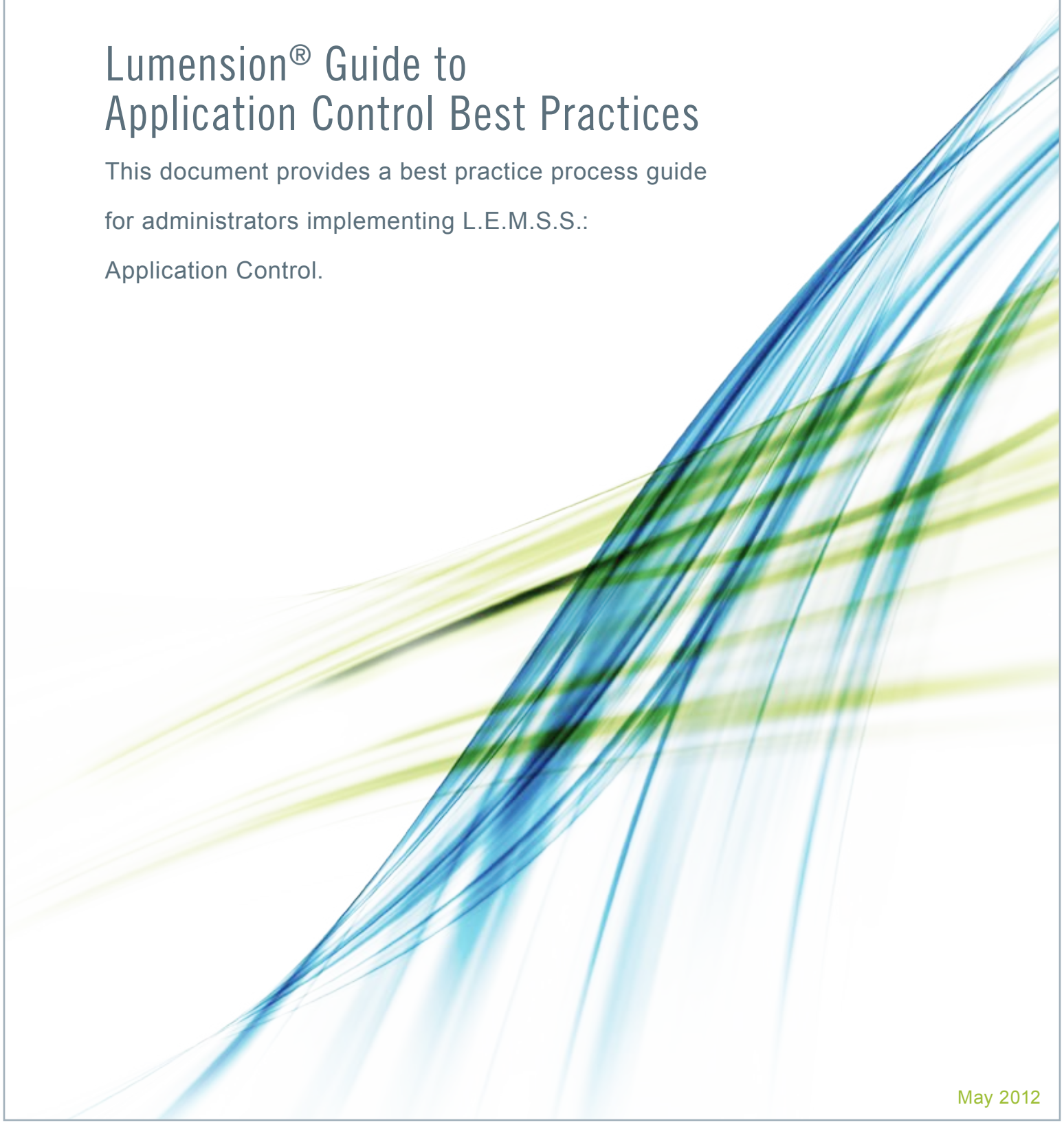
Lumension® Guide to Application Control Best Practices

This document provides a best practice process guide for administrators implementing L.E.M.S.S.: Application Control.



May 2012

WP-EN-05-17-12

Table of Contents

Introduction

The *Lumension*® Endpoint Management and Security Suite Application Control (L.E.M.S.S.:AC) provides complete malware protection and increases IT and end-user productivity by preventing any unknown, un-trusted or malicious applications from executing. With L.E.M.S.S.:AC, IT administrators can quickly identify all applications running in their environment and enforce a comprehensive whitelist policy that prevents unauthorized applications, malware and un-trusted change.

This document provides a best practice workflow to act as a guide for administrators when implementing L.E.M.S.S.:AC.

While L.E.M.S.S.:AC has been designed to minimize administrative burden, it is important to invest time during the deployment phase to ensure that the implementation is successful. This will allow that lower administrative burden to be realized once the endpoints have been locked down. In particular, administrators should avoid the temptation to quickly put endpoints into lockdown and to then start to define policies once issues arise.

Following the workflow outlined in this document should significantly reduce the possibility of issues occurring on your endpoints once the system is locked down.

Theory of Operation

L.E.M.S.S.:AC prevents malware and zero-day attacks without impacting productivity. The following are the key principles behind L.E.M.S.S.:AC:

- Application control is achieved by creating and enforcing an endpoint whitelist containing a list of the executables that that are allowed to run on that endpoint.
- The whitelist is initially created by scanning the endpoint to compile the list of executables via an Easy Auditor or Easy Lockdown scan. In the case of Easy Auditor, the endpoint goes into Audit mode once the scan has completed enabling the administrator to understand application execution and update patterns. In the case of Easy Lockdown, the endpoint goes into Enforcement mode once the scan has completed so that an executable is only permitted to execute if it is on the whitelist or if it is authorized by an L.E.M.S.S.:AC policy.
- When the endpoint scan has completed, the list of executables is added to the Application Library. The administrator then organizes the files in the Application Library into Applications and Application Groups so that they can either be authorized for additional users/groups or added to a Denied Applications Policy to prevent specified user/groups from executing them.

- The endpoint whitelist can be supplemented via a Supplemental Easy Lockdown/Auditor policy or automatically updated by a Trusted Updater to minimize administrator overhead. Updaters install new applications and/or patch existing applications and can also update the endpoint whitelist if they have been trusted by the system administrator to make endpoint changes.
- In addition to being authorized to execute because they are on the endpoint whitelist, files are also allowed to execute if they are authorized by a Trusted Change policy, which can include:
  - Trusted Publisher – Executables are authorized if they are signed with a Trusted digital signing certificate.
  - Trusted Path – Executables are authorized if they execute from a path which has been trusted by the system administrator
- Users that are assigned a Local Authorization policy are able to authorize or deny executables that are not otherwise authorized via whitelist or Trusted Change policy. If locally authorized, the files are allowed to execute; of course, administrators can then choose to add those files to the whitelist or to the Denied Apps group, overriding the end user decision.
- The system administrator can monitor endpoint activity via Application Event Log Queries and update policies as needed to authorize or deny executables.
- L.E.M.S.S.:AC connects to the *Lumension*® Endpoint Integrity Service (EIS), a cloud-based reputation data repository, to provide both administrators and users with verification rating information on files so that authorization decisions can be made

Via these principles, L.E.M.S.S.:AC enables administrators to establish and maintain a secure environment while simultaneously minimizing administrative burden.

Workflow Summary

The recommended workflow can be summarized as follows:

- **Clean.** Scan endpoints for malware prior to introducing L.E.M.S.S.:AC.
- **Discover.** Scan a small number of endpoints (the smallest number that will give you the widest cross-section of variability within the organization but ideally no more than 10 endpoints initially) using Easy Auditor to create an endpoint whitelist. This will populate the L.E.M.S.S. Application Library with a list of the executables from where they can be organized into Applications and Application Groups and then Authorized or Denied as appropriate.
- **Define.** Review Easy Auditor logs daily to determine what Trusted Change policies need to be implemented in your environment. Trusted Updater should be used where possible to handle application updates. Apply other policies (Trusted Publisher or Trusted Path) to cater for exceptions thereafter. A Windows Update Trusted Updater policy is a must-have if Windows Update is used to patch endpoints.

- **Monitor.** Once the initial Trusted Change policies have been implemented, continue to review Application Event logs daily and refine Trusted Change policies in preparation for going into blocking mode (Easy Lockdown). The monitoring phase should last for at least one (1) month to ensure that logs have stabilised and infrequently updated applications have had an opportunity to update. Use Local Authorization as a transition stage between Easy Auditor and Easy Lockdown.
- **Enforce.** Start to migrate endpoints from Easy Auditor to Easy Lockdown in a phased manner.
- **Manage.** Continue to monitor logs regularly to determine if policy updates are required and ensure that a process has been implemented so that users can request approval for new or blocked applications.

