Lithik Security Manager
Quick Start Guide

Table of Contents

Getting Started 1
- Hardware Requirements 1
- Bare Metal Installation 1
- Registration and Credentials 1

Initial Setup 2
- General Settings 2
- Network Configuration 2
  - Networks 2
  - Exclusions 3
  - Cache Servers 3

Configuring Automation Policies 4
- Managing Policies 4
- Default Policies 5
  - Scan Everything 6
  - Reboot 6
  - Update Everything 6

Alert Policies 9
- Configuring Alerts 9
- Configuring Alert Recipients 10

614.890.0026 | support@lithik.com | 635 Park Meadow Road, Suite 208, Westerville, OH 43081

Getting Started

The Lithik Security Manager (LSM) can be set up in any of three ways: pre-installed on an appliance provided by Lithik, downloaded as a virtual machine (*https://www.lithik.com/downloads*), or a bare metal installation onto hardware of your choosing. In all cases, a rule must be added to your firewall allowing the LSM to contact scvpn1.lithik.com (currently 199.182.189.106) using UDP port 1194. For bare metal installations, please follow all of the instructions listed below. To set up a physical appliance or a downloaded virtual machine, please skip to the **Registration and Credentials** section below.

Hardware Requirements

- Computer with 64-bit processor, at least 4GB of memory, and hard drive with at least 36GB of space
- LSM Installation media (USB drive received in mail)

Bare Metal Installation

1. Connect the computer to power, a keyboard, and the LSM installation media. Disconnect any ethernet cables or any other USB storage, to avoid booting the Laptop from the wrong media.
2. Boot from USB. This may require a modification of boot order in the computer's BIOS.
3. Start the installer, choose the hard drive that the LSM should be installed to (36GB minimum), and wait for the installation to complete. This may take 5-10 minutes.
4. When the copy is finished, remove the USB drive and press the enter key.

Registration and Credentials

Unless you are certain that the LSM's default IP address of 192.168.1.1 does not conflict with anything on your network, make sure that no ethernet cable is connected. Turn on the LSM. After the machine fully boots, a status screen appears. Type ALT-F2 to display the login screen. Log in using the default credentials of admin/admin.

Enter the IP and DNS settings for the appliance. Configure the appliance's network settings, choosing values suitable for your LAN. If you have chosen not to use DHCP, you will need the following information:

- The fixed (static) IP address you have assigned to the appliance
- The netmask for that static IP address
- The IP address of the LAN gateway (the default route)
- The primary and secondary DNS server IP addresses

Once the initial settings are entered, connect the LSM's ethernet cable (or enable the ethernet interface, in the case of a virtual machine). Use a web browser to connect to the appliance's local configuration interface at *https://IPADDRESS:8443*, using the IP address you selected in the previous step. Log in with the same default credentials of admin/admin as before. It is recommended that you change these credentials after logging in.

Click **Enter License Key**, then type or paste the license key you were provided. This registers your device with the LSM cloud. If this step fails, the error messages provided should help you discover and correct the problem.

Under **Windows Credentials**, enter the username and password of an administratively privileged Windows account for use by the LSM appliance. For the username, use the standard format: DOMAIN\USERNAME. Note that these credentials can only be configured from the local interface, and will never be transmitted to the cloud.

Initial Setup

Log in to the LSM interface, located at the IP address you set, but without the ":8443", as follows: *https://IPADDRESS*. At the LSM login screen, enter "admin" for the username and your license key as the password. You will be prompted to create a new password for the admin account, and then the Home screen of the LSM will be displayed.

The Lithik Security Manager has a series of "tabs" across the top. The **Administration** tab contains a variety of links you can use to configure the system to properly interact with your network and devices. Both the **General Settings** and **Network Configuration** sections must be filled out for the LSM to function properly.

General Settings

Configure the **Customer Name**, **Internet Domain Name**, **Patch Management**, and **Time Zone** settings. Other settings are optional.

