Create Site** page, provide the site information, then click **Save**:
 - **Site Group**—Select a **Site Group** from the list.
Optionally, you can create a new site group by selecting **Add Site Group** from the list and providing the support organization, name, and address of the site group.
 - **Name**—Provide a name for the site.
 - For an office, enter the office or building name.
 - For a specific user, enter the user principal name (UPN) of the user.
 - **Address**—Provide the city and country using the format `City, Region, Country`, where `Country` is the 2-letter country code. For example `Ottawa, Ontario, CA`.

Next Steps

- Install and configure a probe for the site; see ["Install a Windows Probe" on page 24](#).

Manage Site Groups

Use this procedure to view and edit details about a site group.

1. Click **Manage > Site Groups** and find the site group that you want to view, using the filter options if required.
 - **Search**—Type in the search box to filter the list of site groups. The results list is filtered as you type. To clear the search, click **Clear Filters**.
 - **Sort By**—Alphabetical
 - **Order By**—Select one of **Ascending** or **Descending**.
2. Click on the site group that you want to view.
The details for the site group are displayed in a panel.
3. Do any of the following:
 - Click the **Edit** link beside the site group name to make changes to the site group name.
 - Click the **Edit** link beside a monitored endpoint to make changes to the settings.



Warning: If you edit the Microsoft Teams endpoint, all of the Teams data previously collected for this site group and associated sites is deleted.

- Click **Go to this Site Group's Dashboard** to view network test summary results for the sites in the site group.
- Click **Add Site** to add a site to the site group.

- Click **Delete** to delete the site group. The site group cannot have any sites associated with it.



Note: If you delete the site group, you must also remove the Vantage DX Diagnostics integration in Vantage DX Analytics.

From the site list table, you can search for a site by typing a search term in the search bar. You can also sort the list by clicking on the column headers. By default, the list is sorted by Site Name.

Manage Sites

Use the following procedure to view and edit sites.

1. Click **Manage > Sites** and find the site that you want to view, using the filter options if required.
 - **Search**—Type in the search box to filter the list of site groups. The results list is filtered as you type. To clear the search, click **Clear Filters**.
 - **Sort By**—Alphabetical
 - **Order By**—Select one of **Ascending** or **Descending**.
 - **Site Group**—Visible to admin users only. Select a site group from the list to display only those sites in the group.
2. Click on the site that you want to view.
The details for the site are displayed in a panel.
3. Do any of the following:
 - Click the **Edit** link beside the site name to make changes to the site name.
 - Click the **Edit** link beside the site address to make changes to the address.
 - Click **Go to this Site's Dashboard** to view network test summary results for the site.
 - Click the site group link to view the site's site group.
 - Click **Delete** to delete the site.

Install the Probes

A probe is the piece of software that monitors and reports on the flow of data along the network path between a site and the target endpoint, such as Microsoft Teams. A probe must be installed for each configured site. Each site can have only one probe installed.

Complete the following tasks for each site that you configure:

Task	Description
Choose one of the following options: <ul style="list-style-type: none"> • "Install a Windows Probe" on page 24 • "Install a Probe Using Deployment Software" on page 25 	Install a new probe. You can install a probe manually, or use deployment software to install probes for multiple sites.
Choose one of the following options: <ul style="list-style-type: none"> • "Configure a Windows Probe" on page 26 • "Configure a Software Deployed Probe" on page 27 	You must configure the probe to communicate with Vantage DX Diagnostics. Select the configuration procedure that corresponds to the method that was used to install the probe.

Install a Windows Probe

Use the following procedure to install a Windows probe for each of your sites. This procedure must be completed for each configured site. Each probe must be installed on a machine that is located at the site you are configuring.

Before you Begin

- A site must already be configured. See ["Create a Site" on page 21](#).
- Ensure the system meets the requirements listed in ["Requirements" on page 7](#).