This workflow is discussed in greater detail in the remainder of this document.

In addition to following this workflow, you should also develop a communication plan to prepare users for what to expect as L.E.M.S.S.:AC is rolled out. You should also develop a support escalation plan for when endpoints go into Easy Lockdown so that users will be able to request authorization for new software. Finally, you will also need to train your IT Help Desk team to deal with such requests.

Phase 1: Clean

Prior to introducing L.E.M.S.S.:AC, you should scan the endpoints in your environment to remove any malware that might be present. This ensures that malware does not get added to the endpoint whitelist via an Easy Auditor scan.

In this phase you will:

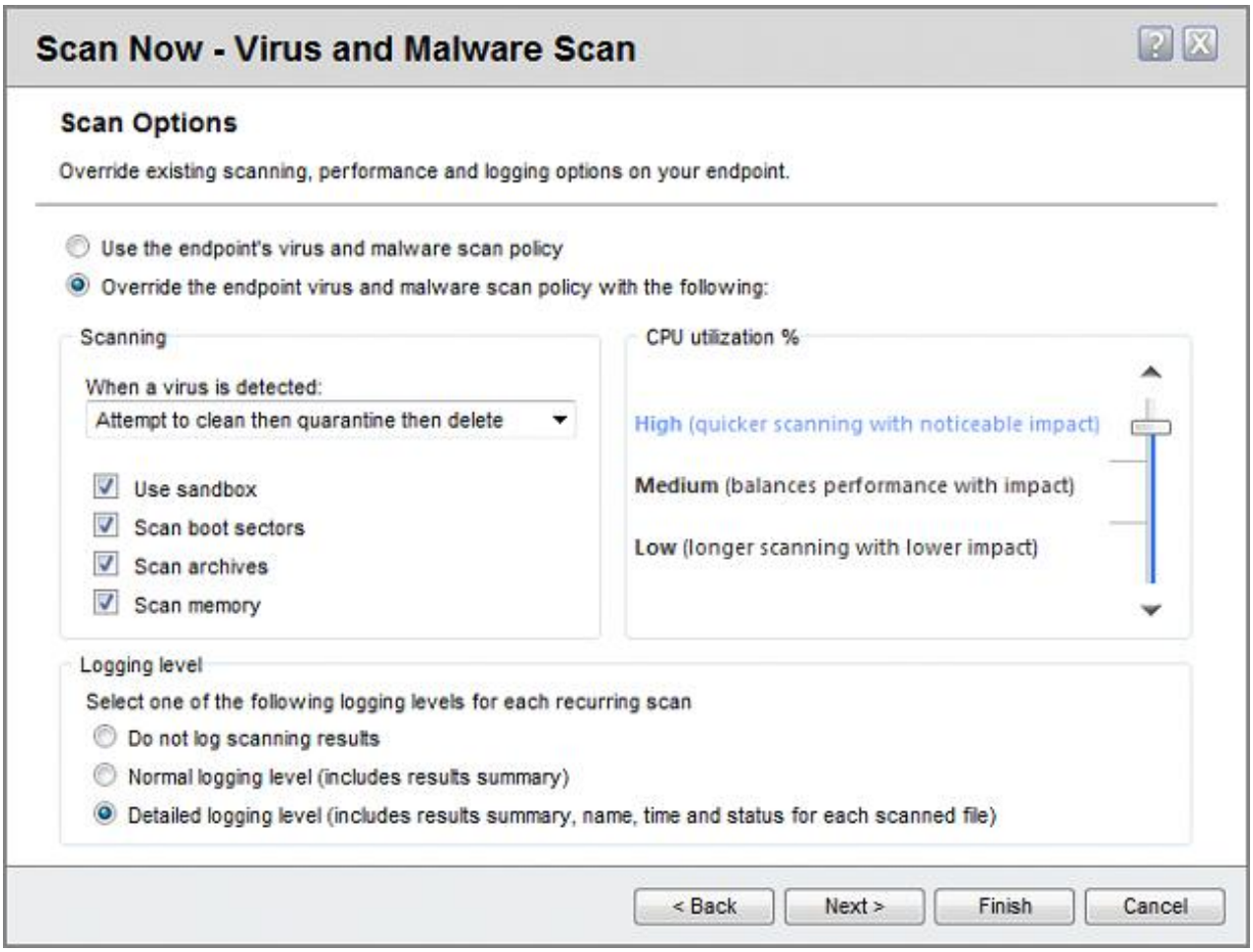
- Conduct a thorough antivirus (AV) scan to remove any dormant malware on your endpoints.
- Schedule the scan to execute out of hours, where possible, to minimize any productivity impact.
- Communicate with your users so they understand why this scan is being performed.

This cleaning process should be repeated prior to transitioning into Easy Lockdown as a significant period of time will have elapsed from the time that the Easy Auditor scan was conducted.

In this section we describe how you would clean your endpoints using the integrated L.E.M.S.S. AntiVirus module (L.E.M.S.S.:AV). Of course you can also use a 3rd party AV solution to perform this task. In either case, the recommendation is to perform a thorough scan to ensure that any dormant malware (e.g., malware buried within archives) is identified and removed.

A thorough AV scan could take an extensive amount of time to complete so you should schedule the scan to execute out of hours, if possible, to minimize any user disruption. If the scan is executed during working hours, ensure that you communicate with the affected users so that they are aware of what is happening.

To implement a thorough AV scan on L.E.M.S.S.:AV, conduct a “Scan Now – Virus and Malware Scan” and select all the scanning options including Archive scan as shown below.



Once these scans have completed and any associated malware has been removed, you are now ready to proceed to the next phase.

Clean Phase - Summary

Prior to introducing L.E.M.S.S.:AC, conduct a thorough AV scan of your endpoints so that you do not add malware to the endpoint whitelist.

This thorough AV scan should be repeated prior to both Easy Auditor and Easy Lockdown scans in L.E.M.S.S.:AC.

Phase 2: Discover

In the discovery phase, endpoints are scanned to create the endpoint whitelist and identify the applications in your environment.

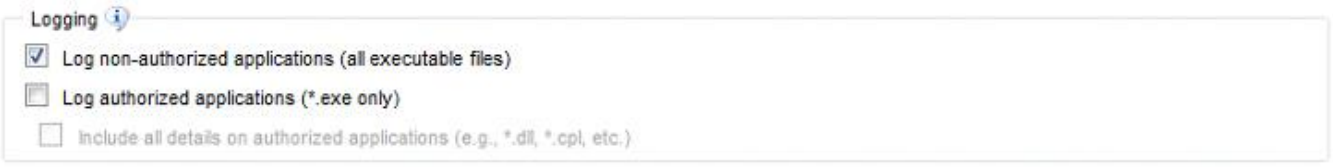
In this phase you will:

- Scan the endpoints to create an endpoint whitelist and discover what applications exist in your environment
- Review these applications in the Application Library and create Denied Applications Policies for any unwanted software
- Communicate with users so that they understand that L.E.M.S.S.:AC is being rolled out and that certain applications are now prohibited and will be blocked.
- Customize the blocked notification dialog so that users understand why applications are being blocked and to provide instructions to escalate in the event they need to use these applications.
- Leverage the cloud-based *Lumension*® Endpoint Integrity Service (EIS) to understand file ratings and the *Lumension*® Endpoint Intelligence Center (LEIC) to obtain more detailed information on files or submit suspect files for malware analysis.

Easy Auditor Scan

Once the whitelist has been created via Easy Auditor the endpoint goes into a non-blocking / audit mode and, depending on the logging settings that were selected when creating the Easy Auditor Policy, the endpoint will log when applications are executed. These logs are sent back to the server so that they can be analyzed by the system administrator.

You should avoid using “positive logging” (i.e., logging execution of authorized applications) when creating the Easy Auditor policy and only log non-authorized applications as shown below. Logging of authorized applications should only be used for troubleshooting purposes. If this setting is selected for a policy which is applied to a large number of users, the logs will become very large very quickly and may result in storage space issues on the L.E.M.S.S. server.



Tip: In the discovery phase, it is recommended to start with a small number of endpoints (<10) so that the administrator can review the initial logs without being overwhelmed with data. Once the L.E.M.S.S.:AC policies have been defined the number of endpoints can then be expanded. The endpoints selected should be from a number of different departments (e.g., HR, IT, Sales and Engineering) and Operating Systems so that the Application Library is populated with a diverse range of applications.

