

Behind the Report:

Secure, Automate, and Monitor Server Environments at Scale

Comparing the baseboard management controller (BMC) and multiple server management tools between Dell Technologies and a leading competitor

In this report, Prowess Consulting compares server management tools from Dell and an enterprise competitor, referred to as Vendor K, across four focus areas: **security**, **ease of use**, **analytics**, and **sustainability**. Table 1 shows the tools we evaluated and the main feature each tool provides.

Testing Summary

Testing included a hands-on review of the Dell and Vendor K server management platforms' interfaces, in addition to a detailed review of related documentation from both providers. We reviewed both the single-server baseboard management controller interface and the tools for managing a large server environment. While we made every effort to ensure a fair comparison, we have omitted the detailed steps taken for the Vendor K tools from this document in order to preserve Vendor K's anonymity.

Table 1 | Summary of Dell and Vendor K server management tools

Feature	Dell Technologies	Vendor K
Embedded/remote server management	Integrated Dell™ Remote Access Controller 10 (iDRAC10)	Vendor K baseboard management controller (BMC)
One-to-many device management console	Dell OpenManage™ Enterprise (OME)	Vendor K enterprise management console
Cloud-based monitoring	Dell Artificial Intelligence for IT Operations (AIOps)	Vendor K cloud management platform

Embedded/Remote Server Management

This section outlines the features and steps taken to compare iDRAC10 against the Vendor K BMC.

System Lockdown

To adjust the current System Lockdown settings:

1. From any page, click the **padlock icon** in the toolbar at the top right of the page.
 - a. The current System Lockdown status will be displayed.
2. Click **Enable** to prevent changes or **Disable** to unlock the system to allow changes. Note that the padlock icon will either open or close to reflect the status.
3. With System Lockdown enabled, navigate to a configuration page, and then note that editing of settings is disabled.

Full-System BIOS Configuration

To access and stage changes to BIOS settings from within the BMC:

1. To access BIOS settings, navigate to **Configuration > BIOS Settings**.
2. Use the tabs at the top of the page to access all BIOS category settings.
3. Modify values per page as desired.
4. Click **Apply** to save the per-page BIOS modifications.
5. To stage the BIOS changes, click **Apply at next reboot**.

Automatic Firmware Updates

To enable automatic updates on a specified schedule:

1. Navigate to **Maintenance > System Update > Automatic Update**.
2. Click **Enable Automatic Updates**, and then click **OK** on the confirmation window.
3. Choose a server reboot behavior from either **Update and Reboot** or **Download but Don't Reboot**.
4. Select **HTTPS** as the location type (**Network Share**, **FTP**, **TFTP**, and **HTTP** are also supported).
5. Select the **Use default address** checkbox.
6. Specify a time of day for the update to occur.
7. Specify the schedule as daily, weekly, or monthly.
8. Click **Schedule Update**.

Import/Export Full Server Configuration Profile

To generate a server configuration export or import a settings file:

1. To export a server configuration backup, navigate to **Configuration > Server Configuration Profile > Export**.
 - a. From the **Location Type** dropdown menu, select **Local**.
 - b. In the **File Name** field, specify a name.
 - c. Specify the elements to be backed up:
 - i. For a full system backup, select **ALL**.
 - ii. For a partial system backup, select the desired components:
 1. **iDRAC**
 2. **BIOS**
 3. **NIC**
 4. **RAID**
 5. **Fibre Channel**
 6. **InfiniBand**
 - d. Specify the file format.
 - e. To start the file generation, click **Export**.
 - f. Once generated, click **Save Locally** to download the resulting backup.

2. To import a server configuration, navigate to **Configuration > Server Configuration Profile > Import**.
 - a. From the **Location Type** dropdown menu, select **Local**.
 - b. On the file path line, click **Choose File**, and then select the server export file to restore.
 - c. Select the components to include in the import from the **Import Components** line of checkboxes.
 - d. If non-default values are desired, specify the desired power state after the import, the shutdown method, and the maximum wait time.
 - e. To start the import, click **Import**, and then click **OK** to confirm.

Connection View

To enable the Connection View feature:

1. Navigate to **iDRAC Settings > Connectivity > Network > Common Settings**.
2. From the **Connection View** dropdown, select **Enabled**.
3. Click **Apply**.

To view the network connection view information for a given server:

1. Navigate to **System > Overview > Components > Network Devices**.
2. Click the name of the network card to view.
3. Scroll down to view the **Switch Connection ID** and **Switch Port Connection ID**.

