



Visionary360.com | 1(818) 459.3950
Consulting@Visionary360.com

RMM Environment Health Checklist

Client & Company Cleanup

- **Inactive Clients** - Remove companies that are no longer active to prevent license waste and reduce alert noise.
- **Endpoint Removal** - Delete all computers, servers, and devices associated with terminated clients.
- **Custom Configurations & Automation** - Remove client-specific monitors, scripts, and policies that are no longer needed.

User Access Review

- **Former Employees** - Disable or remove accounts for staff who have left your organization.
- **Inactive Client End Users** - Clean up user accounts for employees at client sites who are no longer with the company.
- **Unused Integration Accounts** - Remove service accounts for integrations that are no longer in use.
- **Test Accounts** - Delete temporary accounts created for testing that may have been forgotten. These accounts are another security vector open to attack.
- **Administrative Account Audit** - Review who has admin access and ensure it's still appropriate.
- **Multi-Factor Authentication** - Verify MFA is enabled for all accounts.
- **Service Account Passwords** - Update passwords for automated service connections and integrations.

Agent & Monitoring Verification

- **Agent Health Check** - Identify agents that haven't checked in or are reporting incorrect data.
- **Communication Verification** - Confirm agents are successfully communicating with the RMM server.
- **Alert Functionality** - Test that monitors are triggering and creating tickets.
- **Threshold Tuning** - Review alert thresholds to reduce false positives.
- **Critical Monitor Validation** - Ensure your most important monitors are working correctly.
- **Automation Execution** - Check that scheduled scripts and auto-remediation are running.
- **Failure Alert Testing** - Verify that you are notified when monitors themselves fail.

Scripting Verification

- **Scheduled Script Review** - Confirm automated scripts are still relevant and functioning.
- **Rogue Script Detection** - Look for unauthorized or forgotten scripts running in the background.
- **Permission Audit** - Ensure only appropriate users can modify or execute scripts.
- **Organization Check** - Verify scripts are properly categorized and easy to find.

Platform Maintenance

- **Plugin Updates** - Install security patches and feature updates for add-ons.
- **Deprecated Feature Management** - Address functionality that's being phased out by the vendor.
- **Platform Patching** - Keep the RMM platform itself updated with latest releases.
- **License Optimization** - Review license usage to avoid paying for inactive endpoints and ensure there are enough available licenses for the next client onboarding.
- **Deprecated Plugins** - Check for outdated add-ons that may pose security risks.

Documentation and Process Improvement

- **Issue Logging** - Record problems discovered during each health check.
- **Time Tracking** - Document how long issues take to resolve for process improvement.
- **Root Cause Analysis** - Identify why problems occurred and implement preventive measures.
- **Process Refinement** - Continuously improve the health check process based on findings.