Setting	
Customer Name	The name of your company, such as "Lithik Systems, Inc."
Internet Domain Name	E.g. lithik.com; after the LSM scans the domain, WHOIS information will be available here.
Alerts "From" Email Address	If you configure email alerts, this is the address they will be sent from. This is not a required setting. If this field is left blank, alerts will come from *alerts@lithik.com*. Make sure your spam filter allows email from this address.
Patch Management	Choose the vulnerability scanning software you have decided to use.
Inject LSM DNS Record	Setting this to 'Yes' will allow machines on the local network to access the LSM at lsm.lithik.com, rather than only by IP address.
Remote Access (alt-click) prefix	Throughout the LSM, clicking an IP address while holding the "alt" key will open a direct connection to the client machine using programs such as Windows Remote Desktop or VNC. Use this setting to configure the connection address. The default setting of rdp:// will attempt to open a connection through your local Windows Remote Desktop client. This is not a required setting. **Note: This feature requires setup on the local computer to handle the selected URL type.**
Time Zone	Choose the time zone for the LSM.
Nexus Access	Allow this LSM to be managed by a Lithik Nexus multi-site administrator.
Lithik Customer Support Access	This setting will grant Lithik Systems customer support staff the ability to log in to your LSM to fix problems or gather statistics for building new features. You can disable or enable it at any time.
Notes	This section is completely for your own benefit. If there's something you need to remember about this LSM or network, jot it down here.

Network Configuration

Networks

Enter each subnet you manage with the LSM using the format IP-address/netmask-size. The netmask size is the number of one bits in the netmask. For example, since each of the four numbers in an IP address is made up of 8 bits, the netmask size of 255.255.255.0 is 24 and the netmask size of 255.255.0.0 is 16. Entering 192.168.1.0/24 will scan all IP addresses matching 192.168.1.*. You may also target a single address by appending /32 to the IP.

Network	Scan Interval	Label	Primary Cache	Secondary Cache	Fallback	
192.0.2.0/29	5 minutes	Office Cable 1	None	None	Lithik Scanner	
198.51.100.0/32	5 minutes	Office Cable 2	None	None	Lithik Scanner	
192.168.1.0/24	5 minutes	Colo LAN	None	None	Lithik Scanner	
10.10.1.0/24	5 minutes	Office LAN	DT1	DT2	Lithik Scanner	
203.0.113.0/27	5 minutes	Colo Public	None	None	Lithik Scanner	
Create New Network						

The LSM will only interact with devices on networks configured in this table. Note that you are able to scan the public addresses of your own network, but be sure you do not scan public addresses that you do not own, as this could be interpreted as a cyber-attack. Each network can also be configured to use one or more cache servers, which are configured in the **Cache Servers** section discussed below.

Exclusions

The exclusion list can contain individual IP addresses as well as subnets, formatted as above.

Exclusion	Label	
10.10.1.117	RICOH Aficio	
10.10.1.161	Office Epson	
Create New Exclusion		

If a machine is excluded, no packets will be sent to it from the appliance, although it will be included in the inventory if information can be found indirectly, such as through an ARP scan by a non-excluded machine. Add fragile machines to this list if scans prove to be disruptive (such as causing your printer to print blank or gibberish pages), but remember that no vulnerability scanning or mitigation will occur on excluded devices.

Cache Servers

The default behavior for applying third party patches is to copy patch files across the network from the LSM as needed. While this works well for machines with high-speed connections to the LSM, it can generate a lot of traffic to remote sites, as some software packages have very large patch files. To reduce such traffic, you can select a Windows machine of your own to host local copies of large patch files so that they only need to be transferred to a remote network once.

Cache Server	Disk Allocation	Status	
DT2	2 GB	0.12 GB	
DT1	2 GB	0.98 GB	
Add Cache Server			

The patch file will be copied to the cache server the first time it is needed by a machine near it. Files will accumulate up to the limit configured under Disk Allocation, at which point the least recently used files will be removed.

Configuring Automation Policies

One of the most powerful features of the LSM is its ability to automate tasks that are traditionally the least enjoyable part of IT work. Doing vulnerability scans and applying missing patches is hugely important, but is a substantially mechanical process. If it's a mechanical process, why not have a machine do it for you? The LSM allows vulnerability scans, patch application, vulnerability remediation, and a variety of alert categories to be configured with a policy that dictates what you want done, what machines you want it done to, and when you want the work to happen.

