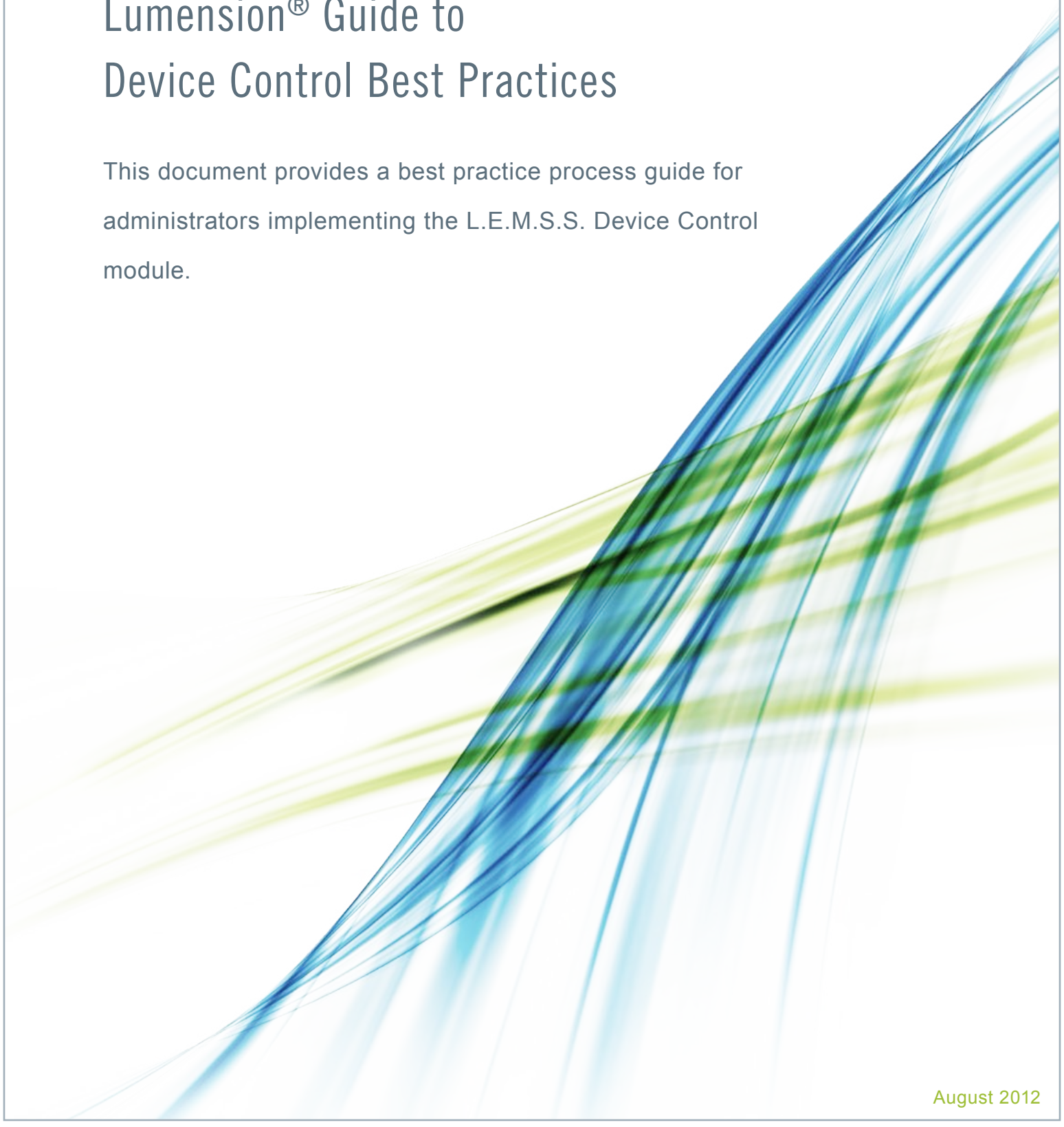
Lumension® Guide to Device Control Best Practices

This document provides a best practice process guide for administrators implementing the L.E.M.S.S. Device Control module.



August 2012

WP-EN-08-20-12

Table of Contents

Introduction

The *Lumension*® Device Control (LDC) is delivered as an integrated module in the *Lumension*® Endpoint Management and Security Suite (L.E.M.S.S.). It enforces flexible usage policies for removable devices, removable media, and data (such as read/write, encryption) that enable organizations to embrace productivity-enhancing tools while limiting the potential for data leakage and its impact.

With LDC, you can:

- Enable productivity and reduce insider risk by centrally managing security policies regarding the use of removable devices (e.g., USB flash drives) and media (e.g., CDs/DVDs/) through a flexible device whitelist approach.
- Ensure data is encrypted and secure when on removable devices / media, using the FIPS 140-2 Level 2 validated cryptography capability.
- Prevent malware intrusion via removable devices / media, adding a layer of protection to your network.
- Ensure protection whether or not endpoints are connected to the network.
- Provide the visibility, forensics and reporting needed to demonstrate compliance with applicable laws via patented bi-directional shadowing.
- Leverage a seamless layer of protection within your defense-in-depth strategy via the integration with L.E.M.S.S.

This document is a practical guide intended to assist you with the deployment of Device Control module within your organization.

What do you want to do?

Before you start to install or deploy LDC, you should have a clear understanding of what you want to accomplish. LDC is very flexible, and can be used for a wide array of enforcement goals. LDC is successfully used in organizations with policies ranging from extremely strict to minimally intrusive. Determining what levels of enforcement your organization needs in the beginning will best prepare you for a successful implementation.

Organizations typically fall into one of three categories:

- **Permissive**: These organizations are looking to do little in terms of enforcement. The primary goal is usually auditing and reporting of user activity, or the need to address a very specific issue such as limiting the access to USB-connected Removable Storage Devices to Read-Only. The written data

security policy at these organizations is usually informal or brief. External regulations and compliance concerns are minimal or non-existent.

- **Moderate**: Most organizations fall into this category. These organizations typically have a written data security policy and want to be able to enforce that policy without relying on voluntary user compliance. Their goal is to prevent any specifically unauthorized usage, and allow flexibility in permitted usage cases to result in maximum organizational productivity. These organizations typically have some external audit or compliance needs they must address, such as encrypting all data-at-rest (including data transferred onto USB flash drives).

