

Interfacing with Uptime Infrastructure Monitor

Some of the Monitoring Station's features require integration with other elements that make up your infrastructure. In some cases configuration is mandatory (for example, an SMTP server must be set at the time of installation), while in others it is required only when particular Uptime Infrastructure Monitor features are used (for example, using the Web Application Transaction monitor requires you to provide Uptime Infrastructure Monitor with your proxy server settings). The following sections outline how to configure Uptime Infrastructure Monitor to communicate with servers and databases.

Monitoring Station Web Server

Monitoring Stations include a Web server component that drives the user interface. Any Monitoring Station that is accessed by users or administrators requires a URL. The Web address used to access the Monitoring Station is configured through the following `uptime.conf` parameter:

```
httpContext=http://<hostname>:<port>
```

- `<hostname>` is the host name of the server on which Uptime Infrastructure Monitor is running (for example, `localhost`)
- `<port>` is the port on which the Uptime Infrastructure Monitor Web server is listening for requests (for example, `9999`); you can optionally omit the port number

If the Uptime Infrastructure Monitor interface is accessed via SSL, the value for this parameter should be `https` instead of `http`.

Topics on this page

- [Monitoring Station Web Server](#)
- [SMTP Server](#)
- [Database Settings](#)
- [Configuring Global Data Collection Methods](#)
- [Global SNMP Configuration Settings](#)
- [RSS Feed Settings](#)
- [VMware vCenter Orchestrator Integration](#)
- [Web Application Monitor Proxy Settings](#)
- [Remote Reporting Settings](#)
- [User Interface Instance Settings](#)
- [Scrutinizer Settings](#)
- [Splunk Settings](#)

SMTP Server

Uptime Infrastructure Monitor uses a mail server to send alerts and reports to its users. After installing Uptime Infrastructure Monitor for the first time, the administrator was asked to enter SMTP server information. These initial values can be modified in the **Mail Servers** configuration panel.

Modifying the SMTP Server Used by Uptime Infrastructure Monitor

To configure Uptime Infrastructure Monitor's mail server, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Config**.
2. In the left panel, click **Mail Servers**.
3. In the sub panel, click **Edit Configuration**.
4. Type the name of the mail server in the **SMTP Server** field.
This value was set the first time the Uptime Infrastructure Monitor administrator logged in after installation; the default value is the name of the host on which the Monitoring Station was installed at that time.
The name of the server could follow the `smtp.<domain_name>` convention, or could be its host name or IP address.
5. Optionally, enter the port used by the mail server in the **SMTP Port** field.
6. In the **SMTP Sender** field, enter the email address that Uptime Infrastructure Monitor uses to send alert notifications and reports.
This value was set the first time the Uptime Infrastructure Monitor administrator logged in after installation, and should be set to your domain (for example, `admin@mail.idera.com`).
A sender's name can be encapsulated with double quotes, in which case, the email address is encapsulated with angled brackets: `"uptime administrator" <admin@idera.com>`
7. In the **SMTP HELO String** field, enter the string that identifies the domain from which a message is sent (for example, `idera.com`).
8. In the **SMTP User** field, enter the user name that is used to authenticate connections with the SMTP server.
9. In the **SMTP Password** field, enter the password that is used to authenticate connections.
10. Click **Save**.
The edit window closes, and you are returned to the **Mail Server Configuration** panel.
11. To test the mail server configuration, click the **Test Configuration** button.
The Monitoring Station attempts to send an email message containing the configuration information to the email address of the Uptime Infrastructure Monitor administrator. If an error message appears in the subpanel, edit and then re-test the configuration.

Database Settings

The database settings are used to determine how Uptime Infrastructure Monitor communicates with the DataStore, and how it performs a database health check. The following are the database-related parameters in the `uptime.conf` file.