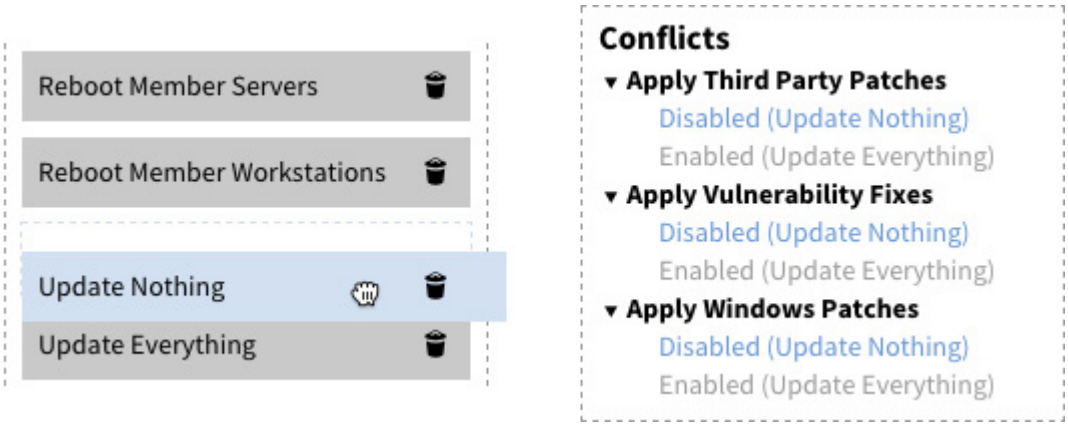
For your first month using the LSM, it is advisable to schedule weekly calls or meetings with Lithik, to make sure you're confident using its features, and aren't overlooking one that might make your life easier. Lithik support is happy to walk you through each phase of installation, setup, and implementation of all the features available to you.

Managing Policies

Once the LSM is up and running on your network, you can set up policies that start and control all the automation features of the LSM. These settings are found in **Automation Policy**, under the **Administration** tab. There is a large power button to the left of the **Automation Policy** title, which suspends automation on all policies.

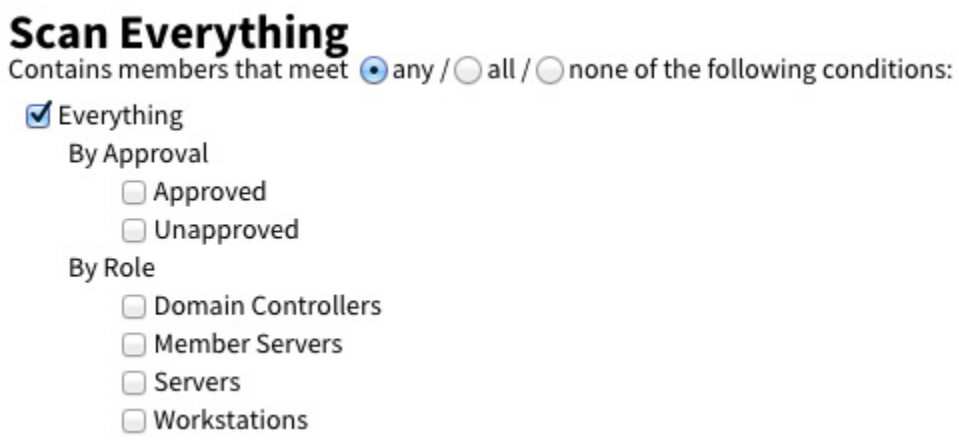
At factory default settings, all automation is suspended, but with default policies in place to make setup easier. When automation is enabled, changes to automation policy take effect immediately. It is advisable to suspend automation while making changes, lest a partially configured set of features be applied to your machines.

In the event that two or more policies conflict, policies higher on the list override lower policies, allowing you to easily make blanket rules overridden by exceptions. Policies can be dragged higher or lower on the list to change priority, and any conflicting conditions are be displayed below the list of policies.