- **Stringent**: These organizations deal in highly confidential information, and are typically very closely monitored either from within the organization or by an external authority. The goal of these organizations is to prevent all types of device usage except for very specific cases which are allowable according to their data security policy. Device usage may be restricted to encrypted devices, and every file transferred to or from devices is retained and reviewed.

Determining which category your organization fits into provides a good baseline perspective when determining how to configure LDC policies as you deploy.

If your organization has a written security policy, determining what you want to do should be straightforward. Simply identify the allowed usage cases in the policy and make a list of those cases. You can then create an LDC policy for each case.

If your organization does not have a written security policy, you should develop one.[1] As part of this exercise, you will have to determine the appropriate level of permissiveness for your organization. The following section may help inspire some thoughts about what is possible with LDC.

1. Note that a written security policy is required by law in many jurisdictions and other regulatory requirements (e.g., PCI).

What can you do?

When starting to define how you will enforce policies, it helps to break the problem down into smaller components. By addressing each different aspect of the problem one component at a time, you can more effectively develop your plan without leaving gaps in your enforcement. Do your planning around the capabilities of the enforcement tool you are implementing. By making sure you consider each aspect of the tool's capabilities your planning process will be simpler and the resulting strategy will be more complete.

You want to consider the most restrictive permissions you can. By not allowing any access to a particular device or device class, you are reducing the risk of malware introduction from those devices. If you have to allow users to read data from devices, do you need to allow them to read *any* file from a device, or can you limit that access to certain types of files. Can you limit access to Microsoft Office documents and Adobe PDF files? That would also reduce the risk of allowing executable malware from transferring itself onto your endpoints.[2]

In cases where you must allow both read and write access, can you limit those file types? Can you limit the amount of data being copied to devices in a 24 hour period? That would mean a smaller risk of a major data breach. Can you limit that access to endpoints connected to the network? Can you limit the times of day or days of the week which access is allowed?

LDC provides a lot of flexibility in terms of enforcement. It's unlikely that your organization has an enforcement need which LDC cannot accommodate. LDC operates on a *default-deny* principle. This means that you only need to consider the usage which you want to allow, and create policies to allow those cases. Everything else will be prevented. This means that you don't need to worry about devices you don't know about, or users you haven't authorized.

When thinking about how you will apply policies, it helps to think about the types of permissions you want to allow on different device classes, to which groups of users or endpoints those policies should apply, and when and where those policies should apply.

2. For our purposes here, endpoints include computing devices like workstations, desktops, laptops and servers.

Device Classes

When a device is connected to a Windows endpoint, it registers itself with the Operating System (OS) as one or more device classes. LDC manages access by these classes, so plan your policies based on this. LDC manages the following device classes in Windows:

Physical Interfaces USB	Wireless Interfaces	Device Types
FireWire	Wi-Fi	Removable Storage Devices
PCMCIA	Bluetooth	External Hard Drives
ATA / IDE	IrDA	CD / DVD Drives
SCSI	Wireless NICs	Floppy Drives
LPT / Parallel		Tape Drives
COM / Serial		Printers
PS/2		Modems / Secondary Network Access Devices
		PDAs and other handhelds
		Imaging Devices (Scanners)
		Biometric Devices
		Windows Portable Devices
		Smart Card Readers
		PS/2 Keyboards
		User-Defined Devices

Table 1 – Supported Device Classes

There are different capabilities within each class. Some can simply be set to allow or block all access, others can be configured as no access, read only, or read and write access. Commonly used classes such as CD/DVD drives (readers / burners) and Removable Storage Devices can be further configured to use encryption and limit the types of files which can be transferred to and from the device or media.

Within some classes, you can set different policies based on the model of the device connected, or more specifically by the unique device, using a unique ID number in the device. For example, within the Removable Storage class, you can set one type of permissions for a specific model of flash drive, and a different set of permissions on all other flash drives. Furthermore, you can authorize specific users to use a specific device, while preventing any other users from accessing that device.

Permission Types

There are several levels of permission which can be enforced with LDC. While not all permission levels are supported by all classes, the most common classes are the most flexible. Here are the permissions you can enforce, by device class, with LDC:

Permission Type	Description	Device Classes Supported
Block all Access	Both read and write access to the device is blocked.	All device classes. **Note**: Human Interface Devices (HID) and the primary hard drive are never blocked. The only exception is that the keyboard can be configured to be blocked when a keylogger is detected.
Read Only	Data may be transferred from the device to the endpoint.	Citrix Network Shares CD/DVD Drives Floppy Disk Drives LPT/Parallel Ports Removable Storage Devices
Read+Write	Data may be written from the endpoint to the device, and read from the device to the endpoint. Note that read permission is required to grant write permission.	All device classes.
Encrypt	Allows the user to encrypt devices or media using LDC's encryption. Encryption methods and determining how devices can be accessed are configured in other settings discussed later in this paper.	CD/DVD Drives Removable Storage Devices

Permission Type	Description	Device Classes Supported
Export to Media (encryption key)	When encrypting a device or media, this allows the user to place the encryption key on the device itself. The key is password protected. The password unlocks the key which then provides access to the data on the device. This is the most convenient method of encryption, since the user needs only the device and the password to access the encrypted data.	CD/DVD Drives Removable Storage Devices
Export to File (encryption key)	When encrypting a device or media, this allows the user to place the encryption key on a separate file, which is password protected. In order to access the data on the encrypted device, one must have the device, the separate encryption key file, and the password. This is the most secure method of encrypting devices since the key file, the password, and the device are required to access the device	CD/DVD Drives Removable Storage Devices
Import from File (encryption key)	This allows the user to use an exported encryption key file to unlock an encrypted device.	CD/DVD Drives Removable Storage Devices
Decrypt	This allows a user to destroy the data on an encrypted device. This action has the effect of formatting the device as a new unencrypted volume. Data on the device is lost. *Note: Decrypt should not be confused with unlocking an encrypted device to access the data on the device.*	CD/DVD Drives Removable Storage Devices
Copy Limit	This limits the amount of data a user can copy to external devices in a 24-hour period. Setting reasonable copy limits can reduce your exposure to data loss.	Floppy Disk Drives Removable Storage Devices