Connection	
dbType	<p>The type of database that is used to store data from Uptime Infrastructure Monitor. The default value is <code>mysql</code>. You can also specify <code>mssql</code> and <code>oracle</code> to use SQL Server and Oracle, respectively.</p> <p>By default, Uptime Infrastructure Monitor uses a JDBC (Java Database Connectivity) driver, and the driver used to connect to the DataStore corresponds to the database selected:</p> <ul style="list-style-type: none">• <code>com.mysql.jdbc.Driver</code> (for MySQL)• <code>net.sourceforge.jtds.jdbc.Driver</code> (for Microsoft SQL Server)• <code>oracle.jdbc.OracleDriver</code> (for Oracle)
dbHostname	The name of the system on which the database is running. The default is <code>localhost</code> .
dbPort	The port on which the database is listening. The default is <code>3308</code> .
dbName	The name of the database. The default is <code>uptime</code> .
dbUsername	The name of the default database user. The default is <code>uptime</code> .
dbPassword	The password for the default database user. The default is <code>uptime</code> .
dbJdbcProperty	<p>Optional property-and-value pairs to append to the JDBC database URL. Note that only MySQL and Microsoft SQL Server supports URL properties, so this setting does nothing if you are using Oracle. The value of the <code>dbJdbcProperty</code> parameter in <code>uptime.conf</code> should be verbatim as that which would be manually added to the URL. The exact format depends on the database type. Consider the following examples:</p> <ul style="list-style-type: none">• <code>dbJdbcProperty=instance=sqlserver;ssl=request</code> (for MS SQL Server)• <code>dbJdbcProperty=instance=mysql&useSSL=true</code> (for MySQL)
Health	
datastoreHealthCheckInterval	When this parameter is enabled with a non-zero value, Uptime Infrastructure Monitor performs a database health check. The value provided is the frequency of the check, in seconds. The default is <code>5</code> .
datastoreHealthCheckTimeLimit	When the health check time limit is reached (the value unit is seconds, and the default is <code>300</code>), Uptime Infrastructure Monitor considers the database down. The Data Collector service is stopped, and administrators that are members of the SysAdmin user group are sent an email.
Performance	
connectionPoolMaximum	The maximum number of connections that are allowed to the DataStore. Setting this option to a lower number helps increase the performance of Uptime Infrastructure Monitor.
connectionPoolMaxIdleTime	(c3p0 library) Sets the amount of time a connection can be idle before it is closed. This parameter should only be modified with the assistance of Uptime Infrastructure Monitor Customer Support.
connectionPoolNumHelperThreads	(c3p0 library) Sets the number of helper threads that can improve the performance of slow JDBC operations. This parameter should only be modified with the assistance of Uptime Infrastructure Monitor Customer Support.

Changing the DataStore Database

The Uptime Infrastructure Monitor DataStore is first linked to a database during the installation process, and contains important historical performance data that is collected. Linking the DataStore to a new database results in lost data unless you properly migrate your data to the new database. As such, changing the DataStore's database should be done only after some consideration and planning.

In cases where you would like to migrate the database (for example, from the default Uptime Infrastructure Monitor MySQL implementation to Oracle) or move the DataStore to a different system from the Monitoring Station, you must modify the aforementioned database values in the `uptime.conf` file. Note that the modification of these values is one of a series of steps. Refer to the Uptime [Knowledge Base](#) for more information on migrating your DataStore.

Configuring Global Data Collection Methods

A Windows-based Element can retrieve metric data either through the Uptime Infrastructure Monitor Agent, or via WMI (see [Agentless WMI Systems](#) for more information). You can configure details for either method at a global level, in the form of agent connection information or WMI access credentials. Having global details defined simplifies individual Element configuration, and also allows you to switch the data collection method for multiple Windows Elements, at once, as a group.

When a system is part of the Uptime Infrastructure Monitor inventory, its data collection method is either configured to be based on an agent, or a WMI agentless method. This configuration option is set when the system is first added as an Element. If agent and WMI details are globally defined, when adding the Element, you are able to use the **Uptime Agent Global Configuration**, or use **WMI Agentless Global Credentials** to skip configuration steps.

Once configured, this data collection method can later be switched from an agent-based, to agentless method, or vice versa. Although this change can be made on a per-Element basis, multiple Elements can also be switched in a single batch. In the latter case, the data collection method must be globally defined.

To configure data collection methods globally, you can provide information for either the Uptime Infrastructure Monitor Agent, or your organization's WMI credentials, or both. Note that batches of Elements can only be converted to a particular data collection source when that method is globally configured in the **Global Credentials Settings** panel.