Telemetry Streaming

To access the iDRAC10 telemetry graphical user interface (GUI) settings:

1. Navigate to **Configuration > System Settings > Telemetry Configuration > Telemetry Streaming**.
2. To enable or disable the feature, use the slider next to **Telemetry Data Stream**, and then click **Apply**.
3. To review available telemetry reports, select the **Metric Report Definition** tab.
4. To review or modify the settings of a specific report, from the **Telemetry Reports** section, click the three dots next to a report, and then review the **Report Settings**.

One-to-Many Device Management Console

This section outlines the steps taken to compare the one-to-many on-premises device management features in OME against the Vendor K enterprise management console.

Heterogeneous Server Monitoring

To confirm discovery support for servers from multiple vendors:

1. Navigate to **Monitor > Discovery**.
2. Click **Create**.
3. Provide a name for the discovery job.
4. From the **Device Type** list, select **Server**.
5. Select **Non-Dell Servers (via OOB)**.
6. Expand the dropdown and note support for **HPE iLO**, **Lenovo XClarity**, and **Other**.

Third-Party Integration Support

To view available management plugins:

1. Navigate to **Application Settings > Console and Plugins**.
2. Note the availability of **vCenter Integration**, **Operations Manager**, and **Virtual Machine Manager and Configuration Manager**.
3. Review Table 9 on pages 25–26 of the [OME user guide](#) for additional details.

Access Control

To set up a user with scope-based access control (SBAC), in addition to role-based access control (RBAC):

1. Navigate to **Application Settings > Users**.
2. Click **Add** to create a new user or **Edit** to modify an existing user.
3. From the **User Role** list, select the **Device Manger** role to access the user scoping options.
4. Next to **User Scope**, either select **All Devices** for no scoping or select **Selected Groups** and then click **Select Groups** to specify the scope.
5. In the **Target** dialog, choose the device groups accessible to this user, and then click **Save**.
6. Specify:
 - a. **User Name**
 - b. **Password** and **Confirm Password**
 - c. **Email address**
7. Click **Add** for new users or **Finish** if editing an existing user.

Alert-Based Automated Actions

To configure alert policies:

1. Navigate to **Alerts > Alert Policies**.
2. Click **Create** to open the alert-creation wizard.
3. Enter a name and description for the policy, and then click **Next**.
 - a. To activate based on a category of alert, choose one or more alert category, or leave the category unspecified, and then click **Next**.
 - b. To activate the policy based on a message ID, select the **Message** radial button, specify a **Message ID**, and then click **Next**.
4. From the **Target** page, select from **Device Groups**, **All Devices**, or **Undiscovered Devices**, and then click **Next**.
 - a. If selecting a device, from the resulting window, select one or more devices, click **Save**, and then click **Next**.
5. Specify a duration window during which the alert will be active, and then click **Next**.
6. Select the severity level of alerts to be considered, and then click **Next**.
7. Select an action to be taken if the alert occurs, such as powering off, and then click **Next**.
8. Review the settings, and then click **Finish**.

Report Builder with Customization

To view built-in reports:

1. Navigate to **Monitor > Reports**.
2. Note the 52 available built-in reports that can be run.

To create a custom report:

1. Navigate to **Monitor > Reports**.
2. Click **Create**.
3. Specify the name and description of the report, and then click **Next**.
4. From **Select Columns**, expand a category, and then select the chosen metric.
5. Repeat step 4 as needed to include all desired metrics.
6. Click **Finish**.

Management Scalability

To validate the system management limits:

1. To confirm the upper limit of manageable servers, review the "Discovery" row of Table 7 on page 22 of the [OME user guide](#) and note the value of 8,000.
2. To confirm the upper limit of monitored servers, review the "Discovery" row of Table 8 on page 24 of the [OME user guide](#) and note the value of 25,000.

Power Management Reporting and Visibility

To view reports specifically related to power consumption:

1. Navigate to **Monitor > Reports**.
2. From the **Category** column, click **Filter**, and then select **Power Managed Devices**.
3. Note the 19 available reports.
4. From the **Category** column, click **Filter**, and then select **Power Managed Groups**.
5. Note the 9 additional reports.

Carbon Emissions and Footprint Analysis

To specify which devices will be monitored for carbon emissions data:

1. Navigate to **Power Management > Power Managed Devices**.
2. Click **Add Device(s)**.
3. View all discovered devices by expanding the various system groups.
4. Select the devices to be monitored, and then click **Add Selected**.
5. Confirm which devices will be monitored via the **Individual Devices** section.

