Updated 01/30/2019

Regular Maintenance Tasks

These tasks should be performed on a regular basis to ensure that all automation and maintenance is functioning properly. The New Customer or Site section will remind you of the tasks that are critical to define to ensure that the automation is working as designed. Most tasks take just a few minutes but go a long way in simplifying operations.

After VSA Patches

After any VSA patch or upgrade, check the Latest Agent Version on the Manage Agents screen:

Latest agent version available: 9.5.0.8

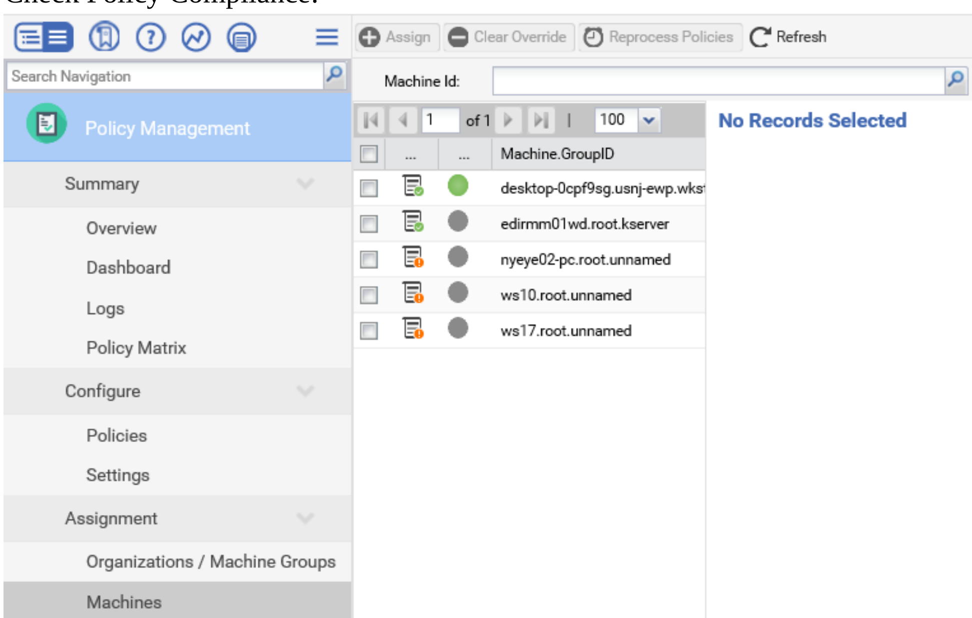
Update the following views: _!_Agent - Agent Version is Current, _!_Agent - Agent Version is Outdated, and XARC_AgentVersion-Outdated. Select each of the views in the View Definitions editor, click the Define Filter button, then update the Agent Ver field (usually only the last 1-2 digits unless there is a version upgrade).

Agent Ver (number only-4050002) < 9050008

The version number is defined as a main number with no leading zero, then the three minor release numbers with leading zeros to make each value be represented as two digits.

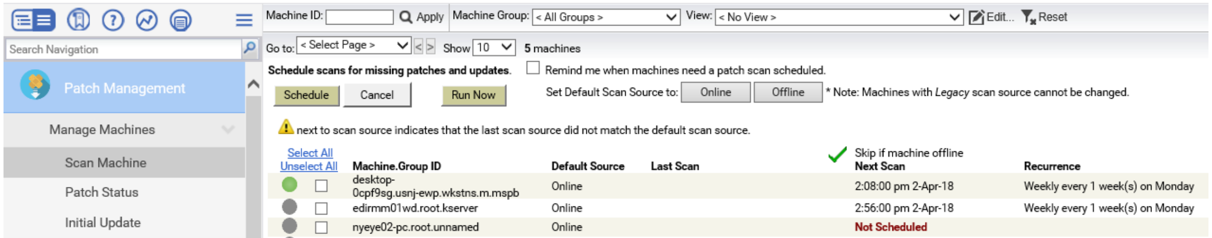
Weekly Tasks

- Check Policy Compliance:



  - Navigate to **Policy Management – Assignment – Machines**
  - Look for agents that have overrides (orange) or non-compliant settings (red) – use the column filter to simplify the search.
  - Select the agents with Overrides, then click **Clear Overrides**
  - Select agents that are non-compliant, then click **Reprocess Policies**
    If the same agents repeatedly report non-compliance, investigate which settings are in conflict and adjust the policies or policy application. Request support assistance if necessary.