Configuring Global WMI Credentials

To provide WMI credentials that can be used to switch Windows Elements from agent-based data collection:

1. On the Uptime Infrastructure Monitor tool bar, click **Config**.
2. In the left panel, click **Global Credentials Settings**.
3. In the **WMI Agentless Global Credentials** sub panel, click **Edit Configuration**.
4. Enter the **Windows Domain** in which WMI is implemented.
5. In the **Username** field, enter the user ID that has administrative access to WMI on the Windows domain.
6. In the **Password** field, enter the password for the WMI account.
7. Click **Save** to retain your changes.
8. Click **Test Configuration** to ensure the credentials provided are correct.

Configuring a Global Uptime Infrastructure Monitor Agent Configuration

To provide the Uptime Infrastructure Monitor Agent information that can be used to switch Windows Elements from agentless, WMI-based data collection, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Config**.
2. In the left panel, click **Global Credentials Settings**.
3. In the **Uptime Agent Global Configuration** sub panel, click **Edit Configuration**.
4. Enter the **Agent Port Number**, indicating the port the Uptime Infrastructure Monitor Agents use to communicate with the Uptime Infrastructure Monitor Monitoring Station.



The port number entered reflects what the Uptime Infrastructure Monitor Agents are configured to use; this setting does not modify the agent-side configuration.

5. Select the **Use SSL** check box if the agents securely communicate with the Monitoring Station using SSL.
6. Click **Save** to retain your changes.
7. Click **Test Configuration** to ensure the information provided is correct.

Global SNMP Configuration Settings

When you add a network device to Uptime Infrastructure Monitor, as part of the configuration process, you must provide details about how SNMP is configured to communicate with and manage other devices on the network. These details describe, among other things, the SNMP protocol used, and encryption methods.

By default, SNMP-specific settings are inputted for each network-type device, as they are added to Uptime Infrastructure Monitor. To facilitate this process, your network's SNMP settings can be defined globally in the **Global Credentials Settings** panel.

Global SNMP Settings

The following SNMP settings are used to configure network-related Elements, and can be defined globally.

SNMP Version	The SNMP version the network device and your network are using.
SNMP Port	The port on which network devices are configured to listen for SNMP messages.
Read Community	A string that acts like a user ID or password, giving you access to the network device instance. Common read communities are "public," enabling you to retrieve read-only information from the device, and "private," enabling you to access all information on the device.

Username	The name that is required to connect to the network device.
Authentication Password	The password that is required to connect to the network device.
Authentication Method	<p>This option determines how encrypted information traveling between the network device and Uptime Infrastructure Monitor is authenticated:</p> <ul style="list-style-type: none"> • MD5: A widely-used method for creating digital signatures used to authenticate and verify the integrity of data. • SHA: A secure method of creating digital signatures. SHA is considered the successor of MD5 and is widely used with network and Internet data transfer protocols.
Privacy Password	The password that is used to encrypt information traveling between the network device and Uptime Infrastructure Monitor.
Privacy Type	<p>From the list, select an option that determines how information traveling between the network device and Uptime Infrastructure Monitor is encrypted:</p> <ul style="list-style-type: none"> • DES: An older method used to encrypt information. • AES: The successor to DES, which is used with a variety of software that require encryption including SSL servers.
Pingable Node	<p>This specifies whether Uptime Infrastructure Monitor can contact the network device using the ping utility.</p> <p>There are scenarios in which you might not want the network device to be pingable (e.g., you have a firewall in place). Before enabling this option, you should try to contact it using the ping utility. If you cannot ping it, ensure this check box is left cleared. Then, change the default host check for the network device. See Changing Host Checks for more information.</p>

Globally Defining SNMP Version 2 Settings

To globally define the SNMP version 2 settings used to communicate with network devices on your network, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Config**.
2. In the left panel, click **Global Credentials Settings**.
3. In the **SNMP Global Credentials** sub panel, click **Edit Configuration**.
4. Enter the **SNMP Port** on which your network devices are listening.
5. Enter the **Read Community** used to access network devices (for example, `public` or `private`).
6. Indicate whether Uptime Infrastructure Monitor can contact the network device with the ping utility by selecting or clearing **Is Node Pingable?** checkbox.
7. Click **Save** to retain your changes.
8. Click **Test Configuration** to ensure the information provided is correct.