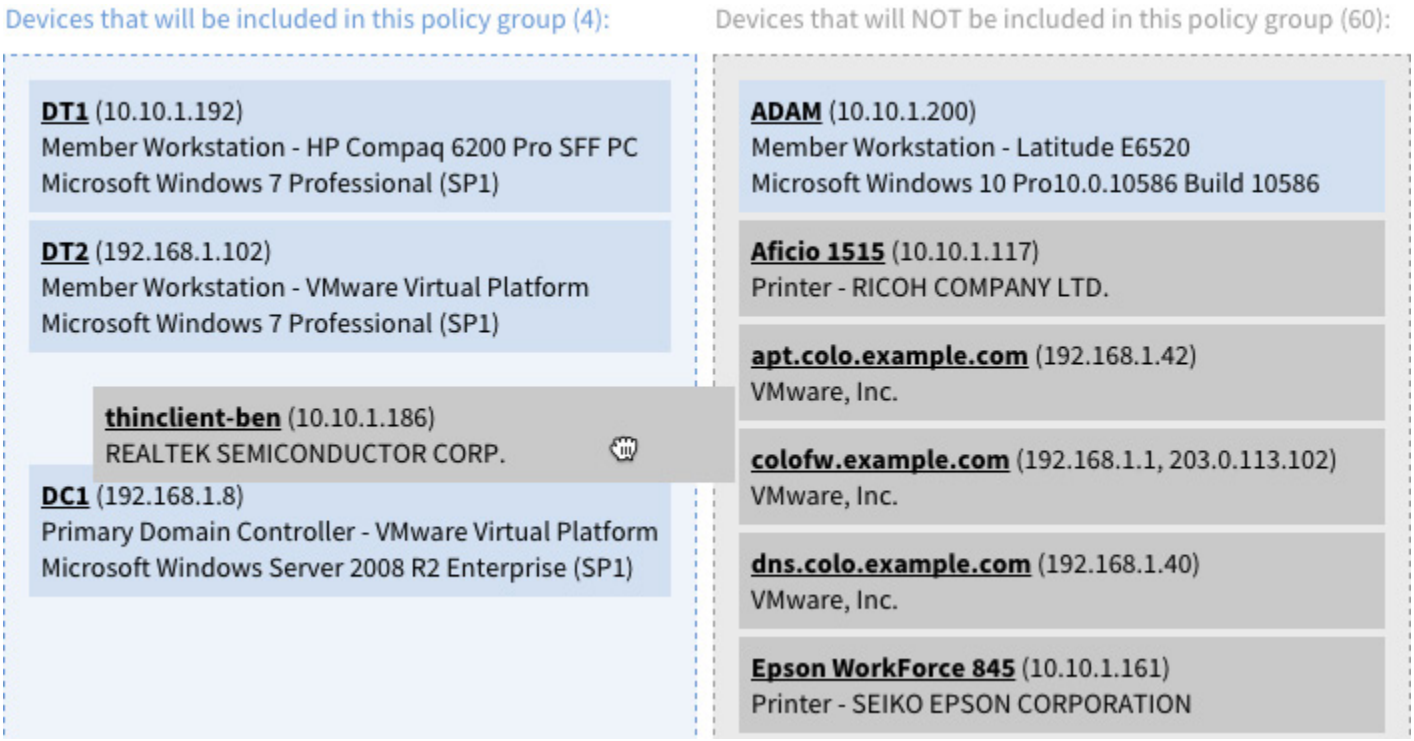


Note that disabling a feature is different than detaching it. While a detached feature has no effect, attaching and then disabling the feature will *prevent* that feature from being applied to included devices, even if it is enabled in a lower policy. If you plan on designing a complex policy that you only want to use occasionally, consider making a "STOP EVERYTHING BELOW THIS" policy, that applies to all machines and explicitly disables every category, placing it at the bottom of the list. To turn off a particular policy at any point, simply drag it below the stop everything policy. Creating policies beneath a stop everything policy is also a safe way to configure policies "live" without disrupting existing operations.

Each policy applies to the groups selected just below the title when the policy is selected.



Clicking the **Show Devices** button expands a pane listing all network devices, showing whether or not they are included in the policy. Included machines are displayed in blue in the left pane, and excluded devices are on the right in gray. Exceptions can be created by dragging a machine from one column to the other. The original color of the device is retained so that it is clear that they are exceptions.



Once the LSM has begun to discover devices on your network, experiment with the checkboxes and Any/All/None radio buttons to learn how they affect device selection. As you modify policies, a box may appear on the left side of the screen listing devices which are not covered by an important policy feature.

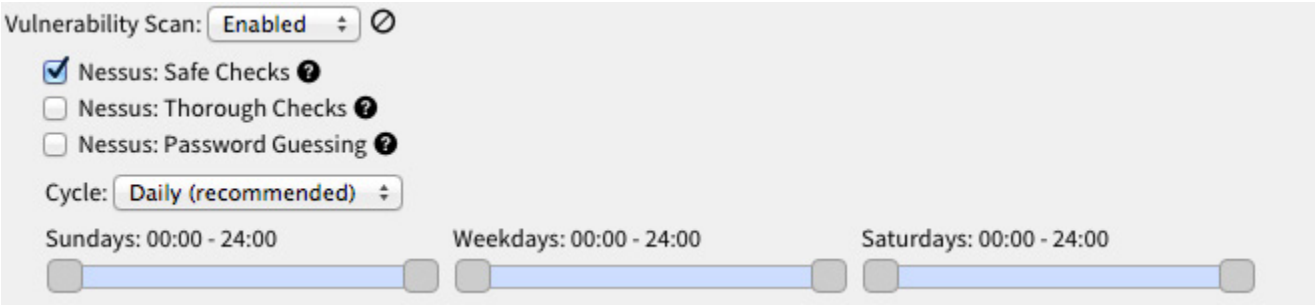
Default Policies

A new LSM will have several policies configured by default, but with automation suspended. The default configuration allows all machines to be scanned and updated throughout the day. Reboots occur overnight, with care taken to prevent domain controllers from rebooting simultaneously, or to have workstations reboot when servers they may depend on are rebooting. A set of commonly desired alert policies are also present by default. While these represent a reasonable starting point, you may wish to change settings, add policies to have more fine-grained control over different groups of machines, or perhaps just change their names.