- Check the Patch Scan schedule:
  Spot check a group of machines or a couple of organizations.



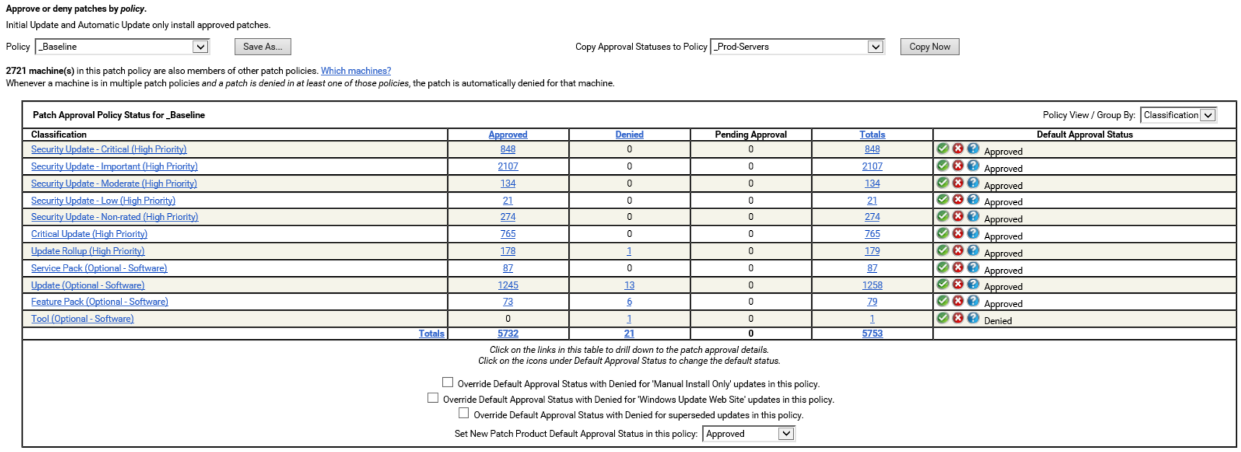
  - Verify that each agent has a scan schedule applied – these times may be different if you customized the patching module.
    - Workstations – Every Monday between 10 AM and 4 PM
    - Servers – Every Monday between 12:30 AM and 4:30 AM
    - Systems without scheduled scans – verify the reason – unmanaged or special group, PATCH setting in the Policy Control field?

- Review/Adjust network monitors (if used):
  - Navigate to Network Monitor – Monitoring – View
  - Check groups with RED status
    - Drill down and select the agent with Alarm status
    - Note the state of the monitors prefixed with "_Monitor:" – if *all* of these monitors are red, it usually indicates a local security issue. Run the **WIN-Verify WMI for KNM Monitoring (MV)** procedure on the affected machine.
    - If the affected machine is the KNM Gateway (listed as "Hostname" on the overview display), make sure that WMI is Disabled (Select the agent, click Edit, select the Advanced tab, un-check **Use WMI**.)

Monthly Tasks

This task will take 20-45 minutes each month, depending on the number of updates that were released and the amount of time required to determine if any update will impact your customers.

Review and Approve Patches by Policy



Approve or deny patches by *policy*.

Initial Update and Automatic Update only install approved patches.

Policy _Baseline Save As... Copy Approval Statuses to Policy _Prod-Servers Copy Now

2721 machine(s) in this patch policy are also members of other patch policies. Which machines?
Whenever a machine is in multiple patch policies *and a patch is denied in at least one of those policies*, the patch is automatically denied for that machine.