Permission Type	Description	Device Classes Supported
Shadowing (filename only)	This records the name of files which are transferred to or from devices. All details such as the machine name, user name, time and date, etc. are also recorded. The shadowed copy can be accessed through the L.E.M.S.S. console.	CD/DVD Drives Floppy Disk Drives Removable Storage Devices
Shadowing (full file)	This retains a complete copy of every file transferred to or from devices. The shadowed copy can be accessed through the L.E.M.S.S. console.	COM/Serial Ports[1] CD/DVD Drives Floppy Disk Drives LPT/Parallel Ports[1] Modem/Secondary NIC[1] Removable Storage Devices [1] Write Only
File Type Filtering	This feature allows you to control the specific file types which can be copied to or from devices. The file content is inspected; the file extension (which can be altered) is not used for enforcement. You can control the import and export of file types separately; for example, you may allow the reading of Microsoft Office documents but only allow the writing of PDF files.	Floppy Disk Drives CD/DVD Drives Removable Storage Devices

Table 2 – Types of Permissions

Users and User Groups

Typically you will find that your written policies are centered on people, not machines. Different policies may apply to people in different locations or at different organizational levels within the organization. It's best to center your enforcement around users as well. Most likely, your organization has already invested heavily in building and maintaining an Active Directory (AD) structure which supports the different needs of the various groups of users. To duplicate that structure in an enforcement tool and try to keep both equally maintained would be very inefficient. Capitalize on the work already done with your AD, and keep one structure to maintain.

Lumension® Endpoint Management and Security Suite (L.E.M.S.S.) has an AD Sync feature. LDC leverages this platform capability to allow for policies to be applied to users, user groups, endpoints, AD Organizational Units (OUs), and endpoint groups – which can be system endpoint groups or custom endpoint groups.

- When a policy is applied only to a user or user group, it applies to those users on all endpoints.
- When a policy is applied only to an OU, endpoint, or endpoint group, it applies to all users on those endpoints.
- When a policy is applied to a combination of users and endpoints, it applies only to those users when they are logged onto those endpoints.

It is best to use User Groups when assigning Device Control policies. Typically you will find that this is how you want to enforce policies instead of by endpoint group. This can be a shift in thinking, especially for operational IT organizations which are accustomed to managing other functions such as patching or anti-virus by endpoint. Using User Groups allows for more efficient policy distribution and enforcement by LDC, and will ultimately reduce your Administrative workload after LDC is deployed.

To ease the administrative workload after deployment, assign as many policies as possible at the largest groups of users, and then consider exceptions.

The largest group of users is the built-in account known as "Everyone." This account includes every other account, including users, administrators, and service accounts, both local and domain. Policies assigned to Everyone will be unilaterally applied.

AD User Groups are the next largest and most common assignment target for device control policies. Organizational policies typically align well with existing groups you have configured in your AD, for example *Sales, Executives, Managers,* or *Tokyo Office*. Leveraging the work your organization has already put into organizing AD is a very efficient way to assign policies, and will result in the least amount of administrative overhead for you in the future.

Many customers choose to manage LDC policies exclusively through AD after initial configuration, rather than using the L.E.M.S.S. console. To do this, you create AD groups and policies which align with those groups. For example, create a policy which allows read-only access to CD/DVD drives, and a corresponding AD group called DVD-CD-Read-Only. In LDC, assign this policy to this AD User Group. Adding and removing users from the AD group as personnel changes are made will result in the policy being applied to them as they are added and not applying when they are removed. You can create policies and corresponding AD groups for all levels of access you wish to permit, such as Read+Write to removable storage devices, those which are approved to burn CDs, administrators or service accounts allowed to use tape backup drives, and so on. You could also assign a set of policies to different user groups with different access levels such as Trainees, Managers, Directors, and Executives. As employees move from one group to another in AD, the LDC policies associated with that group will automatically apply to them.

Individual Users are the most finite level of policy assignment to users. Use this type of policy assignment only to deal with exceptions. Customers who have attempted to manage every individual user's permissions at the user level find the overhead to be too great to be practical. An example of a case which would require assignment to individual users may be a policy which requires everyone to use encrypted devices only, with the CEO is permitted to use both encrypted and unencrypted devices.

Endpoints and Endpoint Groups

Using Endpoints and Endpoint Groups is a less efficient method of assigning policies, so these should be used only as required. Hardware changes, is refreshed, and sometimes moves. Trying to keep up with these changes in your policies will be a challenge. Also, because policies assigned only to user objects are the same on every endpoint, they can be distributed as a single policy. Endpoint-specific policies must be also distributed to endpoints, but since each is unique, a policy file per endpoint-specific policy must be distributed. When done for a large number of endpoints, this can result in large policy files being transmitted across the bus and through your network.

Recall that policies assigned only to endpoints or endpoint groups will be applied to all users on those endpoints.

Suitable situations for endpoint-specific policies are those in which the endpoint serves in a relatively unique role, such as a computer in a lobby or other publicly accessible area which should never have devices attached to it, or perhaps a server which needs specific hardware devices to perform its function and those devices are inappropriate outside of that scenario.

LDC policies can be assigned to any group of endpoints in L.E.M.S.S., including system and custom groups. System groups include the AD groups you have configured, and several other groupings such as IP subnets, OSes, virtual machines, and more. Custom groups are fully user defined, and membership can be based on AD membership, system groups, or manual configuration.

When and Where

By limiting when and where users can use devices, you are reducing your risk for data loss and malware introduction. It's not always practical to introduce these limitations, but where it can be done it contributes to your overall security posture. If local printers shouldn't be used on weekends, or a computer in a common area doesn't need to have device access after working hours, why not close that window of opportunity for unwanted usage?

LDC allows for different policy enforcement in different contexts. The most common type of policy enforcement is Always. These policies are applied without regard to context.

Another type of policy enforcement is *Scheduled*. Scheduled policies are in effect for a time range and on the days of the week which you specify. If a particular device should only be accessible during office hours and not accessible after hours or on weekends for example, then use Scheduled policy enforcement.

When you want to enforce different levels of restriction based on whether or not the endpoint is in the organizational network, you can use *Online* and *Offline* policy enforcement. Online policies will be enforced when the endpoint can contact the L.E.M.S.S. server, and Offline policies will be enforced when the endpoint can not contact the L.E.M.S.S. server. You would typically configure Online and Offline policies in pairs, assigning them to the same assignment target (user, user group...). These are normally used instead of a policy with Always enforcement. This allows you to apply a more restrictive policy when the endpoint is out of the network; for example, preventing field personnel from copying data off of their endpoints when at customer sites or turning Wi-Fi off while connected to the network in order to prevent bridging.