Globally Defining SNMP Version 3 Settings

To globally define the SNMP version 2 settings used to communicate with network devices on your network, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Config**.
2. In the left panel, click **Global Credentials Settings**.
3. In the **SNMP Global Credentials** sub panel, click **Edit Configuration**.
4. For the **SNMP Version**, select **v3**.
The configuration fields relevant to that SNMP version appears.
5. Enter the **SNMP Port** on which your network devices are listening.
6. Enter the **Username** used to connect to network devices.
7. Optionally enter the **Authentication Password** required to connect to network devices.
8. Indicate the **Authentication Method** used for encryption.
If no password is provided, the authentication method is ignored.
9. Optionally enter the **Privacy Password** used to encrypt communication between network devices and Uptime Infrastructure Monitor.
10. Indicate the **Privacy Type** used for encryption.
If no password is provided, the authentication method is ignored.



You can set both the authentication and password types, only one of them, or neither.

11. Indicate whether Uptime Infrastructure Monitor can contact the network device with the ping utility by selecting or clearing **Is Node Pingable?** checkbox.
12. Click **Save** to retain your changes.
13. Click **Test Configuration** to ensure the information provided is correct.

RSS Feed Settings

Uptime Infrastructure Monitor displays a list of recent knowledge base articles in the **My Portal** panel. This list is fed to the **My Portal** panel via RSS (Really Simple Syndication, a method for delivering summaries of and links to Web content). Clicking the title of an article opens it in your Web browser.

By default, RSS feeds are drawn directly from the Uptime Infrastructure Monitor Support Portal without the use of proxy server information. If your Monitoring Station accesses the Internet through one, feeds are most likely unavailable, and the following message appears in the **My Portal** panel:

You can change the RSS feed settings to point to the proxy server rather than directly to the Uptime Infrastructure Monitor Web site by manually inputting settings in the **Uptime Configuration** panel, as outlined in [Modifying Uptime Infrastructure Monitor Config Panel Settings](#).

Changing Proxy Server Information for RSS Feeds

You can manually configure the settings for RSS feeds through the following parameters (default values, if applicable, are shown):

Parameter	Description
rssFeedUrl	the URL of the RSS feed (for example, <code>rssFeedUrl= http://support.idera.com/rss/kb.xml</code>)
httpProxyHost	the host name of the proxy server that the Monitoring Station uses to access the Internet
httpProxyPort	the port through which the Monitoring Station communicates with the proxy server
httpProxyUsername	the user name required to use the proxy server
httpProxyPassword	the password required to use the proxy server

VMware vCenter Orchestrator Integration

Administrators can configure Action Profiles to automatically carry out tasks in the event of an Uptime Infrastructure Monitor alert. One such task is the initiation of contact with VMware vCenter Orchestrator, and the execution of a workflow. To have access to this functionality, Uptime Infrastructure Monitor needs to know how to communicate with Orchestrator.

For information about Action Profiles and VMware vCenter Orchestrator, see [Action Profiles](#).

Integrating Uptime Infrastructure Monitor with VMware vCenter Orchestrator

To configure Uptime Infrastructure Monitor integration with Orchestrator to execute workflows, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Config**.
2. In the left panel, click **VMware vCenter Orchestrator**.
3. In the sub panel, click **Edit Configuration**.
4. Ensure the **VMware Orchestrator Enabled** check box is selected.
5. In the **VMware Orchestrator Server** field, enter the host name of, or IP address assigned to the Orchestrator server when it was configured.
6. In the **VMware Orchestrator Port** field, enter the port the Orchestrator server was configured to use in order to communicate with other systems.
7. Optionally select the **Use SSL** check box if Orchestrator was configured to use an SSL certificate.
8. Enter the **Username** and **Password** of an appropriate user account on the Orchestrator server.
For proper integration, an Orchestrator account with View and Execute permissions is required.
9. Click **Save**.
The configuration window closes, and you are returned to the **VMware vCenter Orchestrator Configuration** panel.
10. To ensure the settings you provided are correct, click the **Test Configuration** button.
The Monitoring Station attempts to communicate with the VMware vCenter Orchestrator server. If an error message appears in the subpanel, edit and then re-test the configuration.