The names for the default policies were chosen for clarity, but you may choose any title you desire. Policy groups can be renamed by clicking the title in the main pane of a selected policy.

Scan Everything

This policy will scan every device on your network (aside from those on the **Exclusions** table under **Network Configuration**) and discover vulnerabilities present on every device on every configured network. If Nessus is being used as the vulnerability scanner, additional options allowing more aggressive or restricted scans are provided here.



This allows you to make a scanning group for sensitive devices like printers, while still having comprehensive scans of systems in other policy groups. Settings which aren't necessarily intuitive, like the Nessus options, have a question mark next to them. Clicking on the question mark offers a more complete explanation of exactly what that feature does.

The scheduling sliders can also be adjusted to specify certain times of day by dragging the handles. To exclude times in the middle of the day, drag the handles past each other to create an inverted scheduling window.

Reboot...

The Reboot policies will restart devices in a variety of categories, according to the configured schedule, only if the operating system requires a reboot. Note the **Reboot Sequentially** option under the **Reboot Domain Controllers** policy.

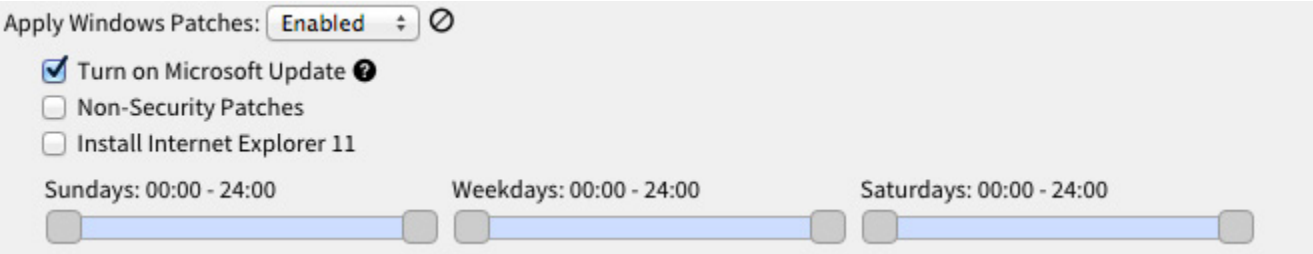
Checking this box will reboot member devices of this policy one at a time. That way, if one of the devices fails to start back up, the others will not be taken offline until the problem with the failing device is resolved. For workstations this usually is not important, but it is the recommended setting for redundant servers.

Update Everything

Now that vulnerabilities are being discovered, it is time to turn on the features that fix them. Start by testing with a few machines to make sure that if an update is going to cause problems, it won't cause an emergency. Once you are confident of the results you are getting, open up the patching features to include all the workstations on your LAN.