The Application Scan (AppScan) which is used to create the whitelist can be a fairly CPU and disk intensive activity. Where possible the Easy Auditor scan should be run out of hours to minimize the productivity impact for the end user. The scan may take a number of hours to complete. The endpoints should be configured so that they do not go to sleep or hibernate as this will force the AppScan to start over from the beginning.

EXCLUDING FILES/FOLDERS FROM APPSCAN

If the scan cannot be executed out of hours, ensure that you communicate with end users to set the expectation that they may experience a productivity impact. If users complain of significant performance impacts, you may need to consider excluding certain types of files or certain file paths from the scan. This should only be performed for files or paths which do not contain executables which will be needed later. VM Archives (*.vmdk) are an example of files which can be considered for exclusion if users are encountering significant performance issues when the scan is being performed. The initial scans with a small number of endpoints should provide a good indication whether such exclusions will be required when applying Easy Auditor to the general population.

Some endpoints, particularly servers, may have a large amount of compressed files/folders and scanning these files may cause the scan to run for an extended period of time and consume a lot of disk space. In the event that the Easy Auditor scan is causing issues on specific endpoints, you can stop this happening by setting an environment variable on the endpoint that specifies file types or file paths that you do not want extracted/scanned.

The environment variable is called %ACAPPSCANEXCLUDE%. Here are some samples:
C:\\Windows\\Temp\\;C:\\Custom\\;*.vmsd;*.vmem;*.vmxf;*.vmdk
E:\\MYDATA\\;C:\\CustomFolder\\;*.7z;*.vmsn;*.dll

Some things to note:

- Use double backslashes as path separators.
- Avoid adding a semi-colon at the end of the list.
- You need to reboot the endpoint before this takes effect.

Application Library

Once Easy Auditor has been completed for one or more endpoints, all of the file details from the scanned endpoints are brought back into the Application Library on the server. Note that when the Easy Auditor scan has completed the new files added to the Application Library will be located in the "Ungrouped Files" folder in the Application Library.

You can then organize these files into Applications and Application Groups so that they can be authorized or denied centrally.

Create Denied Applications Policies

At this point in the rollout, you should focus only on Denied Applications. Authorizing applications is unnecessary while in Easy Auditor but becomes important once endpoints are put into Easy Lockdown. We will discuss Authorizing Applications later in this document.

Denied Applications Policies can now be defined to block any applications or versions of applications that you do not want to be allowed to execute in your environment. These policies can be applied for all users or can be limited to specific groups as appropriate. Unwanted software (e.g., hacking tools, music streaming software, insecure Instant Messaging or VoIP applications) can be installed onto a test endpoint, scanned via Easy Auditor and grouped in the Application Library.

By creating a "Denied Applications" group under Application Groups in the Application Library and assigning this to all users, you can simply add applications to this group and they will then be denied for all users.

Tip: Denied Applications policies can be applied to users even prior to the endpoints being put into Easy Auditor or Easy Lockdown. As such, you can get an immediate benefit from L.E.M.S.S.:AC by denying any applications that you do not want to have execute in your environment. Applications can be denied, not just for the users in Easy Auditor but for any endpoint which has the L.E.M.S.S.:AC module installed. In the endpoint decision flow, the Denied Applications policy is checked prior to all other policies including the endpoint whitelist (see Appendix: Decision Flow at the Endpoint). As such, Denied Applications policies prevent anything from executing which might otherwise to be authorized via whitelist or a Trusted Change policy.

Customize the Blocked Notification Dialog

You should inform users of any applications which are being denied and provide an escalation mechanism for them to be authorized for such applications if they have a legitimate business need. The blocked notifica-

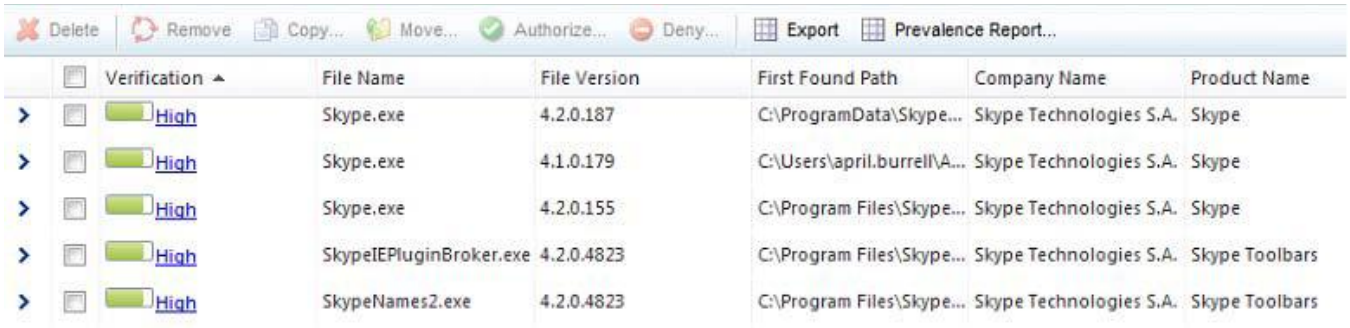
tion dialog should be customized so that your users understand why an executable has been blocked and how to escalate if this executable is required for business reasons.

The dialog can be customized via the Application Control tab under the Tools > Options menu on the L.E.M.S.S. server. On this tab you can do the following:

- Add your own company logo so that the user is aware that this is a message from your organization.
- Add a customized message (up to 1000 characters) to inform the user why this executable has been blocked and what steps they should take if they need this application.
- Add a URL which could be a link to the help desk ticketing system or to a repository of approved software.

Lumension® Endpoint Integrity Service

The Application Library connects to the *Lumension*® Endpoint Integrity Service (EIS) to obtain file rating information which can then be used to make trust decisions. These ratings are displayed in the verification column in the App Library as shown below. The verification ratings supplied by EIS provide the level of confidence that the file is actually what it proclaims to be and these ratings are useful as you make trust decisions.



Lumension® Endpoint Intelligence Center

Further information on specific files can be obtained from the *Lumension*® Endpoint Intelligence Center (http://leic.lumension.com/index.html) to guide decision making. Individual files can be uploaded to perform a hash lookup via EIS or alternatively suspect files can be submitted for malware analysis.

Discover Phase Summary

The discovery phase is used to create endpoint whitelists and to populate the Application Library with the files that are used in your environment. From the Application Library, any unwanted software can then be blocked for some or all users.

Phase 3: Define

The define phase is used to create policies to allow Trusted Change to take place on the endpoints that are in Easy Auditor. These policies automate whitelist maintenance and minimize the burden associated with managing software changes in your environment.

In this phase you will:

- Review the applications in your environment and develop strategies for how change in these applications will be supported.
- Avoid the temptation to put endpoints into lockdown until after policies have been defined.
- Define Trusted Change policies including Trusted Updater, Trusted Publisher and Trusted Path.

Investing in policy creation is key to a successful implementation, so you should spend the time to develop the Trusted Change policies to support changes in the applications in your environment. Making this investment now will save on support calls and greater effort in the long run.

Review Applications and Develop Change Strategy

You should develop a strategy for all applications in your environment and decide how you are going to allow change to occur for them including determining which applications you allow users to update themselves versus which applications you update centrally. You can use the Easy Auditor logs which will tell you when changes have taken place on the endpoints or you can get ahead of the logs and start to put policies in place for applications that you know are going to change.

Tip: While this phase assumes you are already in Easy Auditor, it is also possible to define policies prior to putting endpoints into Easy Auditor. In terms of best practices, once the initial group of endpoints have gone into Easy Auditor and policies have been created for them, these policies should be applied to additional endpoints before they are put into Easy Auditor. Doing this reduces the number of Easy Auditor log events that you need to review as log events are only created when files are executed which are either not on the whitelist or are not covered by a Trusted Change policy.

Avoid Putting Endpoints into Lockdown Just Yet

It is important to remain in Easy Auditor until the necessary policies to allow Trusted Change to occur on the endpoint have been created. From the time that L.E.M.S.S.:AC policies have been created at least one (1) month should be allocated to monitoring the Application Event logs for any additional changes which are not covered by the existing policies. This period should include at least one (1) Patch Tuesday and ideally

a major event like a quarter-end. This duration is necessary to validate that policies are working correctly because some applications may only make updates once a month or even less frequently.