Web Application Monitor Proxy Settings

When the Web Application Transaction monitor is recording a user session on an external site, it is intercepting URLs by acting as your browser's proxy. For the monitor to do this, you must replace your organization's proxy server information with the Web Application Transaction monitor in your browser settings. In order for the monitor to access the Internet, you must provide your proxy settings in Uptime Infrastructure Monitor.

This monitor-specific proxy information is used during transaction recording; during session playback, the proxy normally used by Uptime Infrastructure Monitor (defined by the `httpProxy*` settings) is used.

For more information about the Web Application Transaction monitor, see [Web Application Transactions](#).

You can change Uptime Infrastructure Monitor's proxy server configuration by manually inputting settings in the **Uptime Configuration** panel, as outlined in [Modifying Uptime Infrastructure Monitor Config Panel Settings](#).

Changing Proxy Server Information for Uptime Infrastructure Monitor

You can configure the proxy server settings used by Uptime Infrastructure Monitor when running the Web Application Transaction monitor with the following parameters:

Parameter	Description
-----------	-------------

webmonitor. proxyHost	the host name of the proxy server that the Web Application Transaction monitor uses to access the Internet during transaction recording
webmonitor. proxyPort	the port through which the Web Application Transaction monitor communicates with the proxy server during transaction recording

Remote Reporting Settings

If you are using a reporting instance (an Uptime Infrastructure Monitor instance that only generates and serves reports), the remote reporting settings enable you to specify the location of the reporting instance, and the port on which it is listening.

Modifying the Remote Reporting Server Settings

To configure the remote reporting instance used by Uptime Infrastructure Monitor, do the following:

1. On the Uptime Infrastructure Monitor tool bar, click **Config**.
2. In the left panel, click **Remote Reporting**.
3. In the sub panel, click **Edit Configuration**.
4. Ensure the **Reporting Instance Enabled** check box is selected.
5. In the **Remote Reporting Server** field, enter the host name or IP address of the server on which the remote reporting instance is found.
6. Enter the port used to communicate with the server.
7. Click **Save**.
The edit window closes, and you are returned to the **Remote Reporting Instance Configuration** panel.
8. To test the remote reporting server configuration, click **Test Configuration**.
A pop-up window appears, indicating whether Uptime Infrastructure Monitor was able to connect to the remote reporting instance. If an error message is displayed, correct your configuration and re-test it.

Note that the modification of these values is one of a series of steps performed to correctly set up a remote reporting instance. See [Remote Reporting Instances](#) for more information.

User Interface Instance Settings

A UI instance is an Uptime Infrastructure Monitor installation that does not perform any data collection tasks, and is primarily used for real-time monitoring and report generation. When there are many Uptime Infrastructure Monitor users who do not need to perform full administrative tasks, UI instances can divert traffic from a core Monitoring Station implementation, improving data-collection performance and UI responsiveness.

You can manually configure UI instance settings with the following `uptime.conf` parameters:

Parameter	Description
uiOnlyInstance	enables the Monitoring Station as a user interface instance
uiOnlyInstance. monitoringStationHost	the host name or IP address of the Uptime Infrastructure Monitor Monitoring Station that is performing data collection, and to which this UI instance connects
uiOnlyInstance. monitoringStationCommandPort	the port through which the UI instance can communicate with the core data-collecting Monitoring Station; in most cases, this port should be 9996, otherwise the UI instance does not communicate properly with the core Monitoring Station

Creating an Uptime Infrastructure Monitor UI Instance

To create a UI instance, do the following:

1. Using the [standard Uptime Infrastructure Monitor installer](#), install a new instance of Uptime Infrastructure Monitor on another server.
During the install process, when prompted to provide DataStore configuration information, ensure the UI instance has the same database settings as the core Monitoring Station (see [Database Settings](#) for more information).
2. After installation, enable the newly installed Uptime Infrastructure Monitor as a UI instance by editing the following `uptime.conf` parameters:
 - `uiOnlyInstance=true`
 - `uiOnlyInstance.monitoringStationHost=<hostname>`
hostname is the hostname or IP address of the core, data-collecting Monitoring Station, with which this UI instance can communicate
 - `uiOnlyInstance.monitoringStationCommandPort=9996`
the port through which the UI instance can communicate with the core Monitoring Station



Unless your core Monitoring Station is customized, it is configured to use port 9996 to communicate with a UI instance. If you wish to use a different port, you must ensure matching `uptime.conf` values exist on both the UI instance and core Monitoring Station. Contact IDERA Customer Support for more information.