Apply Windows Patches

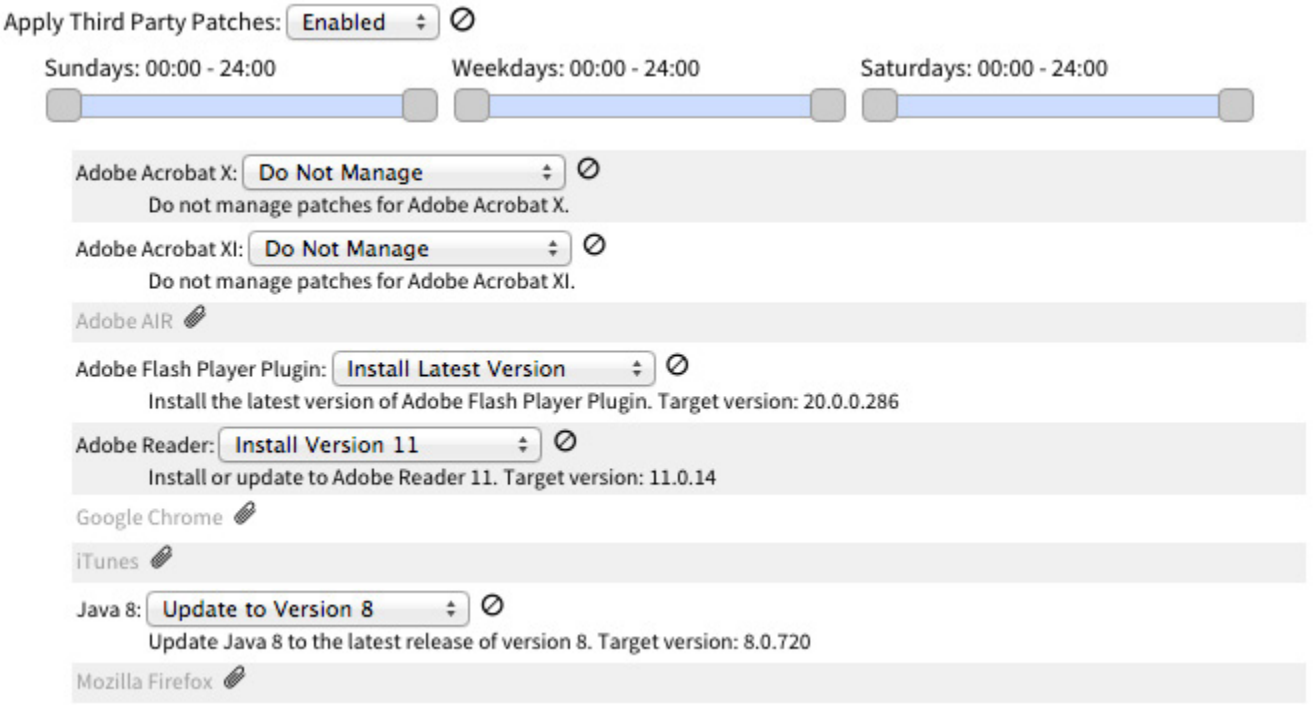
The Lithik Security Manager can deploy the Windows Update service on a custom schedule to make sure Windows machines receive important security updates in a timely fashion, without pop-up messages disrupting users. Optionally, non-security updates or Internet Explorer 11 can also be installed on target machines.



Be aware that **Apply Windows Patches** downloads updates from the WSUS server (if applicable) configured on the target machine. If an update is blacklisted or unavailable through the WSUS server, it will not be applied by the LSM. Note that Internet Explorer 11 installations will be performed independent of WSUS policy.

Apply Third Party Patches

Lithik maintains the latest patches for a select set of prevalent third-party software that can be updated or installed automatically as patches are released. A representative subset is pictured below:

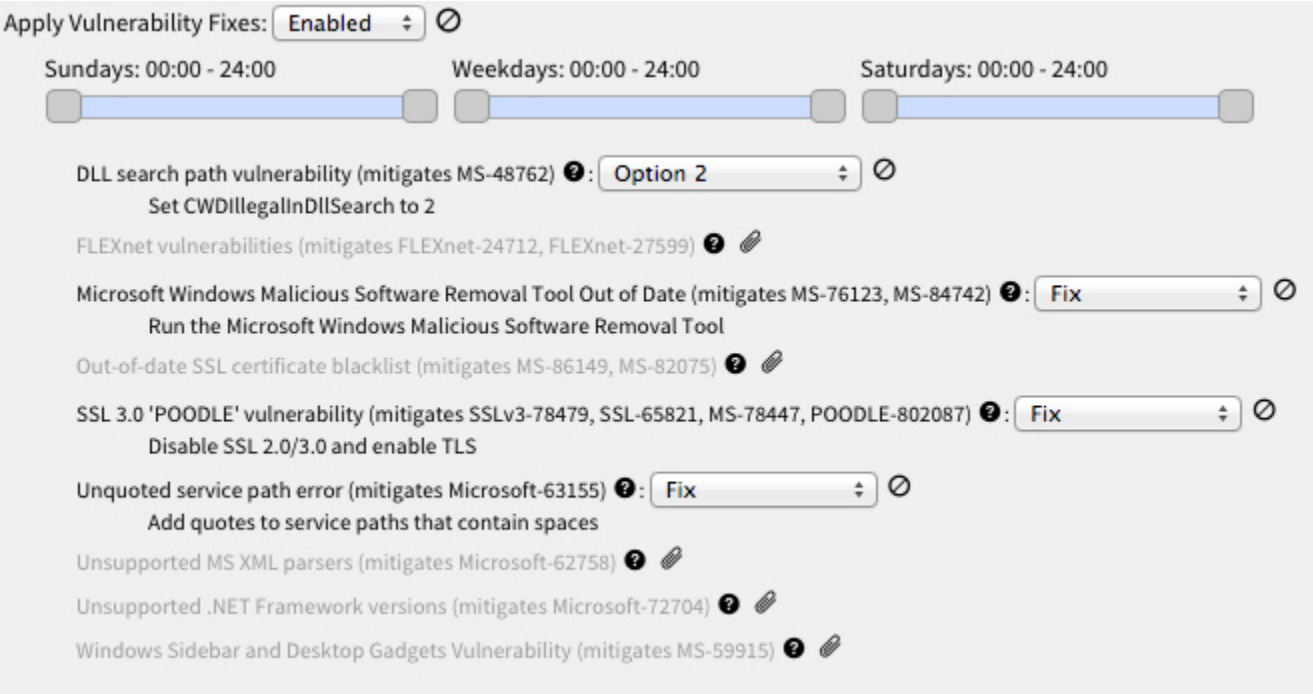


Each software package can be configured independently by the drop-down menu. Selections beginning with **Update to** will keep existing installations on member machines up to date. Selections beginning with **Install** will install the selected software when it does not exist and keep it updated when it does. Detaching the software package from the feature list will cause the policy to ignore the software altogether, while selecting **Do Not Manage** prevents member machines from being affected, regardless of their settings in lower-priority policies.

You may want to divide this policy into several policies, as different devices or branches often have different needs.

Apply Vulnerability Fixes

This section offers something unique to the LSM. Applying vendor supplied security patches prevents many attacks, but several of the most popular methods of breach use security vulnerabilities that depend on a particular configuration rather than software defects. This section allows management of common unsafe settings on a case by case basis.



Some of these changes are relatively benign, and are enabled by default. Some, like removing outdated versions of the .NET framework, can cause software that depends on the vulnerable version to stop working. More so than with any other portion of the Update policy, care should be taken to read and understand the explanation of the fix. Testing these fixes on a small subset of machines before deploying them network-wide is also highly recommended. This section should be checked regularly, as new vulnerability fixes are added from time to time. While new low-risk fixes may be set to be on by default when a new update policy is created, they are not enabled automatically in an existing policy, so if this is set once and forgotten, new vulnerability fixes created by Lithik will not be applied to your network.

Alert Policies

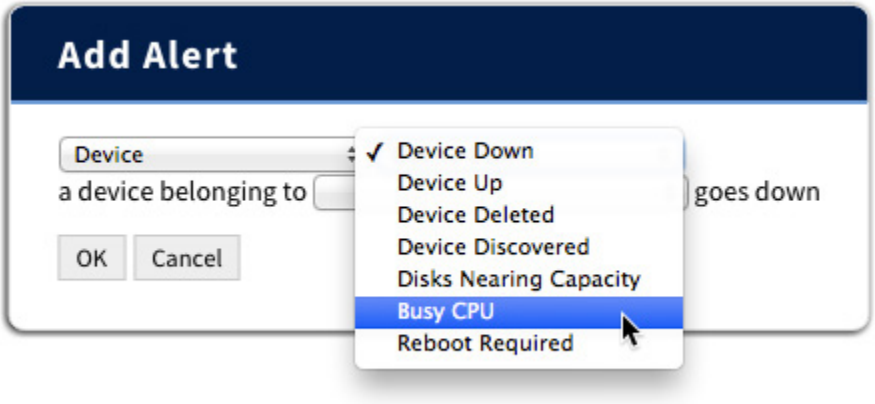
The Lithik Security Manager has the ability to notify you in the case of a configurable set of network events or conditions. These alerts can be sent to individuals or distribution lists, and abridged versions can be sent to mobile phone numbers.