To configure the carbon emission conversion factor:

1. Navigate to **Power Management > Settings**.
2. Click **Edit**.
3. Scroll down to the **Emissions Conversion Factor** and set the field according to the local power supplier data.
4. Click **Apply**.

To view carbon emissions data based on actual usage:

1. From the main menu, navigate to **Devices**.
2. Select a device from the list.
3. Click the **Telemetry** tab.
4. Review the **Energy Consumption Cost and Carbon Emission** section for data.

Automated Power and Thermal Management Policies

To configure a power management policy:

1. Navigate to **Power Management > Policies**, and then click **Create**.
2. From the **General** section, in the **Type** list, select either **Static** or **Temperature Triggered**.
3. Provide a policy name, and then click **Next**.
4. In the **Device/Groups** section, select the device or group where the policy will be applied, and then click **Next**.
5. In the **Settings** section:
 - a. For a static policy, specify the **Power Cap Limit** value.
 - b. For a temperature-triggered policy, specify the **Temperature Threshold** value from the available American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) class options.
 - i. Per page 314 of the [OME user guide](#), when a temperature-triggered policy is active, emergency power reduction (EPR) will be applied automatically.
6. Specify the duration, and then click **Next**.
7. From the **Schedule** section, specify the **Time Span**, **Days**, and **Active Date** that the policy will be active over, and then click **Next**.
8. Review the **Summary** section, and then click **Finish**.

To manually apply EPR:

1. Navigate to **Devices**, and then click the name of a device.
2. Select the **Policies and EPR** tab.
3. Click **Apply EPR** to activate.

Cloud-Based Monitoring

The following section outlines the steps taken to compare the cloud-based monitoring features of AIOps against the Vendor K cloud management platform.

Cybersecurity Advisories

This section outlines the steps taken to confirm support for security risk scoring, alerting, and remediation in the AIOps platform.

1. Review [Dell AIOps: A Detailed Review](#) (pages 28, 79, 85, 158, 184, and 187) noting the following passages:
 - a. **Composite risk score per system:** “The Risk value for each system provides an overall assessment for the system based on the enabled evaluation tests, and has one of the following values: Normal, Low, Medium, High, Unknown. The Risk score is calculated based on the impact of Cybersecurity issues, the tests in the evaluation plan, vulnerabilities from Dell Security Advisories, and detected ransomware.”
 - b. **Environment-level risk rollup:** “[This element] summarizes the active cybersecurity risks in the environment The overall environment has an assigned risk level.”
 - c. **Security advisories with impacted-system counts:** “The **Security Advisories** page provides a full list of applicable Security Advisories along with their impact, a synopsis, component, number of impacted systems, and publish date.”
 - d. **Alerting via email subscription:** “The **Notifications** tab allows users to subscribe to email notifications for various events such health change notifications, job status change notifications, cybersecurity risk notifications, and ransomware incident notifications.”
 - e. **Alerting pushed to third-party tools:** “The Webhooks feature is a push mechanism to integrate with third-party applications such as ServiceNow and Slack.”
 - f. **Remediation from within the security view:** “Selecting one or more issues in the list and then clicking the Resolve button resolves those issues after the user confirms the action in the verification window.”
 - g. **Ransomware incident detection:** “Ransomware Incidents enables users to monitor for cybersecurity ransomware incidents in near real time.”

Policy-Based Security Configuration

This section outlines the steps taken to confirm support for policy-based security in the AIOps platform.

1. Review [Dell AIOps: A Detailed Review](#) (pages 79–83), noting the following passages:
 - a. **Cybersecurity:** “Dell AIOps compares configurations and setups to a set of security-related evaluation criteria, notifying users of any deviations from the configured plan.”
 - b. **Misconfiguration settings:** “The **Misconfiguration Settings** page, accessed through the gear icon on the Misconfigurations page, is where users enable, disable, and configure the tests in the Evaluation Plan.”
 - c. **Systems:** “The Systems tab lists the Cybersecurity-enabled systems. It includes information such as the associated template, status of the evaluation plan, number of selected tests, custom tags, and the last time the evaluation plan was updated. From this page, Cybersecurity Admins can assign or unassign templates to systems, enable or disable the evaluation plan for systems, or edit the evaluation plan for an individual system.”
 - d. **Templates:** “The **Templates** tab lists the configured templates and allows users to create templates and view, edit, and delete existing templates. A template contains a list of configured tests which can be assigned to multiple systems of the same product technology.”

Multiple Performance Reports

This section outlines the steps taken to confirm support for customized reporting in the AIOps platform.