3. Ensure the proxy used by the Controller on the UI instance directs to the core Monitoring Station. By default, this proxy is configured with the assumption that the Controller and Monitoring Station are running on the same host. See [Configuring the Uptime Infrastructure Monitor Controller](#) for more information.
4. Shut down the Data Collector service on the UI instance.
5. Ensure you are logged in with a domain account, and that this account has access to the `<installDirectory>/gadgets` directory on the Monitoring Station.

6. To accommodate sharing user-created gadgets, on the core Monitoring Station system, make the <installDirectory>/gadgets directory accessible by the UI instance system.
How you make the /gadgets directory accessible depends on the Monitoring Station platform:
 - On Linux, you can use NFS to share the directory on the core Monitoring Station, then mount it on the UI instance
 - On Windows, you can use the mklink command to create a symbolic link on the UI instance that points to the /gadgets directory on the core Monitoring Station, such as in the following example:
mklink /D "C:\Program Files\uptime software\uptime\gadgets" "\\host\gadgets"
You most likely need to modify sharing and security permissions for the directory.
7. Restart the Data Collector service on the UI instance.

Scrutinizer Settings

Scrutinizer is a NetFlow analyzer that can be installed to monitor network traffic managed by compatible switches and routers. Scrutinizer can be integrated with Uptime Infrastructure Monitor as a **NetFlow** dashboard, and can directly link network devices monitored by Scrutinizer to their NetFlow data from each Element's Graphing tab. In order to access Scrutinizer, Uptime Infrastructure Monitor needs to be pointed to your installation. For more information about using Scrutinizer, see [Integrating Scrutinizer with Uptime Infrastructure Monitor](#).

Modifying the Scrutinizer Settings

You can configure Scrutinizer's integration with Uptime Infrastructure Monitor through the following parameters:

Parameter	Description
netflow.enabled	determines whether Scrutinizer is integrated with the Monitoring Station
netflow.hostname	the host name or IP address of your Scrutinizer installation
netflow.port	the HTTP port through which Scrutinizer sends and receives communication
netflow.username	(Pre Scrutinizer 16.7 versions only) the username required to log in to Scrutinizer
netflow.password	(Pre Scrutinizer 16.7 versions only) the password required to log in to Scrutinizer
netflow.authToken	(Scrutinizer 16.7 and later only) the token required to log in to Scrutinizer

Creating a Scrutinizer authentication token (Scrutinizer 16.7 and later only)

NetFlow Scrutinizer 16.7 introduced the use of an authentication token instead of a username and password to integrate with other products. You must create the token in Scrutinizer, and then provide it to Uptime Infrastructure Monitor.

Splunk Settings

Splunk is a third-party search engine that indexes log files and data from the devices, servers, and applications in your network. Using Splunk, you can quickly analyze your logs to pinpoint problems on a server or in a network, or ensure that you are in compliance with a regulatory mandate or Service Level Agreements. You install Splunk on a server in your datacenter.

When values are provided for the Splunk settings listed below, the Splunk icon appears in the **My Portal** panel beside the names of services that are in WARN or CRIT states. When you click the Splunk icon, you are automatically logged in to your Splunk search page.

You can change your Uptime Infrastructure Monitor-Splunk integration by manually inputting settings in the Uptime **Config** panel, as outlined in [Modifying Uptime Infrastructure Monitor Config Panel Settings](#).

Changing Splunk Server Information for Uptime Infrastructure Monitor

You can enable automatic login to the Splunk search page, or modify an existing configuration through the following parameters:

Parameter	Description
splunk.url	the URL of the server on which your Splunk search page is hosted (for example, http://webportal:8000)
splunk.username	the username required to log in to your Splunk search page
splunk.password	the password required to log in to your Splunk search page
splunk.soapurl	<p>the URL that points to the SOAP management port that Splunk uses to communicate with the Splunk daemon (for example, http://webportal:8089).</p> <p>In the URL, you must include the port on which the Splunk server listens for requests. See the Splunk Admin Manual for more information.</p>