Temporary policy enforcement will result in the policy being automatically revoked after the period you specify. Normally these are not utilized in the initial roll-out of LDC, and are used more for daily administration such as allowing access to a USB drive from a conference room computer for an hour. However, some organizations, particularly those with high employee turnover such as external contractors use Temporary policies in place of Always policies. In this case, they may assign permissions to users for a temporary period of 6 months or one year. At the end of the temporary period, the policy must be extended by the Administrator or it expires and the permissions are automatically removed, reducing the need to maintain the list of users on an ongoing basis.

LDC also allows for the granting of *Temporary Permissions Offline*. These are used to allow a user access to a device when the endpoint cannot connect to the L.E.M.S.S. server to receive a policy change. This is a maintenance activity rather than an initial configuration concern and is covered in a later section in this paper.

Summary

When planning the practical enforcement of your data security policy, there are several factors to consider, and several options available to meet your needs. It's worthwhile spending time to plan how you will construct and apply your policies. Changing strategies after deployment results in a duplication of effort on your part, and can result in enforcement gaps if something is overlooked.

Take the time to write out your enforcement strategy on paper. As you go through the planning process you will adding more detail and will sometimes want to go back to revisit decisions you had made earlier in the process. A working copy of your strategy on paper is a useful tool during this period.

For each Device Class, determine whether or not that class is used in your organization or should be allowed by your policy. If not, then the strategy for that class is simply not to define any policies which apply to that class. The default-deny nature of LDC will prevent access to devices in that class.

If there are devices in that class which need to be allowed access, determine the highest level of granularity you need to manage those devices. The best option is to manage the entire class uniformly. This means you would be giving all devices in that class read access only, or read+write access for example. If you can't allow the same access for all of the devices in a particular class, then you can use Device Collections. Device Collections allow you to group devices of the same class together and you can apply different sets of permissions to different collections, and an entirely different set of permissions for devices you have not placed into a collection. Device Collections are discussed in more detail later in this paper.

Likewise, when considering the policy assignments work from the highest level possible. Start with the largest group of users possible, the built in user *Everyone*. Policies assigned to Everyone will apply to all AD and local users, system accounts, and service accounts. If Everyone is not appropriate, then select an AD User Group or groups which match the intended policy enforcement. Use individual AD users for exceptions to the standard policies. Only assign policies to endpoints as a last resort, when users won't work for the security policy in question (e.g., a kiosk in the lobby).

Policy Applicability	Policy Assignment
1. Device Class 2. Device Collection	1. Everyone 2. AD User Group 3. AD User 4. Endpoint Group, Endpoint, OU

Table 3 – Policy scope in order of preference to reduce administrative workload after deployment

The table below can be used as a worksheet to aid you in creating your policy strategy.

Device Class	Permissions (Read, Write, Encrypt, Decrypt, File Type Filters, Copy Limit, Shadowing)	Policy Enforcement (Always, Online, Offline, Scheduled)	Policy Assignment (User Group, User, Endpoint Group, Endpoint)
Biometric Sensors			Must be '*Everyone*' or '*LocalSystem*' since device is used prior to user login
Citrix Network Shares			Must be User/User Group. Can not be endpoint or endpoint group based.
COM/Serial Ports			
CD/DVD Drives			
Floppy Disk Drives			
Imaging Devices			
LPT/Parallel Ports			
Modem/Secondary NICs			
Palm Devices			
Windows Portable Devices			
USB Printers			
PS/2 Ports			Must be '*Everyone*' or '*LocalSystem*' since device is used prior to user login
Removable Storage Devices			
RIM Blackberry Devices			
Smart Card Readers			Must be '*Everyone*' or '*LocalSystem*' since device is used prior to user login
Tape Drives			
User Defined Devices			
Windows CE Devices			
Wireless NIC			Must be '*Everyone*'. Can also be assigned to an endpoint or endpoint group

Table 4 – Policy Worksheet

Groundwork

Once you have a good idea of your enforcement strategy, the tangible work begins. Moving an organization from unfettered use of devices to a state of enforcing a device usage policy is a significant culture change and should be approached slowly and methodically. It's not simply a matter of deploying the enforcement into the production environment. You will need a communication plan, executive backing for the project, defined feedback mechanisms for users, and of course you'll want the deployment to go smoothly.

This section will walk you through some initial steps you can take with *Lumension*® Device Control (LDC) to make the deployment go more smoothly, and then revisit the importance of a good communication plan.

Preparing the Server for Client Deployment

There are steps to take to deploy the Device Control module to endpoints which are covered later in this paper. Before you reach that point, there are some considerations to plan for in configuring your server, which are covered in this section.

Reboot Required

The first consideration is that the installation of the Device Control module requires a reboot of the endpoint to complete the installation. The Device Control kernel level driver provides enforcement at a very low level in the OS for maximum security, and must be loaded early in the OS boot sequence.

Reboots can of course be disruptive, so there are three methods of managing the required reboot. Different methods can be applied to different groups of machines. This is accomplished through the use of Agent Policy Sets in *Lumension*® Endpoint Management and Security Suite (L.E.M.S.S.). Refer to the L.E.M.S.S. documentation for a full description of the use of Agent Policy Sets. Essentially, you can create different Agent Policy Sets and apply them to different endpoint groups in L.E.M.S.S. The agents on endpoints in those groups will abide by the settings in their respective Agent Policy Sets.

