opentext™

What's new in OpenText ZENworks Suite?

Unified endpoint management and protection for your Windows, mobile, Mac, and Linux devices

Benefits

- Streamline endpoint management
- Improve productivity for remote workers
- Protect data across all endpoints
- Reduce licensing costs and security risks

Every OpenText™ ZENworks™ Suite release brings a host of new features. Here is a sampling of the new features released in ZENworks 2020 Update 3, ZENworks 23.3, ZENworks 23.4, and ZENworks 24.2.

Azure AD as a user source

Many customers are now using Azure Active Directory® (AAD) as a directory source for users and devices in their environments. In such environments, devices are joined to AAD and users log in to their devices with their AAD credentials. Version 23.3 adds support for AAD as a user source within ZENworks.

With this capability, a ZENworks administrator can assign a bundle or a policy to a AAD user or group. When an AAD user logs into an AAD joined device, ZENworks pulls down bundles and policies based upon the identity of the logged in user, like what currently happens with Active Directory/E-Directory sources. Additionally, a user-assigned bundle or policy follows an AAD user across AAD joined devices.
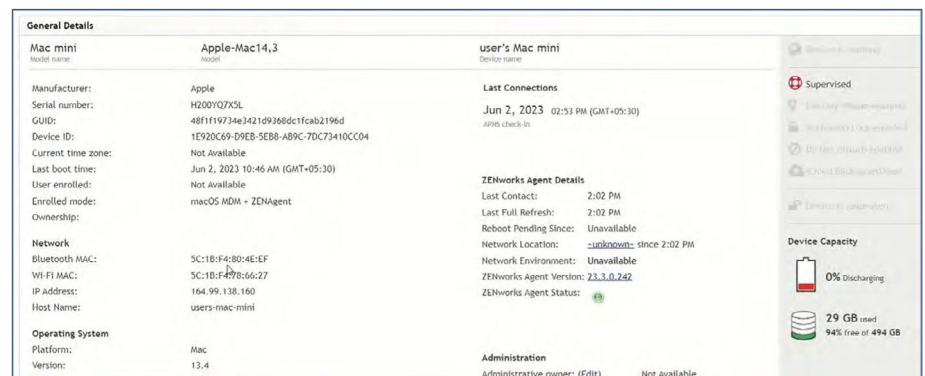
Mac device managed via ZENworks Agent and MDM

Management of Mac device via MDM

Many management capabilities on a Mac® device are better done via MDM. ZENworks 23.3 introduces limited support for managing Mac devices via MDM and subsequent ZENworks releases extend that support. These releases include the following capabilities:

- 23.3 Enrolling Mac devices via Apple's Automated Device Enrollment (ADE)
- 23.3 Provisioning Mac devices via download and installation of an enrollment profile
- 23.3 Dual management of Mac devices via ZENworks agent and MDM, while still retaining a single view (screenshot above)
- 23.3 Deploying configuration profiles and commands to managed Mac devices

- 23.4 Provisioning applications from an Apple Volume Purchase Program (VPP) account to Mac devices
- 23.4 Unenrolling, retiring, and deleting Mac devices
- 24.2 Enforcing registration rules during device enrollment
- 24.2 Supporting removal options when a device is lost

Enhanced security for ZENworks

For many of our customers, ZENworks is a core IT solution at the center of their endpoint management strategy, serving as a gateway to all endpoints in the organization. A gateway like this needs to be protected against malicious actors. OpenText is continually working to enhance the security posture of ZENworks. Here are two things we have done recently:

1. Multi-Factor Authentication for ZENworks Control Center (ZCC)—ZCC is a window to your ZENworks zone, and it is imperative to ensure that only authorized people can access it. ZENworks 2020 Update 3 introduces a built-in capability for two-factor authentication during ZCC login. This is achieved by integrating ZENworks with OpenText™ NetIQ™ Advanced Authentication via a "Limited" entitlement covering common multi-factor authentication methods.

2. API Gateway—ZENworks 23.3 introduces the API Gateway, a ZENworks server gateway service that listens to requests on port 443 (or a customized port) and routes them to the correct ZENworks service. The API Gateway provides greater security for public facing ZENworks servers and cloud environments

Remote Management updates

The Remote Management viewer (the one used by administrators to view the session) has been completely overhauled to be much faster and more stable. It also has some nifty enhancements built into it, including:

1. Chat with session participants—It is now possible to chat with an end user or other session participants right from the Remote Management viewer. This chat can also be audited and viewed later.