Patch Approval Policy Status for _Baseline Policy View / Group By: Classification

Classification	Approved	Denied	Pending Approval	Totals	Default Approval Status
Security Update - Critical (High Priority)	848	0	0	848	Approved
Security Update - Important (High Priority)	2107	0	0	2107	Approved
Security Update - Moderate (High Priority)	134	0	0	134	Approved
Security Update - Low (High Priority)	21	0	0	21	Approved
Security Update - Non-rated (High Priority)	274	0	0	274	Approved
Critical Update (High Priority)	765	0	0	765	Approved
Update Rollup (High Priority)	178	1	0	179	Approved
Service Pack (Optional - Software)	87	0	0	87	Approved
Update (Optional - Software)	1245	13	0	1258	Approved
Feature Pack (Optional - Software)	73	6	0	79	Approved
Tool (Optional - Software)	0	1	0	1	Denied
Totals	5732	21	0	5753	

Click on the links in this table to drill down to the patch approval details.
Click on the icons under Default Approval Status to change the default status.

☐ Override Default Approval Status with Denied for 'Manual Install Only' updates in this policy.
☐ Override Default Approval Status with Denied for 'Windows Update Web Site' updates in this policy.
☐ Override Default Approval Status with Denied for superseded updates in this policy.

Set New Patch Product Default Approval Status in this policy: Approved

- Navigate to Patch Management – Patch Policy – Approval by Policy
- Select each Policy from the drop-down list
- Select any classification from the Pending Approval column, select all patches from the approval window, and either approve or deny as per the Default Approval Status column. These are patches that have been discovered on agents after the auto-approval period and require manual approval or denial.
- Select the classifications where the default status is ‘Pending Approval”
    - Review the updates, looking for any that should be denied. Select these and click Deny.
    - Select All remaining updates and click Approve
- Repeat for each policy in the drop-down list that has pending approvals.

Use the filter to focus on what you need to select. Set the “Published” field to something like < "20180430" to exclude updates from the current month (set to the end of the prior month) – giving you time to listen for problematic updates before you approve them. The Security Bulletin field can also be filtered to look for things like “.Net” or “IE” depending on the policy you are validating. Search for .NET in the Block DotNET policy and deny all updates found, then you can safely clear the filter and approve all remaining updates for that policy.

Spot Checks – Monthly

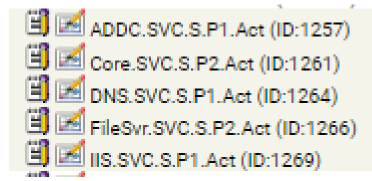
These checks should take 10-15 minutes each month to ensure the automation is being deployed properly.

Verify Configuration Steps were followed

- Review the steps for new customer or site and insure that all settings are defined properly, particularly for Managed Variables and Monitor – New Agent Check-In as these are particularly important to automation. These are easy to spot and will indicate which customers or groups might not have been fully configured when created and need further validation.
- Ensure that all agents are in proper groups. Search for agents that are directly in the "unm" group and move them to the correct sub-group. Any agent in the unm group *will be managed*, which will lead to unexpected operations on these endpoints.

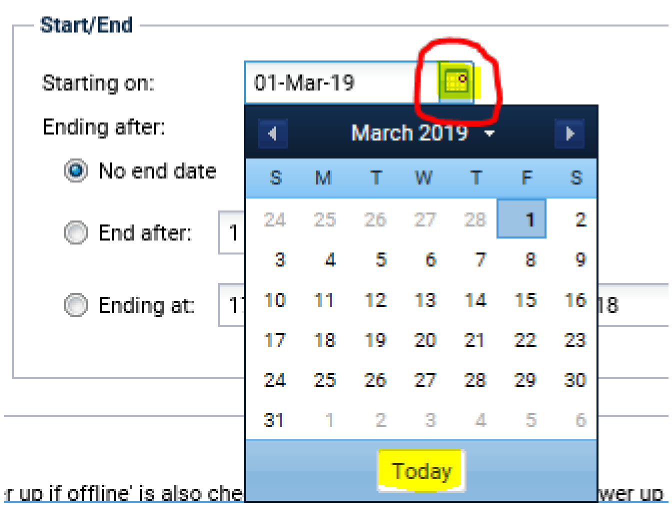
Verify Monitoring and Automation

- Confirm monitoring via spot-checks
  - Navigate to Monitor – Agent Monitoring – Assign Monitoring
    - Select an "All Servers – Windows" view
    - Verify that appropriate monitors are applied – several monitors will usually be present on servers, as shown here.