1. Review [Dell AIOps: A Detailed Review](#) (pages 71–78), noting the following passages:
 - a. **Central reporting hub:** “The **Report Browser** is accessed from the Create/View My Reports menu. It acts as a user’s reporting workspace and dashboard. It allows users to create, view, and modify reports. Reports can be scheduled, duplicated, bookmarked, and exported in PDF format. Reports can consist of any combination of tables and line charts.”
 - b. **Report content categories:** “When adding a table to a report, the user can select one of the following categories: ... Server, Server Firmware.”
 - c. **Column customization:** “When the user selects the Category, a list of available and selected columns is displayed. Dell AIOps prepopulates the report with common columns. The user can either drag and drop or double-click a column name to add or remove it.”

- d. **Performance metrics in line charts:** “A line chart requires the user to select the Product and Category. ... After choosing the objects, the final step is to choose the metrics. ... Metrics available for line charts are shown in Appendix D: Report Browser metrics.”
- e. **Scheduling:** “Schedule the report. Choose an initial runtime and one of the following intervals: Daily, Weekly, Biweekly, Monthly, or Quarterly. Choose a format of PDF or CSV. Enter email addresses for recipients.”

Performance Metrics with Anomaly Detection

This section outlines the steps taken to confirm the presence of performance metrics with anomaly detection.

1. Review **Dell AIOps: A Detailed Review** (pages 15, 155, and 156), noting the below passages:
 - a. **Anomaly detection:** “Using machine learning and analytics, Dell AIOps identifies performance anomalies It compares current performance metrics with historical values to determine when the current values deviate outside of normal ranges.”
 - b. **Anomalies highlighted in charts:** “Performance anomalies are highlighted in the charts as dark blue shaded areas.”
 - c. **Forecasting charts:** “Dell AIOps also provides performance forecasting charts for PowerEdge servers. The forecasting charts are available for: CPU Usage, Memory Usage, System Usage, IO Usage.”
 - d. **Predicting resource exhaustion:** “Dell AIOps uses predictive analytics to understand the historical trends and usage and determine when these resources will reach their maximum value.”

GPU Utilization and Visibility

This section outlines the steps taken to confirm the ability to access server-level metrics for GPUs.

1. Review **Dell AIOps: A Detailed Review** (pages 154 and 211), noting the following passages:
 - a. **Per-GPU utilization metrics:** “For servers, the first chart on the tab shows the GPU utilization for each GPU in the system. Color-coded lines graph the usage for each GPU for the past 24 hours.”
 - b. **Near-real-time GPU:** The GPU – Line Charts table shows “Usage (%Avg. over last 15 min).”

Carbon Footprint Analysis

This section outlines the steps taken to confirm the ability to analyze the carbon footprint of running systems.

1. Review **Dell AIOps: A Detailed Review** (pages 44–46), noting the following passages:
 - a. **Carbon footprint summary:** “The **Carbon Footprint** page provides summary, system, and workload level metrics for carbon emissions and energy usage.”
 - b. **Calculated rather than static:** “Carbon emissions calculations are based on location-specific emission factors provided by the International Energy Agency (IEA) and industry average Power Utilization Effectiveness (PUE) values. Users with the Admin role can override these default values by clicking the Settings button.”
 - c. **Year-to-date usage:** “At the bottom of the page is a table listing each system, location, YTD energy usage, energy forecast, YTD carbon emissions usage, carbon emissions forecast, and daily power consumption.”
 - d. **Emissions forecasting:** “Clicking the details icon for a system displays seven-day charts for energy consumption and carbon emissions ... Selecting the Forecast option shows trend and forecast data for each of these charts.”

Feature	Dell management tools		Vendor K management tools	
System Lockdown		✓		✗
Access control		✓		✓
Cybersecurity advisories		✓		✓
Policy-Based Security Configuration		✓		✓

Figure 1. Comparison of Dell and Vendor K essential security features

Referenced Documents

The following documents were used in our evaluation:

[OME User Guide](#)

[Dell AIOps: A Detailed Review](#)



Legal Notices and Disclaimers

The analysis in this document was done by Prowess Consulting and commissioned by Dell Technologies. Performance results are based on Prowess Consulting's testing using the configurations shown here. Any difference in system hardware or software design or configuration may affect actual performance. Prowess and the Prowess logo are trademarks of Prowess Consulting, LLC. Copyright © 2026 Prowess Consulting, LLC. All rights reserved. Other trademarks are the property of their respective owners.