2. Recording Remote Management sessions—Starting with ZENworks 2020 Update 3, it is possible to record a Remote Management session. The recorded session is stored on the ZENworks server as part of the ZENworks Audit and can be converted into an mp4 file for later downloading and viewing. ZENworks 23.4 adds the policy option to automatically start session recording.

3. Re-connect an RM session after reboot—ZENworks 2020 Update 3 provides the capability to automatically re-connect a Remote Management session after the reboot of an end user's device. If a device reboots within a set time period (configurable), an ongoing Remote Management session automatically reconnects itself, thus sparing you the hassle of calling up a user and trying to re-establish the connection.

Next generation Patch Management

OpenText™ ZENworks Patch Management provides both policy-driven maintenance patching and tracking and remediation of critical known vulnerabilities using Common Vulnerability and Exposure (CVE) IDs. Keeping all the same excellent administrative workflows, ZENworks 2020 Update 3 adds:

- Faster scanning on managed devices to detect applicable patches and their status (installed/not installed).
- A new patch feed with an actively growing catalog of third-party and operating system patches.

- On-demand streaming of patch content if it is not available on the target Content Server.
- Automatic cleanup of unused patch content from Content Servers.
- Decreased amount of patch data stored in the ZENworks database. Each patch is no longer represented by a bundle in the database.
- A new patch microservice running on each Primary Server to handle patch processing and patch-related tasks.
- Mainstream support for issues, new patches, and new platforms.

ZENworks 23.4 adds the following capabilities:

- Generating predefined and ad-hoc patch reports through ZENworks Reporting using the ZENworks domain.
- Generating ad-hoc patch reports through ZENworks Reporting using the Vertica Patch domain.

Note: The new patch management solution requires administrators to perform a migration from the legacy patch management solution. The patch migration is not part of the system update, allowing administrators to complete the system update on all Primary Servers and Satellites before transitioning to the new patch management solution.

Basketful of customer ideas!

In every release, we bring into ZENworks a host of enhancements requested by our customers. Here are select few ideas spread across ZENworks 24.2, ZENworks 23.4, ZENworks 23.3, and ZENworks 2020 Update 3:

1. Zero-touch enrollment of Samsung Android ™ Devices—added in ZENworks 24.2.
2. Device log collection—ZENworks 24.2 lets you collect log files from a device via a Quick Task in ZCC.
3. Bundle copy and export—ZENworks 24.2 lets you specify a destination folder when copying a bundle and name the export file when exporting a bundle.
4. Windows® 11 readiness—ZENworks 23.4 lets you see which Windows 10 devices meet the requirements to upgrade to Windows 11.
5. ZENworks application navigation— ZENworks 23.4 supports navigating between folders in the non-tree view.
6. Pin your favorites—ZENworks Control Center (ZCC) provides an easy way to jump right back into an object by displaying a running list of recently used objects. It is now possible to pin one object or more in the list, so that you can keep coming back to it as many times as you like.
7. Display of ZCC sessions—Discover who else is logged in to ZCC. A new section within diagnostics displays active ZCC sessions and their duration.
8. Additional device attributes—It is now possible to view the network location and network environment of a device right on the device summary page. This data is updated as and when a network change happens for a device. This data is also available as a search filter apart from being exposed as part of Inventory reports. Information about when the device last rebooted and if a reboot is pending on a device is also displayed and reported.

Additional information added to the device Summary page

9. More bundle details—Starting with ZENworks 2020 Update 3, the Bundle Summary page now includes information about which administrator created a bundle, who modified it, and when. This information is supplemented by improved searchability for disabled and sandbox bundles and the ability to look up a bundle based on its GUID.

10. Email notification of detected malware threats—ZENworks 23.3 introduces the ability for select administrators to receive email notifications whenever ZENworks Endpoint Security Antimalware detects a malware threat on a device.

11. Easily view complex system requirements—In ZENworks 2020 Update 3, a simple tool has been added that displays the system requirements in an easy-to-understand manner. This tool is not just limited to bundles, but also extends to advanced device search and dynamic group creation wizard.

12. Enforcement of individual patch policies—ZENworks 23.3 provides the ability to apply different patch policies at different times, rather than all policies at one time. This gives administrators the opportunity to apply critical policies more frequently or at different times than non-critical policies.

This list doesn't encompass the full breadth of features that have been added to ZENworks. For more details, check out the ZENworks Version Comparison Chart or What's New section of ZENworks documentation.

Easily view complex system requirements

opentext™