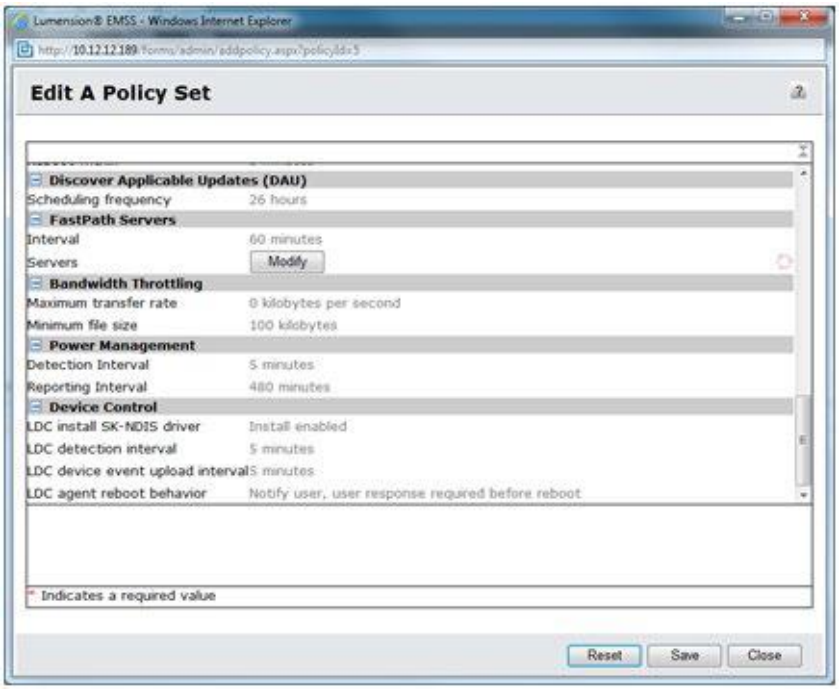


Figure 1 – Editing Device Control options in an Agent Policy Set

To configure the reboot settings for the Device Control module installation and un-installation, navigate to Manage>Agent Policy Sets in L.E.M.S.S. Edit the desired policy set. Locate the section of settings titled Device Control (not *Reboot Notification Defaults*). In the Device Control section, there is a setting called LDC Agent Reboot Behavior. This can be set to one of three values:

- **Notify user, user response required before reboot**: This value will prompt the end user with a dialog stating that the system must be rebooted. The system will wait indefinitely for the user to acknowledge and approve the reboot before initiating the reboot. The user will be able to save their work prior to approving the reboot. This setting is the default; it is good for endpoints which will have users present at some point, and where you do not wish to risk data loss of unsaved documents by rebooting the machine without user intervention.
- N**otify user, automatically reboot with 5-minute timer**: This value will prompt the end user with a dialog stating that the system must be rebooted. The dialog will contain a 5-minute countdown timer. The system will reboot when either the user approves the reboot, or at the expiration of the countdown timer if there is no user response. Use this setting for endpoints you want to reboot, but may have a user present.
- **Don't notify user, wait for next user-initiated reboot**: This value will not display a prompt, and will not reboot the endpoint. Keep in mind that the Device Control module is not active until after the endpoint is rebooted. You can remotely reboot the endpoint later if you have *Lumension*® Patch and Remediation (LPR) by deploying the Reboot Task. This setting is good for unmanned endpoints such as servers, ATMs, and kiosks which can be rebooted in a scheduled maintenance window.

NDIS Protection

The second consideration to take into account when deploying Device Control to endpoints is that of the NDIS control, SK-NDIS. SK-NDIS is a driver which allows LDC to control access to secondary network adapters in endpoints including Wi-Fi, Infrared, and Bluetooth devices. This allows you to prevent network bridging, for example, by disabling wireless network adapters such as 802.11 or Bluetooth when the endpoint is connected to the physical network. However, for endpoints such as servers which legitimately use multiple network adapters simultaneously, the driver may disrupt the network adapter configuration.

It is highly recommended you deploy Device Control to a test machines which represent your production machines as accurately as possible, and SK-NDIS is one of the reasons behind this recommendation. If you determine that SK-NDIS is introducing issues on machines with multiple network adapters, such as servers, you can configure the system not to install SK-NDIS on those endpoints.

This is also accomplished using Agent Policy Sets. Again, editing an Agent Policy Set, in the Device Control section, locate the setting LDC install SK-NDIS driver. There are two values:

» **Install enabled**: The SK-NDIS driver will be installed and started.

» **Do not install**: The SK-NDIS driver will not be installed on the endpoint.

Default Policies

As you are deploying the DC module to endpoints, you will want to be monitoring the success of those deployments and address any issues which you may encounter. You will not want to be addressing user crises introduced by enforcement at the same time. LDC helps you work the deployment and enforcement phases separately.

This is also important because you will want to deploy the DC module to start getting visibility into the devices being used your environment before you start enforcement. You may find that you will need to make some adjustments to your planned policies based on actual user activity.

Recall that LDC works on a default-deny basis. By deploying Device Control without configuring any policies, this would normally block all device usage. To ease the transition into enforcement there are two mechanisms to prevent this initial blocking of device access.

The first is *Audit Mode*. All Device Control enforcement is governed by the Global Device Control Policy which can be found at the top of the policy list on the Manage>Device Control Policies page. By default this policy is set to Audit mode. When in Audit mode, endpoints will not block device access, and no policies created in the console will be sent to endpoints. The other mode for this policy is *Enforcement Mode*. When in Enforcement mode, all policies which are enabled and assigned in the console will be distributed to endpoints and the endpoints will manage access according to those policies.

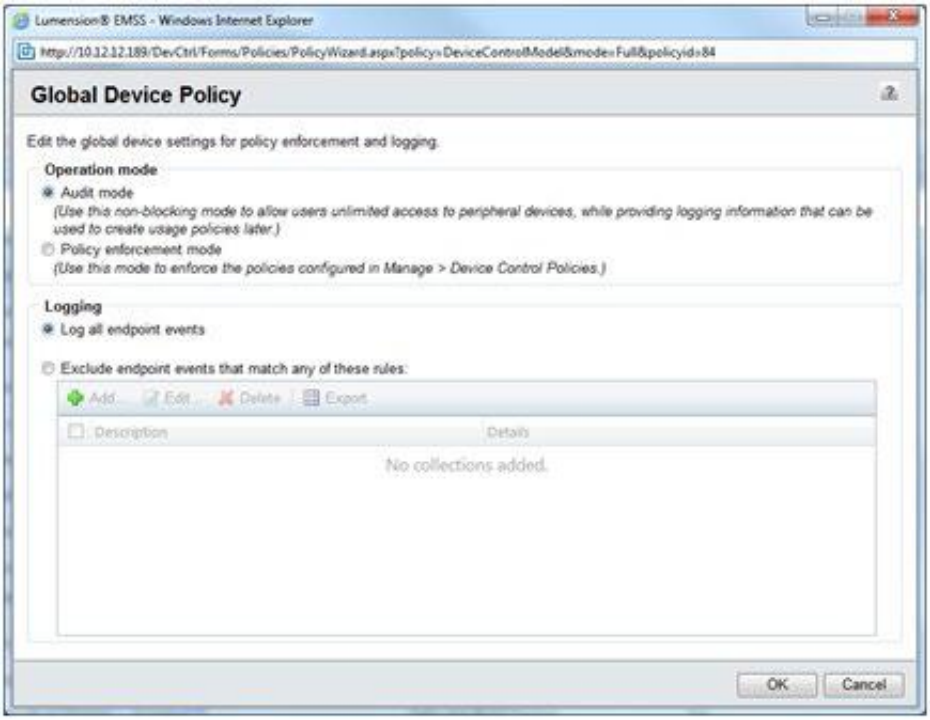


Figure 2 – Global Device Policy in Audit mode

The second mechanism is intended to allow you to roll-out enforcement device class by device class, rather than all at once. To accomplish this, there are Default policies for each device class pre-populated in the console. These policies allow for full access permissions for each class, and are assigned to the user Everyone. You can edit or disable these policies class by class to roll out enforcement, which is discussed later in this paper.