Configuring Alerts

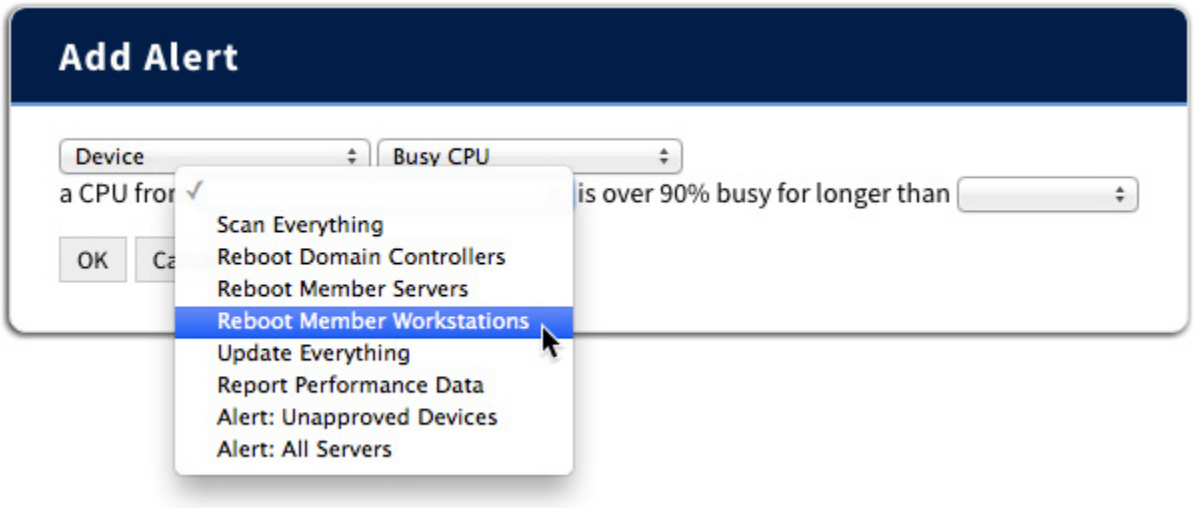
If you wish to receive email alerts, they can be configured by navigating to **Alert Policy** under the **Administration** tab. Alerts are organized in groups called alert blocks. The functional purpose of these blocks is to enable you to create custom distribution lists for sets of alerts. Blocks can be reordered by dragging them up and down in the list, but this is only for convenience; it has no effect on operation.

A default set of alert blocks is configured automatically, but without recipients. As with Automation Policy, the alerts they contain are only suggestions. You may add, delete, or modify as it suits the needs of your organization.

Click **Add Alert** to add an alert to a block. As you browse the alerts that are available, descriptions appear below.



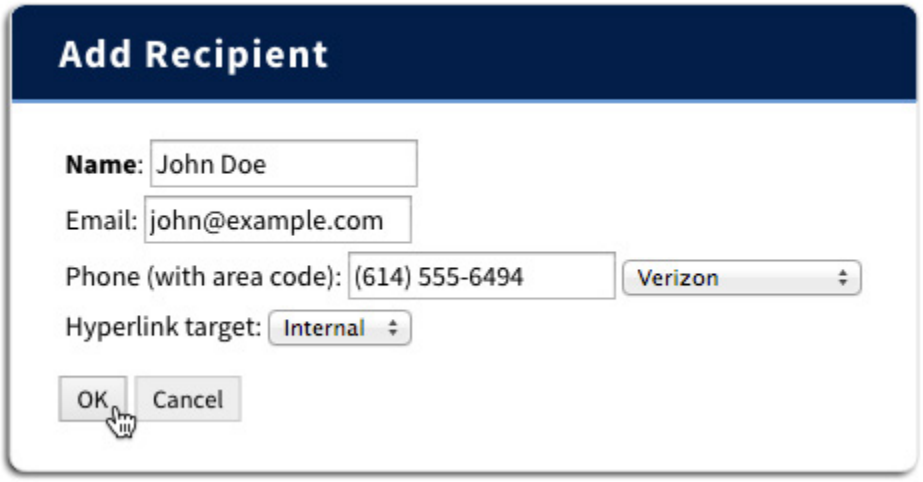
Many alerts must be linked to a policy group. The drop-down list of policy groups mirrors Automation Policy.



If you want to create an alert for a particular group of machines, first create an Automation Policy group with no features selected, then attach the device categories or individual machines as described above. The new policy group will now appear in the drop-down list when creating a new alert. The position of such a policy in the priority list is not important.

Configuring Alert Recipients

Click **Add Recipient** to add recipients to an alert block. There is no limit to the number of recipients that can be added to a block. The recipient's name must be provided, as well as one or more contact methods. If an SMS number is listed, it must contain the area code, and a mobile carrier must be specified.



Hyperlink target can be set to *Internal* or *VPN*. Some email alerts contain links to LSM locations pertaining to the alert. Internal hyperlinks lead to the internal address of the scanning appliance from inside the network, for example: *https://IPADDRESS/location*. VPN hyperlinks should only be used by those who have enabled the Inject LSM DNS Record feature or have set up LSM VPN Certificates on the LSM Users page. These links appear in the form of *https://lsm.lithik.com/location*.

614.890.0026 | support@lithik.com | 635 Park Meadow Road, Suite 208, Westerville, OH 43081