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the **Manage Sites** page, select the site where you want to install the probe, then click the **Windows - Download** link to download the installer.
3. Extract the file and ensure that the installer is not blocked by your operating system. After you download the installer, follow these steps:
 - Right-click on the MSI file.
 - Click **Properties**.
 - In the **Security** section, select the **Unblock** checkbox.
 - Click **OK**.
4. Run the file to install the probe software on a machine that is located at the site being configured.
5. If prompted, click **Yes** to allow the application to make changes to the computer.
6. Follow the instructions in the Install Wizard to complete the installation.
7. When the install process is complete, click **Finish** to exit the Wizard.

Next Steps

- Configure the probe to communicate with Vantage DX Diagnostics. See ["Configure a Windows Probe" on page 26](#).

Install a Probe Using Deployment Software

Use the following procedure to install a Vantage DX Diagnostics probe for each of your sites. You must be an administrator to perform this procedure.

Before you Begin

- A site must already be configured. See ["Create a Site" on page 21](#).
- Ensure the system meets the requirements listed in ["Requirements" on page 7](#).

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the **Manage Sites** page, select the site where you want to install the probe, then click the **Windows - Download** link to download the installer.
3. Extract the file and ensure that the installer is not blocked by your operating system. After you download the installer, follow these steps:
 - Right-click on the MSI file.
 - Click **Properties**.
 - In the **Security** section, select the **Unblock** checkbox.
 - Click **OK**.
4. Run the installer using your own deployment software. To complete the installation without user input, ensure that you run the installer with the `/quiet` option.

Next Steps

- Configure the probe to communicate with Vantage DX Diagnostics. See ["Configure a Software Deployed Probe" on page 27](#).

Configure a Windows Probe

After you install the probe software at a site, you must configure it to connect with Vantage DX Diagnostics. Complete this procedure for each installed Windows probe.

Before you Begin

- Ensure the probe software is already installed on a computer at the site.
1. Click **Manage** to access the Application Management page, then click **Sites**.
 2. On the Site Management page, select the site you are configuring and generate the probe PIN by clicking **Generate PIN**.



Tip: Make note of the Hostname and PIN displayed on this page.

3. From the Start Menu on the Windows computer where you installed the probe software, navigate to **Vantage DX Diagnostics > Vantage DX Diagnostics Config**.
A command window appears.



Note: If you changed the name of the install directory during the installation, **Vantage DX Diagnostics Config** is found under that directory name instead.

4. In the command window, at the Vantage DX Diagnostics server FQDN prompt, type the **Hostname** and press **Enter**.
5. When prompted, type the PIN that you generated in step 1 and press **Enter**.
6. Once the Probe configuration successfully completes press **Enter** to exit the command window.
7. To confirm that probe is successfully installed go to the site configuration page in Vantage DX Diagnostics and check that the Probe's status is now **Connected**.



Tip: You might need to reload the page in the browser to see the updated status.

Configure a Software Deployed Probe

After you install the probe software at a site, you must configure it to connect with Vantage DX Diagnostics. Complete this procedure for each probe that was installed via deployment software.

You must be an administrator in Vantage DX to perform the steps on the Vantage DX Diagnostics interface. You do not need to have administrator permissions on the computer where the probe software is installed.

Before you Begin

- Ensure the probe software is already installed on a computer at the site.

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the Site Management page, select the site you are configuring and generate the probe PIN by clicking **Generate PIN**.



Tip: Make note of the Hostname and PIN displayed on this page.

3. On the computer where you installed the probe software, navigate to C:\Program Files\VantageDxDiagnostics\non-admin-probe-config.bat. Alternatively, you can enter "Non admin Vantage DX Diagnostics config" in the **Search** menu.
A command window appears.



Note: If you changed the name of the install directory during the installation, **Vantage DX Diagnostics Config** is found under that directory name instead.