    - Service monitors are optional on workstations and may or may not be present. This is MSP-specific and should be noted as part of your specific checks.
  - Navigate to Monitor – Agent Monitoring – Event Log Alerts
    - Verify that all agents have appropriate monitors applied.

    Note that agents in a special, audit, or unm group will not have monitors applied. Monitors can also be suppressed via Policy Control settings. Verify that systems without monitors have these controls in place or determine why monitors are not applying as expected. Request support if needed to ensure that effective monitoring is being performed.
- Verify that the Daily Tasks and Patch Scans and Updates are scheduled on endpoints. Reprocess the policies and check again if they are not.
  In some cases, VSA will not accept the scheduled start date of the scheduled events and thus refuse to schedule the procedures on many if not all endpoints. When this occurs, simply edit the procedure, edit the scheduled event (procedure or patch object), then set the Start date by clicking the calendar icon and click on the Today button in the displayed calendar. Save and Apply the policy change. This refreshes the start date without any effective change to the schedule itself and almost always resolves the problem.



Creating a New Customer or Customer Site

These steps are needed to ensure that all automation functions after adding a new customer or a new location (site) to an existing customer.

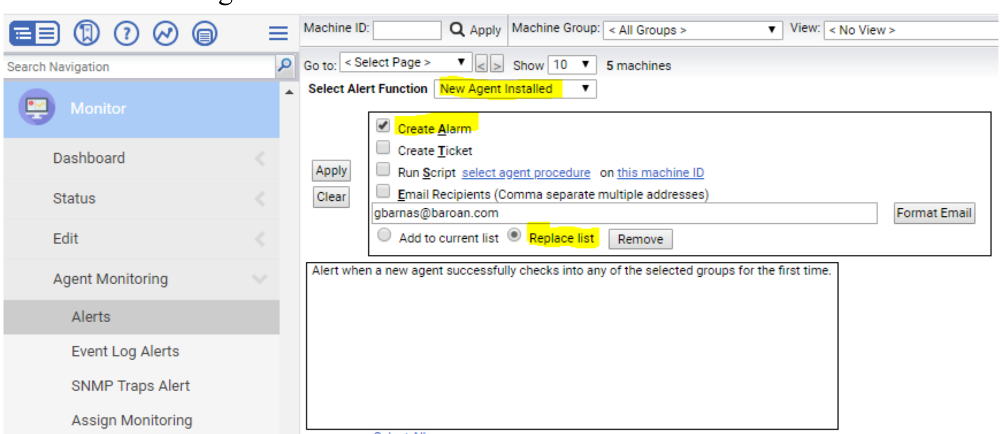
New Customer

Use the Offline Management tool to automatically create the customer organization and site group(s) – this will automate the first 4 steps below. *Using the Offline Management Tools is the preferred method! See the additional instructions at the end of this section for use of the offline tools.*

- *Create the root group – "m" for managed or "unm" for unmanaged or break/fix.*
- *Create the servers, wkstns, and special machine groups below the customer root.*
- *Use the LOCODE.XLSX spreadsheet to determine the Site ID, create the Site ID group(s) under wkstns and, if necessary, servers. Use the optional offline tools for automated management.*
- *Assign the proper Set-up Type to define the coverage hours for monitoring/alerting.*
- Optional – define the MSP Identity in the Org Custom Fields / MSP field to use custom ITP processing and notification via Tenancy. If this is done, the alerts will be sent to an alternate PSA as defined by ITP.
- Add the organization to the Personal (or MSP) scope; optionally create a Customer-name scope to restrict customer access to this specific organization.
- Optional – If the customer wants to be notified of priority events, create a Staff Member for that customer; define the Function field as "PriNotify", and (due to a VSA bug), enter the notification email address into the Email Address, Phone Number, and Text fields.
- Complete the New Site(s) tasks below when creating a new org.