You should avoid the temptation of going into lockdown too early. If you put endpoints into lockdown and do not have policies in place to support changes in those applications, they will update and the updated applications will be blocked from executing as the updated files will not be on the whitelist.

Trusted Change Policies

The following Trusted Change policies are available for use:

- **Trusted Updater.** Trusted Updaters enable administrators to install and automatically authorize software patches and/or new applications without additional administrator overhead. Trusted Updater updates the endpoint whitelist and should be used where possible to manage change on your endpoints.
- **Trusted Publisher.** Trusted Publisher automatically authorizes software installers, updates and/or new applications to execute at the time the user executes them, with no required administrator overhead, when those installers, updates or applications have been signed by a trusted certificate. When a Trusted Publisher policy is assigned, any application will be allowed to execute so long as the initial executable is signed with one of the certificates in the policy. Trusted Publisher does not update the endpoint whitelist and should only be used to install or update applications if it is not possible to implement a Trusted Updater policy for a specific application.
- **Trusted Path.** Trusted Path authorizes applications to run based on their location as an alternative to adding them to a whitelist. You can optionally specify ownership restrictions so that the file can only execute in the Trusted Path if the owner is as specified in the Trusted Path policy.

Let's look at each of these policies in more detail.

Trusted Updater

Trusted Updaters enable administrators to install and automatically authorize software patches and/or new applications without additional administrator overhead. By assigning trust to particular executables (Trusted Updaters), any files added to the endpoint by these executables are automatically whitelisted for that endpoint. A Trusted Updater policy is used for:

- Software Distribution tools or Patch & Remediation tools such as:
  - *Lumension*® Patch and Remediation (default Trusted Updater policy in L.E.M.S.S.)
  - Novell Zenworks

- HP Radia
- Microsoft SCCM (System Center Configuration Manager)
- Windows Update
- Altiris
- Tivoli
- Shavlik

- 3rd party Antivirus solutions such as:
  - Sophos
  - McAfee
  - Symantec
  - Kaspersky

- Self-updating applications such as:
  - Adobe
  - Apple iTunes
  - Java
  - Mozilla Firefox

Use the software inventory to identify the applications that are installed on the endpoints in Easy Auditor.

Note that Trusted Updater is the only trust mechanism that updates the endpoint whitelist directly. Using other trust mechanisms to install or update applications can cause problems and could even result in un-bootable endpoints if those installations or updates change files which are required during the endpoint boot sequence (e.g., driver files).

IMPORTANT – WINDOWS UPDATE

Windows Update is enabled on endpoints by default. If Windows Update is being used to update endpoints, you should absolutely avoid going into Easy Lockdown until a Windows Update policy has been created. Otherwise, Windows Update will run and will update system files which will not be whitelisted resulting in unbootable endpoints.

Lumension has created a Windows Update policy kit which contains a list of all the hashes of the updater files for Windows Update contained in the *Lumension*® Endpoint Integrity Service (EIS), a cloud-based

reputation data repository. Given the number of different versions of the updater files and also the number of different updater files, this kit greatly simplifies the task of creating a Windows Update Trusted Updater policy. To arrange having this policy kit imported to your L.E.M.S.S. server, please contact your Lumension Sales Engineer.

SOFTWARE DISTRIBUTION TOOLS OR PATCH AND REMEDIATION TOOLS

Lumension® Patch and Remediation is a default Trusted Updater so no configuration is required. In the case of other software distribution tools or patch and remediation tools, the application executable should be added to the Trusted Updater policy. In addition, any updater files for the application should also be added to the policy.

3RD PARTY ANTIVIRUS SOLUTIONS

Antivirus solutions are updated every day with new signature files and also occasionally with new engine files. To accommodate these changes, you need to create a Trusted Updater policy. Note, however, that you need to trust the AV updater and not the AV scan engine. If you trust the AV scan engine, every file that the scan engine touches (i.e., every file accessed by the user) will inherit this trust which has the same effect as turning off application control on the endpoint.

BROWSERS

As with AV solutions, you should not trust browsers (e.g., iexplore.exe, firefox.exe, etc.) as this has the same effect as trusting the entire Internet! Instead, you should add the browser updater (e.g., updater.exe for Firefox) to the Trusted Updater policy to support browser updates.

SELF-UPDATING APPLICATIONS

Software applications will be updated over time to address bugs, address security issues and add new features. Each application will typically have one or more updater files which are used to perform these updates. These updater files will already have been whitelisted via the Easy Auditor scan so they can execute. However, the new files that they add to the endpoint will not be allowed to execute as they are not whitelisted. To accommodate these changes, every updater in the environment should be explicitly denied or added as a Trusted Updater (e.g., softwareupdate.exe for Apple Software Update).

IDENTIFYING UPDATER FILES

The biggest challenge in creating a Trusted Updater policy for an application is identifying and locating the updater files. You should contact your Lumension Sales Engineer if you are unable to determine the updater for a specific application.

The following mechanisms can be used to identify updaters:

1. **Use the logs.** Create a daily Application Event Log query for "Easy Auditor: Applications Blocked when Enforcement is Enabled." This query highlights any executables which would have been blocked if the endpoint had been in lockdown. The parent process for these executables may be updaters. Note, however, that this is not always a good indication as the parent process in the logs is the immediate preceding process and this could be a process like "explorer.exe" which would not be the actual original updater/parent process.
2. **Search for "update" or updater" in C:\Program Files.** Applications which update themselves have specific executables which perform these updates. These often have "update" in the name of the executable or the folder containing the executable or executables.
3. **Refer to vendor documentation.** Application vendors often provide information on the update mechanism for that application for use in firewall configuration (e.g., http://kb2.adobe.com/cps/837/cpsid_83709/attachments/Acrobat_Reader_Updater.pdf).

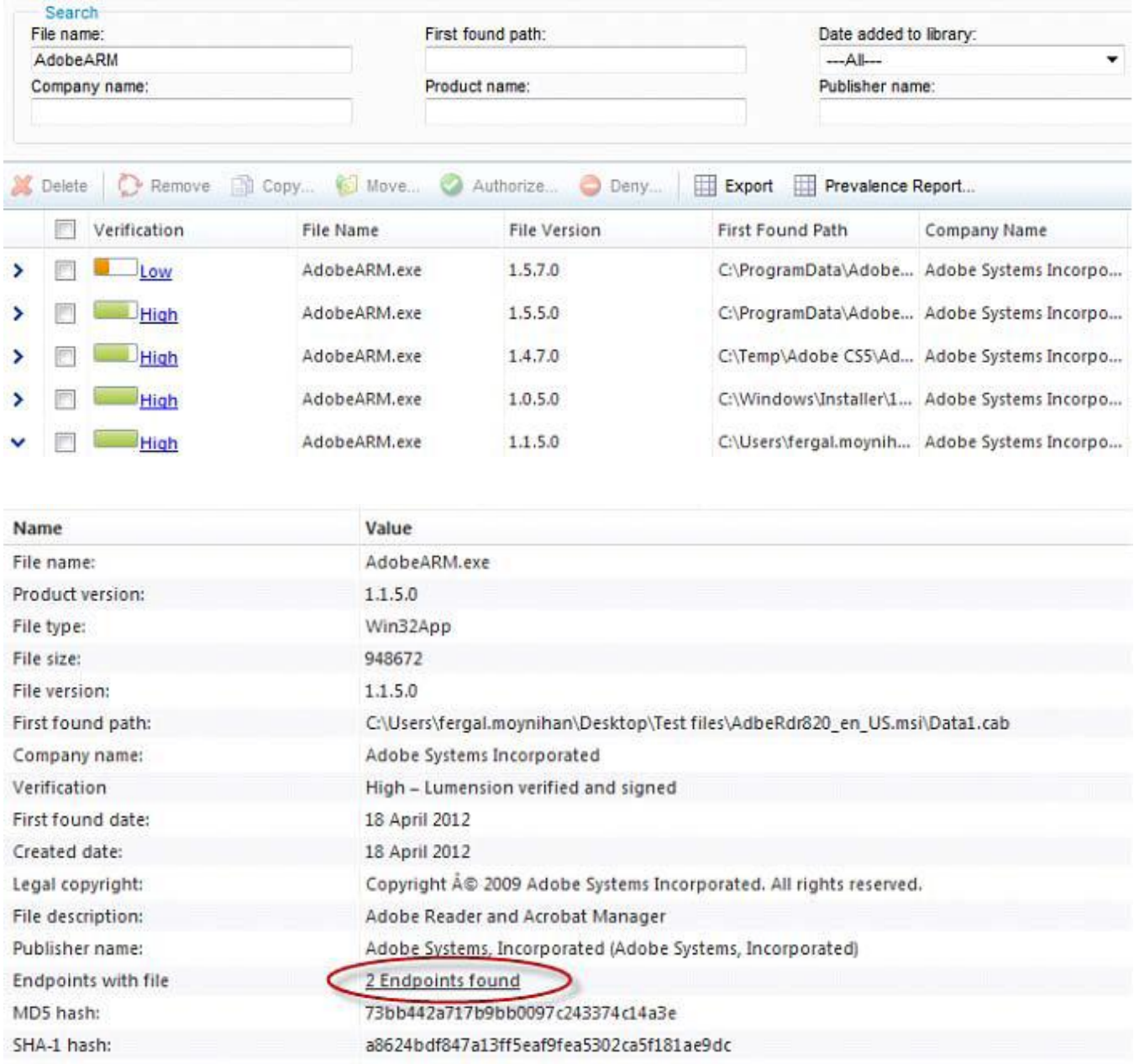
CREATING A TRUSTED UPDATER POLICY

Once the updater files have been identified, the next step is to create a Trusted Updater policy and add the updaters to that policy. Note that there may be multiple versions of the updater file on each endpoint and it is also likely that different endpoints will have different versions of the updater.