When you deploy the Device Control module, you will not start blocking access to devices if these mechanisms are in their default state.

AD Sync

When you developed your policy strategy, a large part of it – if not all – should have been based on user groups from Active Directory (AD). You'll need that AD information in L.E.M.S.S. The Device Control module leverages the AD Sync feature of L.E.M.S.S. Configure your AD Sync from the Tools>Directory Sync Schedule page.

The AD Sync will bring User Group and OU information into L.E.M.S.S. You can sync to a single domain, multiple domains, or parts of a domain. For domains with frequent changes, you can configure more frequent sync schedules. For domains which change infrequently, you can configure the sync to occur at longer intervals.

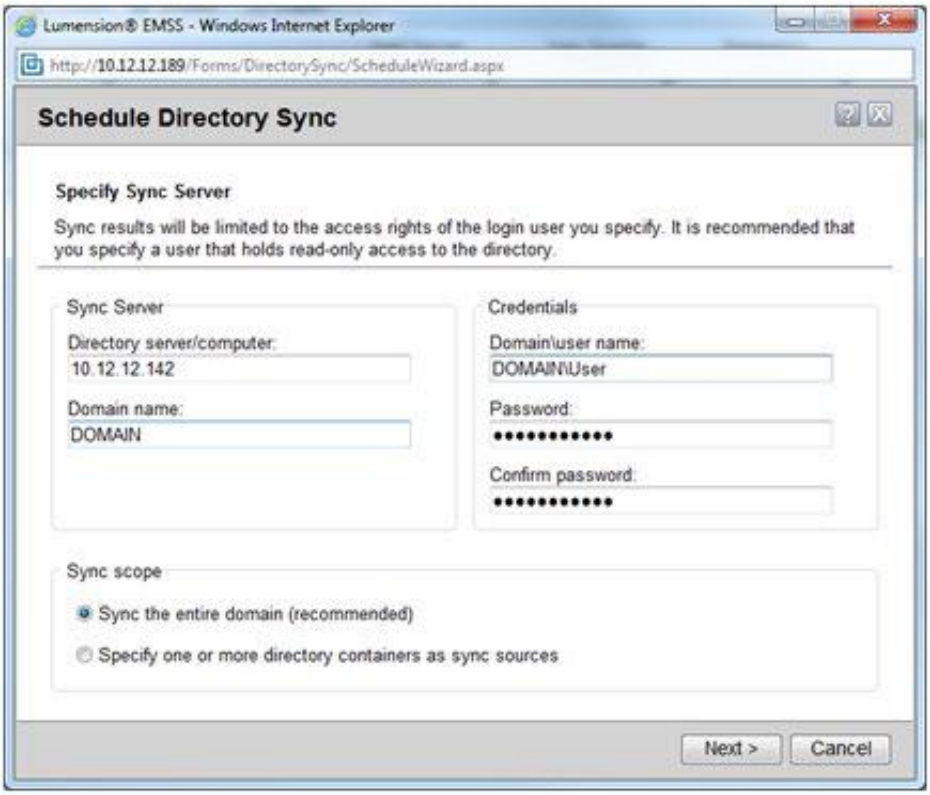


Figure 3 – Creating an Active Directory Sync job

Recall that User Groups are the preferred and most common assignment for Device Control policies. Configuring and completing the AD Sync allows that assignment.

Configuration

Now that the Device Control module is installed on the L.E.M.S.S. server, on the Tools>Options page you will find a Device Control tab. This tab contains several settings which will apply globally to your Device Control installation. These should be configured as early as possible, and should not need to change much after deployment. Most of the options are self-explanatory or described in the product Help. Here are some considerations.