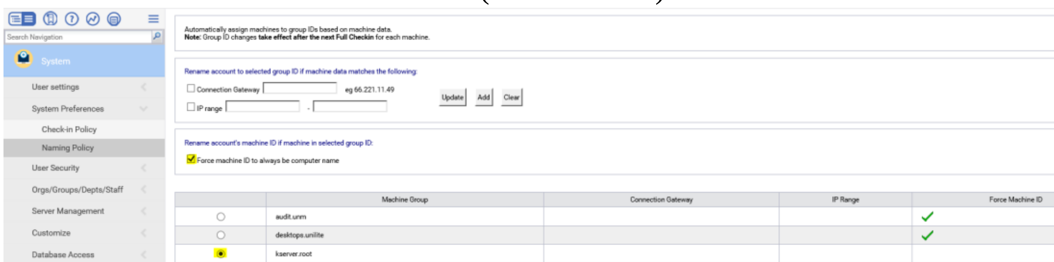
New Site(s)

- Define the New Agent Installed action as "Create Alarm"



  - Navigate to **Monitor – Agent Monitoring – Alerts**
  - Select **New Agent Installed**
  - Select **Create Alarm**
  - Select **Replace list**
  - Choose **Select All**
  - Click **Apply**

- Define the Managed Variables for the new customer and site group(s). Other variables may be required by the client for local customer credentials and various application licensing used by installation procedures.
    - Navigate to **Agent Procedures – Manage Procedures – Schedule/Create**
    - Click the **Manage Variables** menu
    - Define the following required variables:
        - RAUserID The local admin user ID used by the MSP
        - RAPassword The local admin account password used by the MSP
        - Define the CA user ID and Password if required by customer request
- Force Machine ID to Follow HostName (recommended)



    - Navigate to **System – System Preferences – Naming Policy**
    - Select the machine group
    - Check **Force machine ID to always be computer name**
    - Click **Update**
    - Repeat for each machine group
- Verify that the agent init process has run after installing the agent.
    - Navigate to **Agent Procedures – Manage Procedures – Schedule/Create**
    - Expand the **_MSP Builder/Core Automation/Agent Init** folder
    - Check the Last Exec Time for **ALL-Agent Onboarding - 1 – Init**
    - If the procedure has not run, invoke it manually. The procedure may not run automatically if the agent previously checked into the system

Offline Management Tool – Org & Group Management.

The offline tools allow a simple management method that provides a consistent configuration. These should be used whenever possible to create new organizations or location groups for existing organizations. The scripts and data files should be located on a local file share, as the applications will not run and access data from most cloud-based storage platforms (Google Drive, SharePoint, etc.).

Open the CustomerLocations.xlsx spreadsheet. Scroll to the end of the worksheet to add the customer org or site.

For a new organization:

- Complete the Customer ID, Name, City, State, Country, M or UNM, and C-Type fields. See the Instructions tab in the spreadsheet for further information.
  - The City must be spelled correctly. Common issues are hyphen/space, abbreviations (St. vs Saint). When in doubt, open and review the LOCODE.xlsx spreadsheet.
  - C-Type can be blank to default to Standard coverage.
  - W/T/S/P can be blank – this will create the site group under both Servers and Workstations. Do not enter the slashes into the data field. If you specify any value other than "P" in this field, you must explicitly define all agent types:
    - "S" creates a site group below the Servers group
    - "W" creates a site group below the Wkstns group
    - "T" creates the TClients group if not present, then creates a site group below TClients. This is used to separate thin-client systems, which often require special methods for updating or configuration changes.

For new sites for new or existing organizations:

- If the customer has multiple locations, duplicate the Customer ID and Name values, then define the remaining fields to uniquely identify the location. The Customer ID and Name must be the same for all locations associated with a customer organization!
  - If this is a second location in the same city/state, provide a custom ID tag in the "Other" column.
  - Perform this step if you are adding a new location to an existing customer.

Save and close the spreadsheet, then run the GenSiteCodes script. Note any locations that failed to be identified – these are often misspellings or are defined slightly differently in the LOCODE spreadsheet. If the location does not exist in the LOCODE spreadsheet, you can either use an alternate location that does exist, or define your own code. If you create a code that follows the LOCODE standard, make sure it does not already exist! Re-run the GenSiteCodes script if you made corrections to city names.

Open the spreadsheet and verify the Code column contains Site-ID data. For any customer with multiple locations in the same city, edit the site code that was generated and add the identifier that you defined in the Other column. We suggest using a "-locn" format – a dash followed by a short location qualifier, based on the site's purpose or street name. Save any changes and close the spreadsheet.

Run the CreateOrgGrps script to create all of the organizations and locations not already defined in the VSA.