Use the Application Library and the prevalence report to identify how many different versions of the updater file exist and which endpoint and path that version is located on. Clicking on the link (as shown below) will identify endpoints from where this file can be obtained.

When creating the policy you can then navigate to the path on the endpoint to add that version of the updater. In order for the Trusted Updater policy to be effective all versions of the updater need to be added to the policy.

If a version is not included, any changes performed by that version of the updater will not be added to the whitelist which would cause those applications to be blocked when in lockdown.



UPDATER BEHAVIOR

There is no standard mechanism by which applications get updated and different patterns of updating behaviour have been observed. The most common updating mechanism is whereby the applications have one or more updaters and these are the files which should be added to the Trusted Updater policy.

As there is no standard, it is also possible that a vendor may change the mechanism that they use to update applications over time (e.g., use a different mechanism for the next major update). If this happens, it may result in the updated version of application being blocked.

This can be resolved by identifying the new updater and adding this to the Trusted Updater policy and also by authorizing the new version of the application for any affected users.

There are also some updating mechanisms which are inherently insecure from an application control perspective. For example, patterns of behavior have been observed whereby the application (e.g., a browser) itself detects that a new version of the application is available and downloads the installer (i.e., there are no specific updater files and trusting the primary application executable would be very insecure). The installer then uninstalls the old version of the application and installs the new version which is not whitelisted so will not execute. In this case, the new version of the installer needs to be added to the Trusted Updater policy and the new application version can then be reinstalled for any affected endpoints.

The best practice is to use the period while endpoints are in Easy Auditor to understand updater behavior. If it is not possible to create a Trusted Updater policy for an application, you could consider using an alternative Trust mechanism (e.g., Trusted Publisher). Alternatively, you could disable automatic updates for this application and use a test endpoint in automatic update mode to obtain the new updater or installer. You could then add this to the Trusted Updater policy and roll out the updated version.

Trusted Publisher

Trusted Publisher automatically authorizes software installers, updates and/or new applications to execute at the time the user runs them, with no required administrator overhead, when those installers, updates or applications have been signed by a trusted certificate.

Trusted Publisher authorizes applications to run based on their digital signing certificate as an alternative to adding them to the whitelist. Trusted Publisher can be used for:

- Cloud-distributed applications which do not reside on disk until time of execution (e.g., Webex, GoToMeeting – signed ActiveX controls downloaded into a browser).
- Browser plugins (which generally do not have updater tools).
- In-house signed custom applications.

The file which is authorized to execute via Trusted Publisher will be allowed to load all dependent processes. They need not be signed. Only the initial executable needs to be signed.

Note that most software vendors have multiple certificates. Not all certificates for the same vendor are authorized; only the specific certificates on the policy. If an executable that you would have expected to be authorized via Trusted Publisher is being blocked, check to see if the certificate matches that in the policy and add to the policy, if it is different.

Trusted Publisher can be used to run programs that install applications and those installed applications will run as long as the initial executable is signed too.

As Trusted Publisher does not update the whitelist, you should only use it to install applications which do not modify core system files or dlls which are shared with other applications. If the installation causes files (e.g., dlls) to be updated which are shared by other applications then those other applications may no longer be able to execute (e.g., if whitelisted files have been replaced by unsigned dlls).

Warning: Trusted Updater should be the default policy for installing and updating applications. You should only consider Trusted Publisher to install or update applications if it is not possible to do so via Trusted Updater.

Trusted Path

Trusted Path authorizes applications to run based on their location as an alternative to adding them to a whitelist. Trusted Path allows execution of an application if it is stored in one of the paths specified in the policy and can be used for:

- Unsigned executables which change frequently (e.g., where every install of the application is unique).
- Shared Network Paths (e.g., build output locations for in-house software development).

While allowing applications to execute based on their location may not seem like a particularly secure solution, you can specify ownership restrictions (Authorized Owner) so that the file can only execute in the Trusted Path if the owner is as specified in the Trusted Path policy. Files in these paths should also be secured via O/S privileges. This greatly increases the security of this Trusted Change policy while still maintaining flexibility.

Define Phase Summary

The define phase is used to create the policies that will be needed to support trusted changes on endpoints. These policies automate whitelist maintenance resulting in reduced administrative burden. Investing in policy creation is key to a successful implementation and saves on support calls in the long run.

Phase 4: Monitor

Once the initial policies have been created and Easy Auditor scans have been completed on a number of test endpoints, the Application Event logs should be monitored daily to identify any missing policies or policies that need to be updated.

In this phase you will:

1. Create scheduled Application event log queries.
2. Review Easy Auditor logs daily and create or adjust Trusted Change policies to accommodate these changes.
3. Re-run Easy Auditor to "reset" logs, if necessary.
4. Optionally, apply Local Authorization policy to users in Easy Auditor once the logs have stabilized.
5. Maintain a test endpoint so that new software can be scanned and added to the Application Library.
6. Ramp up the number of endpoints in Easy Auditor and adjust your policies to accommodate these new endpoints.

By the end of this phase you should be ready to move endpoints into lockdown. This phase continues until the logs have stabilized. The stabilization period should last for at least one (1) month incorporating at least one (1) Patch Tuesday and a significant corporate event, such as quarter-end.

Application Event Logs

By reviewing the "Easy Auditor: Applications Blocked when Enforcement is Enabled" logs you can identify when and how changes have taken place on endpoints. Log entries appear when executables are run that are not on the whitelist or are not covered by a Trusted Change policy. If the endpoint had been in lockdown, these files would be blocked so it is important to create or update policies to cater for these changes prior to going into lockdown.

When creating the Easy Auditor policy, logging options are provided to log non-authorized applications and/or authorized applications, as shown below.

Logging of authorized applications should only be used for troubleshooting on an endpoint and only for a limited period. Authorized applications logs (also known as positive logging) become very large very rapidly and if used, even on a relatively small number of endpoints, for a period of time will cause the hard disk on the server to fill up. Instead, select the default option to log non-authorized applications as these logs provide all the information needed to ensure your policies are complete prior to going into Easy Lockdown.

During the initial monitoring period, the "Easy Auditor: Applications Blocked when Enforcement is Enabled" logs should be monitored daily. Avoid leaving this for a number of days as the logs can rapidly build up and it becomes a bigger challenge to maintain. Create a daily log query for this log file and have the completed log file emailed to you. This acts as a daily reminder to review the logs and update the policies. After the initial week or two have passed and the number of new log entries start to dwindle, start to roll Easy Auditor out to an increased number of endpoints and/or reduce the frequency of the query to once or twice per week.

Tip: Note that if a log entry appears, it may continue to appear even after a policy has been created to cater for that scenario. This could happen because an application is updated and the new application version is not on the whitelist. You could create a Trusted Updater policy for this application which will add files to the whitelist the next time the application is updated. However, each time the current version is executed it will still result in log entries. You can address this by unassigning and reassigning the Easy Auditor policy for that endpoint which will then cause the Easy Auditor scan to re-run and "reset" the logs by adding these new files to the whitelist.