4. Execute the script and include the Hostname and PIN using the following format:
`.\non-admin-probe-config.bat <hostname> <pin>`
If you do not include the Hostname and PIN, the script will prompt you to enter them
5. After the script successfully completes, press Enter to exit the command window.
6. Wait up to 5 minutes for the probe configuration to complete.

7. To confirm that probe is successfully installed go to the site configuration page in Vantage DX Diagnostics and check that the Probe's status is now **Connected**.



Tip: You might need to reload the page in the browser to see the updated status.



View Network Path Data

Vantage DX Diagnostics provides visual representations of network paths between your sites and the target endpoints.

To visualize and understand the network path data see ["View Data for a Site Group or Site" on page 29](#).

View Data for a Site Group or Site

A site group consists of one or more sites. You can view data for all of the sites in a group at once to have a global view the network performance between the target endpoints and your sites. You can also choose to view performance data for a single site.

Use this procedure to view and understand the test data for a site group or a site.

1. From the sidebar on the left of the interface, use the following options to filter and group the data:
 - **Test Type**—Displays site-to-service network paths by service. This option allows you switch between service endpoints to easily determine which sites are having issues with a specific service. Alternatively, you can view all service endpoints to view all of the site-to-service network paths, and all of the correlations between those network paths.
 - **Date**—Display results for a selected date. The default is the current date.
 - **Time of day**—Display results for a selected time, in 15-minute increments.
 - **Site**—Display results for selected sites. The top 10 sites with recent test results are displayed by default. These sites are organized in the following order: sites with failed tests, sites with passed tests, and sites without test results.

If you have many sites, or the site you want to view is not in the top 10 sites, type the site name in the search bar to find the specific site.

You can also click **Select All**, to display the path visualization for all sites. Use the **Deselect All** button to remove any selected sites from the path visualization.

Optionally, you can set the **Auto-select sites with results** option to **On** to only display the sites that have network path test results in the diagram.

- **Grouping**—Click the **Grouping** link to display the grouping options:
 - **Group by network hop**—Select one of none, by network, or by network owner.
 - **Show network owner**—Set to **On** to highlight each network owner in the diagram in a different color. You can also select which networks to highlight in the diagram.
- 2. Review the information in the **Path Analysis** panel. This panel displays the following information about the paths from site groups or sites to the endpoints:
 - **Microsoft Teams Servers** map—(Only displayed when viewing the Microsoft Teams service.) This map displays a global view of the entry points to the MS data centers that contain MS Teams servers.
 - Site-to-service path details:
 - **Name of the path**—The name of the site to the URL of the endpoint. For example "MySite to world.tr.teams.microsoft.com".
 - **hops taken**—Number of intermediate devices that a packet passes through from the source site to the endpoint.
 - **round-trip time**—The time in milliseconds that it takes a data packet to travel from point A to B and return.
 - **jitter**—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.
 - **packet loss**—Percentage of packets that are lost in a given period of time. Packet loss directly affects audio quality.
 - **! messages**—Warning messages that inform you about detected performance issues. Issues that can be related to a specific hop include information about the hop where the path started to experience an issue.
- 3. To view detailed information about each hop in the path, choose one of the following options from the **Path Analysis** panel:
 - If you are viewing Microsoft Teams services and want to view the details about any site that displays on the Microsoft Teams Servers map, click the site pin icon on the map.

- If you are viewing any monitored services, click the **View Path Details** link in the site-to-service details.
4. Use the **Hop Breakdown** selector to display details for:
- **Round-trip time**—The time in milliseconds that it takes a data packet to travel from point A to B and return.
 - **Jitter**—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.
 - **Packet loss**—Percentage of packets that are lost in a given period of time. Packet loss directly affects audio quality. The packet loss is calculated based on the frequency configured for the target endpoint (5, 15 or 30 minutes) and the packet count configured for the site group (10, 30, or 50).



© Copyright 2024, Martello Technologies Corporation. All Rights Reserved.

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

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