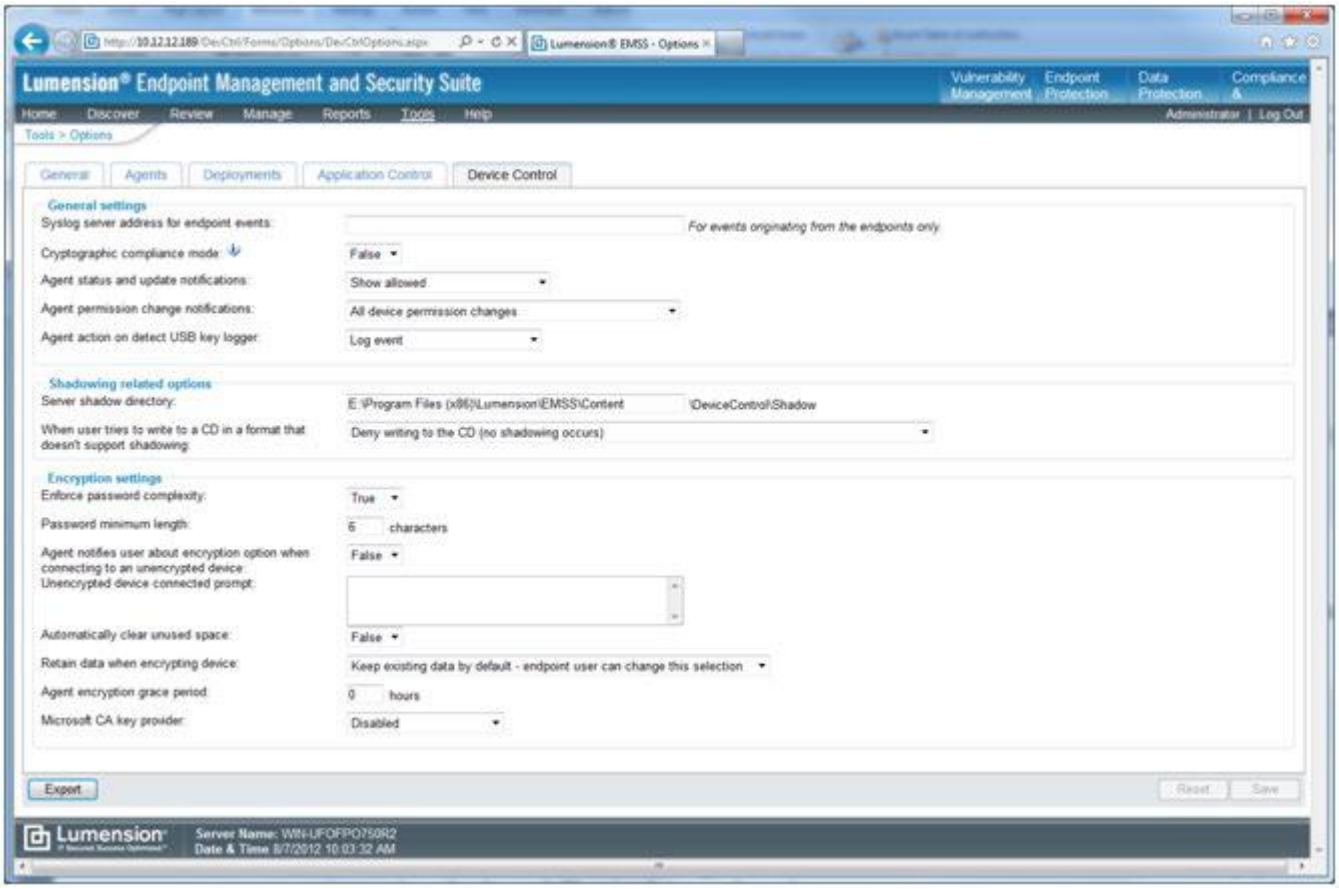


Figure 4 – Tools>Options page, Device Control tab

Some of the options on this tab control what the end user will see in specific situations.

- **Agent status and update notifications**: This controls what is visible to the end user in the Status dialog which is accessible from their system tray icon. You can control whether or not the user is able see if there is a shadowing policy in place for his user account, and you can control if the user sees all devices with permissions in the system, or only those associated with the logged in user's account.

- **Agent permission change notifications**: When you make policy changes and those changes are received by the endpoint, a notification is displayed stating that settings have changed. You can limit that notification to only display when temporary permissions are assigned to the logged in user, or disable the notification altogether. The notification is useful in letting user's know that you have updated their permissions. Some Administrators find that users start to ask a lot of questions when they see these notifications initially and prefer to suppress them.

- **Unencrypted device connection prompt**: This is optional text you can enter which will be displayed to the user if (a) they connect an unencrypted device to the endpoint, and (b) their permissions allow them the option to encrypt the device, but do not force them to encrypt the device. This is intended to serve as a reminder to those with the ability to encrypt that they have that option before copying data to the device. Any text you enter here will be followed with "Do you wish to encrypt *D*: now?" where *D*: is the volume to be encrypted.

- **Automatically clear unused space**: If set to False, the user will have the option of overwriting unused space on a device during the encryption process. If set to True, the user will have no option and unused space will be overwritten to obscure residual data which was on the drive prior to encryption. This is more secure and takes longer.

- **Retain data when encrypting device**: You can configure the system to automatically retain data on a device when encrypting it or to destroy data on the device when encrypting it. Optionally you can allow the end user to choose. Most users will assume that whatever data is on the device will still be there after they encrypt it. Retaining the data would be a good choice in those cases. Conversely, if you are allowing full access to encrypted devices and are concerned malware may exist on devices being encrypted, then you may want to allow the system to remove existing data when it encrypts the device.

There are some considerations for Shadow related options:

- **Server shadow directory**: If you use full file shadowing, this is the location where the copies of the files users are transferring will be kept. Depending on how widely you use full file shadowing, the storage needs can grow to be substantial. Be sure you configure this option to a location with an appropriate amount of storage based on your intended use of the full file shadowing feature. Changing the location in the future will not move existing shadowed files to the new location, it will simply start to store new incoming shadowed files in the new location.

- **When a user tries to write a CD in a format that doesn't support shadowing**: When burning a CD or DVD disc, files are not written directly to the media on a file-by-file basis. Rather, an intermediate

file is created which represents the entire disc image, and that single file is used to create the disc. In some cases, LDC is not able to access the individual files stored in this image file. Therefore LDC cannot create individual shadow copies of the files being stored on the disc. This setting allows you to determine what action LDC takes in this case. LDC can block the write operation so no data is written without being shadowed, LDC can allow the write and not record any shadow information meaning you will not know what was written to the disc, or you LDC can capture the entire disc image file and store that as the shadowed file. This last option can consume a lot of storage space if frequently encountered.

Configuring other encryption related settings:

- **Enforce Password Complexity**: Forces users to use complex passwords when encrypting devices. LDC uses Microsoft's definition of password complexity so that users who are required to have complex AD passwords will understand the complexity requirements more readily.
- **Microsoft CA key provider**: This determines if user certificates issued by a Microsoft Certificate Authority (CA) can be used to encrypt devices. When set to Disabled, users must select passwords to encrypt devices and cannot associate AD users with the device. When set to Enabled (Decentralized), users will be able to add “Windows Users” to devices. When an added user connects the device, the user's certificate will unlock the device automatically, providing transparent access. You must have a Microsoft Certificate Authority in your environment to use this option. The 'Enabled' setting is unused in L.E.M.S.S., use either Enabled (Decentralized) or Disabled.

Compatibility Testing

It is important when introducing any new software into your environment to perform compatibility testing. Install the Device Control module on a small group of test endpoints to ensure there are no conflicts with other software in your environment and that the devices used in your organization continue to function properly. The endpoints, software, and devices you use should be representative of the equipment used in your organization. Cover all endpoint (server, desktop, laptop, etc.) configurations, and a reasonable sample of devices which may be mission critical or unique to your organization.

When compatibility testing Device Control, be sure to include your anti-virus software, firewall, and any other data protection products. Also be sure to use hardware such as laptops, which often have built-in devices and drivers which are customized to those devices for those hardware configurations.