Local Authorization

Prior to going into Easy Lockdown, you can apply a Local Authorization policy which will then request the user to authorize any executables which are not on the whitelist or authorized by a Trust mechanism. Local Authorization acts as a 3rd mode of enforcement:

1. Non-blocking (Easy Auditor)
2. Blocking with Local Authorization
3. Blocking (Easy Lockdown)

Warning: Prior to applying local authorization in Easy Auditor, you should unassign and reassign the Easy Auditor policy so that any system files which were modified while in Easy Auditor are now added to the whitelist. Otherwise, these files could cause problems at boot-up before local authorization is available for the user to respond. You should also ensure that the necessary policies have been implemented to cater for

the modification of these system files in the future. In particular, you should not apply a Local Authorization policy to an endpoint which does not have a Windows Update Trusted Updater policy (if Windows Update is enabled) as this could result in boot-up issues if Windows Updates are authorized via local authorization.

Using Local Authorization as a 3rd enforcement mode provides a number of benefits:

- Users will become aware that this is a transitionary stage to a full blocking mode in that they are now being requested to authorize executables whereas prior to this point (in Easy Auditor) they would be unaware of the potential impact of decisions that they made to install new software or update existing software. You should ensure that you communicate clearly with your users that they are entering this new phase of L.E.M.S.S.:AC so that they know what to expect. User productivity will not be impacted but they will become aware that the applications that they use are now being controlled.

- The administrator still retains the option to monitor any executables that are being locally authorized by the user community and has the option to add these to a Denied Applications policy if they do not want these applications to be used in their environment. Alternatively, they can be added to a Supplemental Easy Lockdown/Auditor policy if these executables should be available for all users or for selected groups of users.

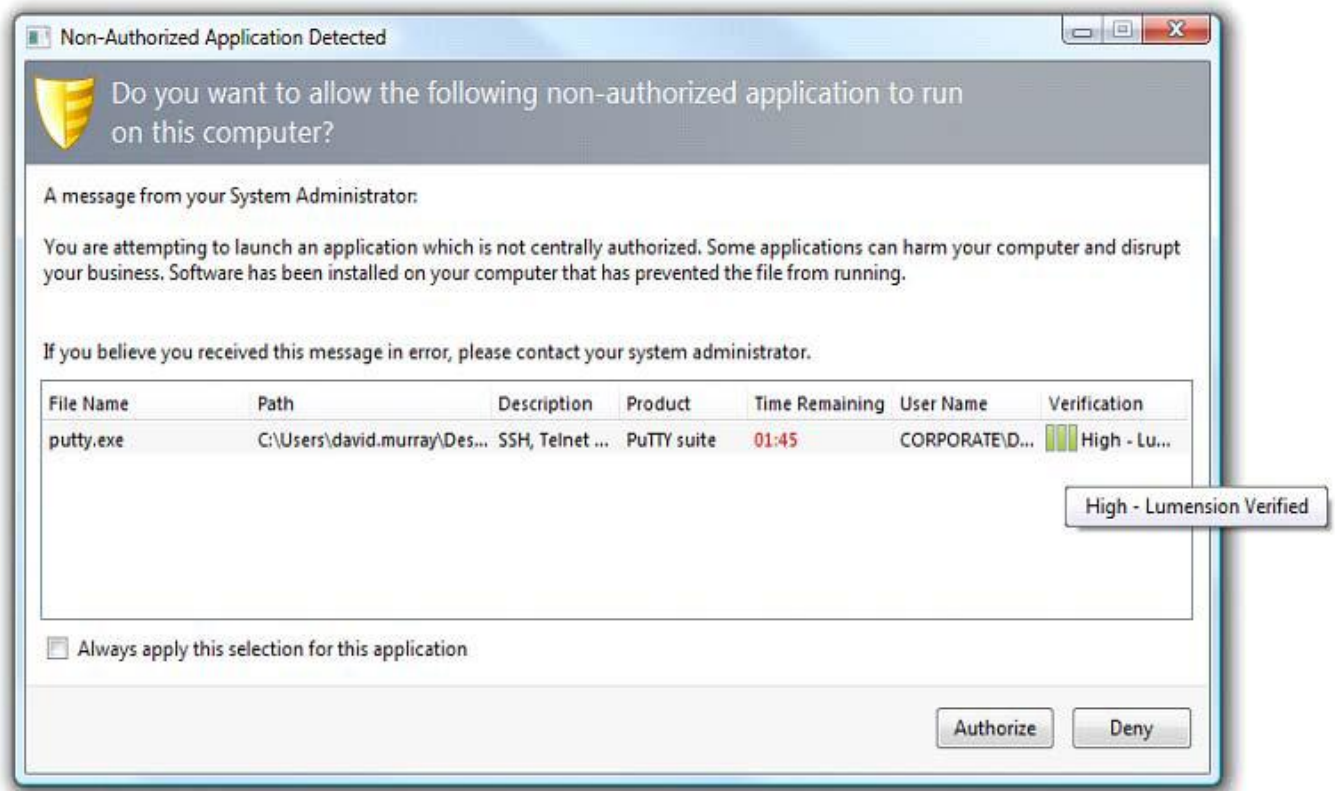
- Using Local Authorization on endpoints in Easy Auditor can provide a level of assurance that these endpoints are really ready to go into full blocking mode (Easy Lockdown). It can be difficult to take that final step because of fears that applications will be blocked across a range of endpoints resulting in lots of support calls and lost productivity. These fears can be mitigated by using Local Authorization to provide end users with the ability to authorize applications which would otherwise have been blocked. In the event that the users are not receiving Local Authorization dialogs (which you can tell by reviewing the Local Authorization logs on the server), you can now be assured that these endpoints are ready to go into Easy Lockdown as they are already in a blocking mode (with Local Authorization).

- Local Authorization can also be used on test endpoints to provide an immediate indication of any executables which would have been blocked if the endpoints were in lockdown. When you receive a Local Authorization prompt on these endpoints, you can then go and immediately update the policies to cater for this situation rather than having to wait for the daily/weekly application event log query email notification. Occasionally, when you review the application event log queries it can sometime be difficult to determine from the blocked executable which application is actually being blocked and what policy needs to be created or updated to address it. In the case of Local Authorization there is a much more immediate cause and effect relationship. In addition to being a prompt to go and update your policies, you now probably know without any analysis which application is associated with this blocked executable.

» Local Authorization acts as a control on malware spreading throughout your environment. As each user is requested to authorize any new executable for their endpoint, the spread of malware is limited by the number of users who authorize this new executable.

LEVERAGE CLOUD-BASED REPUTATION DATA

The Local Authorization dialog presents the user with a file verification rating which is obtained dynamically from the *Lumension*® Endpoint Integrity Service (EIS). This can be leveraged by users along with the other file metadata presented in the dialog to make authorization decisions.



You should provide training for your users so that they understand why they are being requested to authorize executables and how to use the metadata, including the cloud-based file reputation data, to make the correct decision.

REVIEWING LOGS WHEN LOCAL AUTHORIZATION POLICY IS APPLIED

Once a Local Authorization policy is applied to the endpoint, you will no longer receive any entries in the "Easy Auditor: Applications Blocked when Enforcement is Enabled" application event log query as all "blocked" executables will now be presented for Local Authorization. Instead, log entries will now appear in the "All applications executed by Local Authorization" log query. You should replace your daily/weekly

scheduled application event log query by an "All applications executed by Local Authorization" log query so that you continue to receive a regular email as a reminder to review the logs and update the policies. Endpoint users may authorize unwanted applications using Local Authorization. Review the logs for any such applications and update your denied applications policies as appropriate.

MAINTAIN A TEST ENDPOINT

Executables need to be in the Application Library so that they can be authorized or denied. If the executables are not already in the Application Library, you will need to maintain a test endpoint onto which these applications can be added and then the endpoint can be scanned via Easy Auditor to add them to the Application Library.

As you review the executables which are being authorized or denied by individual users via Local Authorization, you may want to authorize or deny these executables for all users. Maintaining a test endpoint onto which you add these applications will facilitate this process.

CONTINUE TO RAMP

Remember that no two endpoints are the same. Just because you have successfully migrated a small number of endpoints from Easy Auditor through policy creation and are now ready to go into Easy Lockdown, it does not mean you can simply apply Easy Lockdown to all the endpoints in your environment.

Different endpoints will have different applications, different versions of applications and different versions of application updaters and your policies need to be updated to cater for these differences.

As you progress through the monitor phase you should ramp up the number of endpoints being monitored and progress these to Easy Lockdown in a phased manner in the Enforcement phase.

Monitor Phase Summary

This phase is used to monitor the logs and update policies in preparation for going into blocking mode. You can also use Local Authorization in this phase both to introduce users to the concept of L.E.M.S.S.:AC and also to provide assurance that the endpoints are ready to take that next step into Easy Lockdown.

