WMI User Permissions

To monitor a system via WMI, it must be added to Uptime Infrastructure Monitor using a user with domain admin or local admin privileges. This requirement is due to Windows permissions. It is important to note that Uptime Infrastructure Monitor does not make any changes to the domain or Active Directory environment or systems in any way; it simply makes read-only requests for the system information.

After the system has been added to Uptime Infrastructure Monitor, if there are security concerns related to the elevated privileges, a user account with the limited permissions described below should be sufficient to enable WMI agentless operation to function properly. Although administrator user credentials should eliminate potential access issues, this level is not strictly required for monitoring.

Permissions required for monitoring a system via WMI:

1. User Roles: Distributed COM User, Performance Monitor Users.
2. Enable Account and Remote Enable for the user to the CIMV2 WMI namespace.

> **Note**
>
> If a restricted user with the above permissions is used, Uptime Infrastructure Monitor will not be able to perform the regular system re-scans to pick up any system changes, as it will not have the required privileges.

> **Note**
>
> Local policies at the Active Directory level may over-ride your local standard user (e.g. wmiuser, as in the example below) so you may need to consult with server or authorization administrators to ensure proper operation and/or to maintain compliance with corporate security policies.

The options format for WMI-based agentless monitoring includes the following fields in addition to the standard element fields:

- WMI Domain (optional)
- WMI Username
- WMI Password

For example:

- Host Name: hostname1
- Display name: windows machine
- Type: WMI Agentless
- WMI Username: wmiuser
- WMI Password: uptime
- %%