The monitor phase represents the end of the preparation. Once this phase has completed you are ready to move endpoints into lockdown.

Monitoring should continue for at least a month and should encompass at least one (1) Patch Tuesday and ideally a major corporate event such as a quarter-end.

Phase 5: Enforce

Once the logs have been monitored for a period of time, policies have been created and the logs have stabilized so that no unexpected entries have appeared for a period of at least one (1) month, you should now start to move these endpoints into Easy Lockdown.

In this phase you will:

- Communicate with users so that they understand that their endpoints are going into lockdown, what this means to them and what the escalation process is to get assistance in the event of problems.
- Conduct a thorough AV scan prior to lockdown because a significant period of time will have elapsed since the Easy Auditor scan was conducted.
- Apply the Easy Lockdown policy.
- Authorize blocked applications when required.
- Use Local Authorization judiciously to provide additional flexibility.

Communicate with Users Prior to Lockdown

Prior to putting them into lockdown, you should communicate clearly with the affected users so that they understand the impact of the change that is about to take place and the process by which they can get assistance in the event that applications they need to perform their job are being blocked. In particular, if you have not already done so, you should customize the blocked notification dialog (under Tools > Options > Application Control tab) to provide a customized message including your corporate logo and possibly a link to the help desk ticketing system or to a location from where they can download approved software. This helps your users understand that this message has been generated by your IT organization rather than appearing as a generic 3rd party message which might be perceived as suspicious or confusing.

Conduct a Thorough AV Scan

As a precautionary step, you should also conduct a thorough AV scan before initiating the Easy Lockdown as a significant period of time will have elapsed since the Easy Auditor scan was conducted.

Apply the Easy Lockdown Policy

As with Easy Auditor, you should implement Easy Lockdown on a phased basis, starting with a number of test endpoints and ramping this up over time with additional groups after the Easy Auditor logs have stabilized for that group.

To move endpoints from Easy Auditor to Easy Lockdown you can simply edit the Easy Auditor policy and convert it to an Easy Lockdown policy.

Authorizing Blocked Applications

Although you may have taken all the necessary steps to create the various Trusted Change policies and monitored the logs for an extended period of time prior to going into Easy Lockdown, there may still be situations in which applications will be blocked and action will need to be taken to authorize these applications. Examples of such situations include:

- **Infrequently updated applications.** Some applications update very infrequently and may have been missed because the monitoring period was not long enough to see an update occurrence. The updated application will now be blocked and will need to be authorized (e.g., via a Supplemental Easy Lockdown/Auditor policy) and a Trusted Updater policy (or other Trusted Change mechanism) will need to be applied to cater for future updates of this application.
- **A new application is required to view a file.** A user receives a file from a customer (e.g., video clip) which requires a specific application or plug-in to be viewed. This is legitimately blocked as you are now controlling which applications can be executed by your users. You should implement a process by which users can request approval for new applications. Once this application has been reviewed and approved, it can then be scanned on a test endpoint and authorized for all users or specific groups as appropriate.
- **Unusual/Unsupported application update patterns.** L.E.M.S.S.:AC has been designed to minimize the administrative burden by providing mechanisms such as Trusted Updater to allow for application updates to be automatically whitelisted without any administrator intervention. As outlined earlier, there is no standard mechanism by which applications get updated and they may also use different mechanisms for major and minor releases. Applications which update in an unusual manner may be blocked and will need to be authorized separately. You may want to consider disabling automatic updates where possible to avoid such occurrences. Approved updates can then be sent out to your endpoints using your normal software update tools.

Local Authorization

As with Easy Auditor, if a Local Authorization policy is applied in Easy Lockdown the user will have the option to authorize otherwise blocked applications. If you have been using Local Authorization with Easy Auditor you might want to consider leaving the Local Authorization policy in place for a short period after the Easy Lockdown policy has been applied to provide additional assurance that users will not encounter any issues associated with Easy Lockdown.

However, note the following points:

- Any executables that are authorized via Local Authorization post-lockdown will no longer be authorized once the Local Authorization policy has been unassigned. These applications will then be blocked if the user attempts to execute them. If you plan to remove the Local Authorization policy after going into lockdown you should monitor the logs carefully and authorize any executables that will be required once the Local Authorization policy has been removed. Alternatively, reapply the Easy Lockdown policy so that the whitelist is recreated for that endpoint.
- The Local Authorization is specific to the user to whom it is assigned. Any executables authorized by a user are authorized for that user on that endpoint only. If an endpoint is shared among a number of users, users who do not have Local Authorization capabilities will be unable to launch any executables that have been locally authorized by others.

To maintain flexibility and minimize administrative burden, you could also leave the Local Authorization policy in place indefinitely. A benefit of this approach is that it maintains flexibility while limiting the spread of malware in your environment to the endpoint which locally authorizes that malware to run.

Enforcement Phase Summary

In the enforcement phase endpoints are moved into Lockdown. If the necessary Trusted Change policies have been implemented and the logs monitored for a period of at least a month, this should be a seamless transition from Easy Auditor. Local Authorization can be used to help ease that transition by providing a mechanism for users to authorize otherwise blocked applications.

Having achieved the goal of locking down your endpoints with L.E.M.S.S.:AC, you can now move on to manage your L.E.M.S.S.:AC deployment.

Phase 6: Manage

Now that endpoints are in Lockdown, you are now in control of the applications which can execute in your environment.

In this phase you will:

- Continue to monitor logs and update Trusted Change policies as required.
- Organize files in the Application Library so that applications can be authorized.
- Use Local Authorization to authorize applications in time-critical situations or to support disconnected users.
- Ensure that a process has been implemented so that users can request approval for new or blocked applications.

Maintain Trust Policies

Continue to monitor logs in Easy Lockdown to determine whether policies need to be updated. In particular, review the "All Denied Application Events" and "Most Frequently Denied Applications" event logs to review executables that have been blocked to determine whether any of these should be authorized or whether communications need to be sent out to the user community to inform them of alternative approved applications and where to obtain them from.

You can schedule these queries and have the results emailed to you as a reminder to review the logs occasionally. The scheduling frequency that should be used will depend on various factors such as the size of the logs and number of endpoints but, assuming you have an escalation process for blocked applications whereby users can get a quick turnaround to address productivity issues, it should be sufficient to review these logs weekly. The goal here is to review trends and understand user behaviour so that you can best serve the needs of your users while still maintaining a secure environment.

Organize Files in the Application Library

Prior to going into lockdown, the focus for the Application Library has been on denying executables/applications that you want to prevent from running in your environment. Once endpoints are in lockdown, you will also need to be able to authorize applications.

- These might be applications that have been blocked and need to be authorized for that user and/or for other users.
- These might be applications which have been locally authorized by a user for their endpoint and you may want to authorize this application for other users.

In either case, you need to organize the files in the Application Library into Applications and Application Groups so that they can be authorized.

ORGANIZING FILES INTO APPLICATIONS

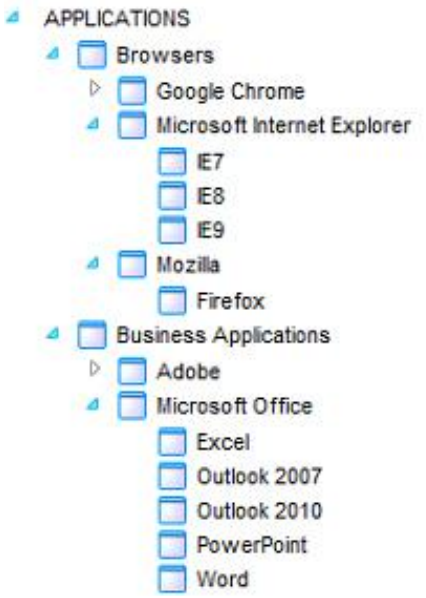
Files can be organized in a number of different ways and you should give some thought to the best strategy for your organization. Folders in the Application Library can be nested up to three (3) levels deep, so a possible implementation would be as follows:

Level 1 = Application Category (e.g., Browsers, Operating Systems, Games, Business Applications)

Level 2 = Application Vendor & Product (e.g., Google Chrome, Microsoft Office, Apple iTunes)

Level 3 = Sub-Product and/or Version (e.g., IE7, Excel 2007, iTunes 10.5)

For example:



Note that the application names must be unique at each level (e.g., you cannot have a “Microsoft” application under both Browsers and Business Applications). This is necessary because these applications will be subsequently organized into Application Groups.

ORGANIZING APPLICATIONS INTO APPLICATION GROUPS

You can organize Applications into Application Groups so that they can be authorized or denied as a group rather than on an individual basis.

Authorizing Applications: Supplemental Easy Lockdown/Auditor Policy

Supplemental Easy Lockdown/Auditor policies can be used to centrally authorize executables or applications and update the endpoint whitelists for the users to which the policy is assigned. This could be used to:

- Authorize executables or applications for users when they have been blocked on their endpoints.
- Authorize executables or applications for users even when those executables or applications are not yet installed on their endpoints.

Once files have been grouped into Applications and Application Groups it is then possible to authorize specific Applications or Application Groups for some or all users/endpoints via a Supplemental Easy Lockdown/Auditor policy. This policy works in conjunction with the Easy Auditor or Easy Lockdown policy in that it supplements the whitelist which has been created via Easy Auditor/Lockdown. Files which are in the Application Library can be authorized for users/endpoints regardless of whether those files already exist on those endpoints. If those files are subsequently added to the endpoint, they are already whitelisted so will be permitted to execute.

Tip: You can use the logging options in the Supplemental Easy Lockdown/Authorization policy to understand if specific applications are being used. This can be useful if you are trying to remove certain applications or application versions from your environment. However, do not use this logging option generally for all applications authorized by this policy as this will result in large numbers of logs for applications that are used widely.

MAINTAIN A TEST ENDPOINT

Executables need to be in the Application Library so that they can be authorized or denied. If you have not already established a test endpoint to scan new applications, you should do this now so that any applications you want to authorize can be scanned and added to the Application Library.

Installing New Applications via Local Authorization

While in Easy Lockdown, there will also be situations whereby assigning a Local Authorization policy is the best option to quickly authorize blocked applications. Use Local Authorization in time-critical situations (i.e., need to get this application authorized in the next few minutes) or in situations where a user may be discon-

nected from the corporate network and may need the ability to install new software (e.g., a sales engineer visiting a customer site). In this latter case, the Local Authorization policy would need to be assigned in advance of them disconnecting from the network.

In either case, prior to unassigning the Local Authorization policy, you should review the logs and decide whether the locally authorized executables should be added to either authorized or denied applications policies.

Requesting Approval for New Applications

Change is inevitable and you need to manage evolving user and business needs. In addition to the reactive escalation process for addressing blocked applications, you also need to implement a more proactive process for introducing change so that IT is the organization that enables rather than inhibits business. You need to have flexibility and you need to decide how much flexibility you want to provide and how you approach balancing security and flexibility across the organization.

Once you have defined the change control process you need to communicate this to users so that they understand how to request approval for new applications ahead of time.

Manage Phase Summary

Now that endpoints are locked down and in a manageable state, you will continue to monitor logs for any anomalies:

- Blocked executables that need to be authorized.
- Executables that have been locally authorized that should be denied.
- Executables that have been locally authorized by one user that should be authorized for other users.

You will group files into Applications and Application Groups in the Application Library so that they can be authorized as such instead of individually.

You can use Local Authorization to enable users to authorize files locally in time-critical situations or when they may need flexibility to add software to their endpoints when they are disconnected from the corporate network.

Finally, you need to document and communicate a change control process so that you maintain flexibility to proactively meet changing business and user needs while still maintaining a secure environment.

Summary

This document has been written to provide a best practice process for administrators when implementing L.E.M.S.S.:AC in their environments. Hopefully you find this to be useful as you roll the product out in your environment.

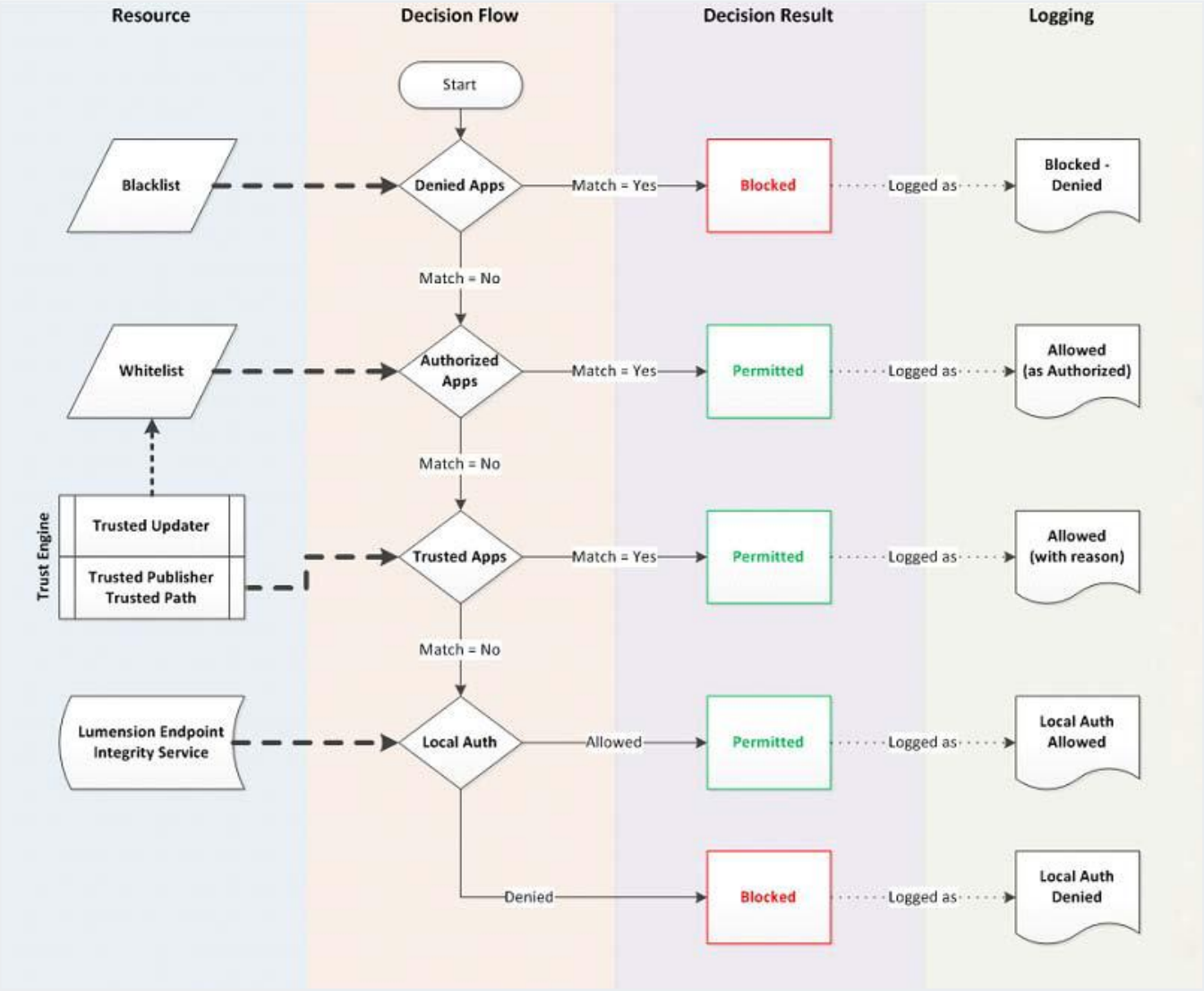
If you have invested correctly in these phases, you should be able to reap the rewards of that investment once you have gone into Easy Lockdown. You will still need to plan for ongoing change and maintenance and you will need to have a process in place to handle escalations associated with blocked applications. You should also review logs for trends that will help shape the strategy for the software that is authorized for use in your environment. However, due to the use of the Trusted Change policies, the administrative burden should not be that significant. You should now be in a manageable state.

If you have any suggestions for product improvements as you work through the implementation, please input these using the Lumension Product Feature Request form available at http://www.lumension.com/Customers/Product-Feature-Request.aspx

If you identify any issues in this document or any best practices you think should be added, please send an email to support@lumension.com with the details.

Appendix: Decision Flow at the Endpoint

To help you understand how L.E.M.S.S.:AC works, the following diagram depicts the decision flow at the endpoint and the workflow that is followed to determine whether to allow or block an executable.



About Lumension Security, Inc.

Lumension Security, Inc., a global leader in endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, Antivirus and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Texas, Florida, Washington D.C., Ireland, Luxembourg, Singapore, the United Kingdom, and Australia.

Lumension: IT Secured. Success Optimized.™

More information can be found at www.lumension.com.

Global Headquarters

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255 USA

phone: +1.480.970.1025

fax: +1.480.970.6323