For additional configuration information, refer to the discussion of Agent Policy Sets in the Installation section above.

Discovery

In order to gain visibility into what devices are being connected in your environment, deploy the Device Control module to the endpoints without disrupting device access. The module will log device activity on the endpoints and you can view that activity in the console. This is important because you will want to review the actual activity in your environment before you implement your policies. No doubt you will find device usage of which you weren't aware. You need to determine if this is legitimate usage, in which case you need to account for it in your policies. If the usage is not legitimate and will be blocked, you will likely want to add this information to your user communications so that there are fewer surprises when enforcement starts.

Module Deployment

Refer to the L.E.M.S.S. documentation for details about installing the L.E.M.S.S. agent on an endpoint. You can install the Device Control module along with the L.E.M.S.S. agent or after the L.E.M.S.S. agent has been installed.

Once the L.E.M.S.S. agent is installed, there are two options for deploying the Device Control module.

The first option is the Manage Modules dialog. From the Manage>Endpoints page or Manage Groups page in Endpoint Membership view, select Manage Modules on the toolbar above the endpoint list. This dialog lists the endpoints and their current module assignments. You can add or remove modules from this dialog. Add the Device Control module by selecting the appropriate checkbox.

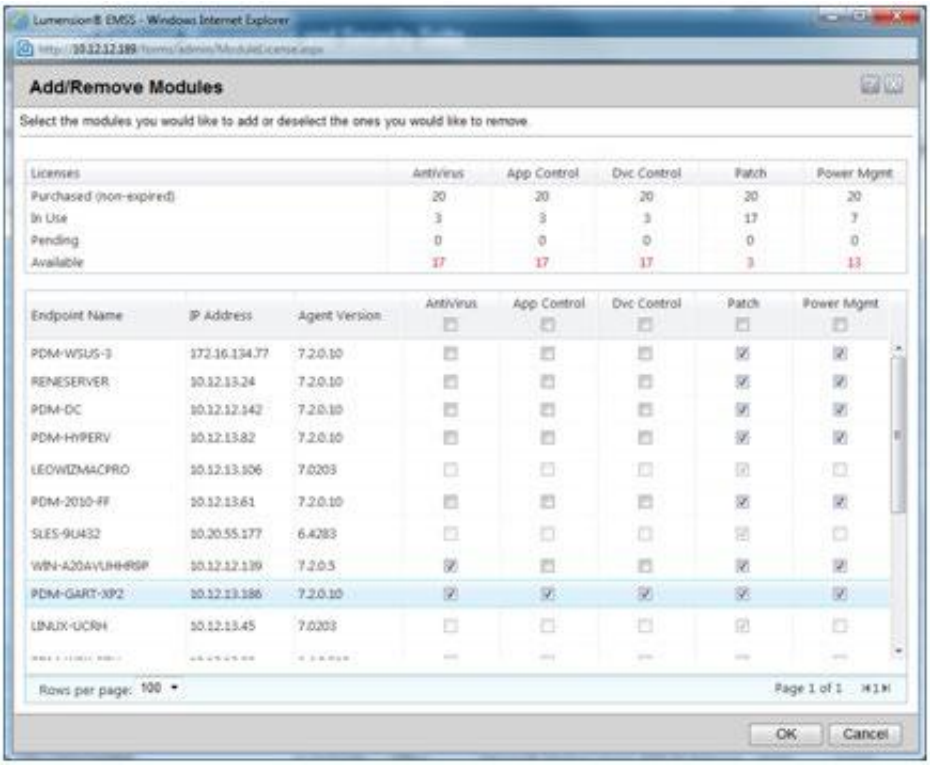


Figure 5 – Manage Modules

The second option for deploying the Device Control module is an Agent Management job. If you use an Agent Management Job, using the Discover>Assets and Install Agents menu option, you can schedule the deployment of the DC module and therefore the reboot to occur during non-working hours or maintenance windows.

If you are LPR user, note that the Device Control module does not take Hours of Operation into account.

Device Event Logging

Once the Device Control module is installed on an endpoint, it will begin to log device activity. These logs are sent to the server, and can be queried from the Review>Device Event Log Queries page.

The types of events which are logged include:

- **Device-Connected, Medium-inserted**: A user connected a device to or inserted media into a drive on an endpoint
- **Read granted/denied**: A read operation from a device was granted or denied
- **Write granted/denied**: A write operation to a device was granted or denied
- **Medium-encrypted**: A user encrypted a disc or removable storage device

With each event, the endpoint name, time/date, and the user initiating the event are logged along with other relevant details.

After the Device Control module has been deployed for some time to allow for user activity, you can view these events on the Review>Device Event Log Queries page. Click the Create button on the toolbar, and select the type of information you want to query for. Fill in the additional details such as a name and date range. On the final page of the wizard, you can further restrict the results to specific users and/or endpoints. Complete the wizard and allow the query to complete. Once the query is listed on the Completed tab, click the query name to drill down into the details.

During this stage, you want to review the Device Event Logs for:

- **Expected allowable activity**: This will be the legitimate business usage of devices which you either have already accounted for in your policy planning or can now account for in your planning.
- **Unexpected allowable activity**: You may find some usage which you did not foresee or plan for in your policy planning. Now is the time to add policies to allow for that usage to the worksheet provided earlier in this document.

Watch for device activity initiated by built-in user accounts such as:

- NTAuthority\System (LocalSystem),
- NTAuthority\Service (LocalService), or
- NetworkService.

Frequently, applications will use these accounts for activities like attaching devices when a laptop is docked, writing to a CD/DVD, or accessing a biometric device prior to a user logging into the endpoint. Policies can be assigned to these users in L.E.M.S.S. For a complete list, navigate to Manage>Users and expand the Built-in Users and Groups node.

- **Prohibited activity**: You will not need to create policies to disallow this activity normally, but be aware of what activity is occurring and ensure it doesn't fall into a scenario which would be allowed by your planned policies. If it does, you may need to consider narrowing the scope of your policy. For example if you had planned to allow access to USB connected printers, but are seeing evidence of some unauthorized printers, you may consider defining which printers are allowed by which users, and leaving the rest without policy so their usage is blocked.

Continue to monitor the activity in the logs until you are comfortable you have seen a broad sampling of usage. Determine which should be allowed and accounted for in policy, and which should be blocked and addressed in user communications.

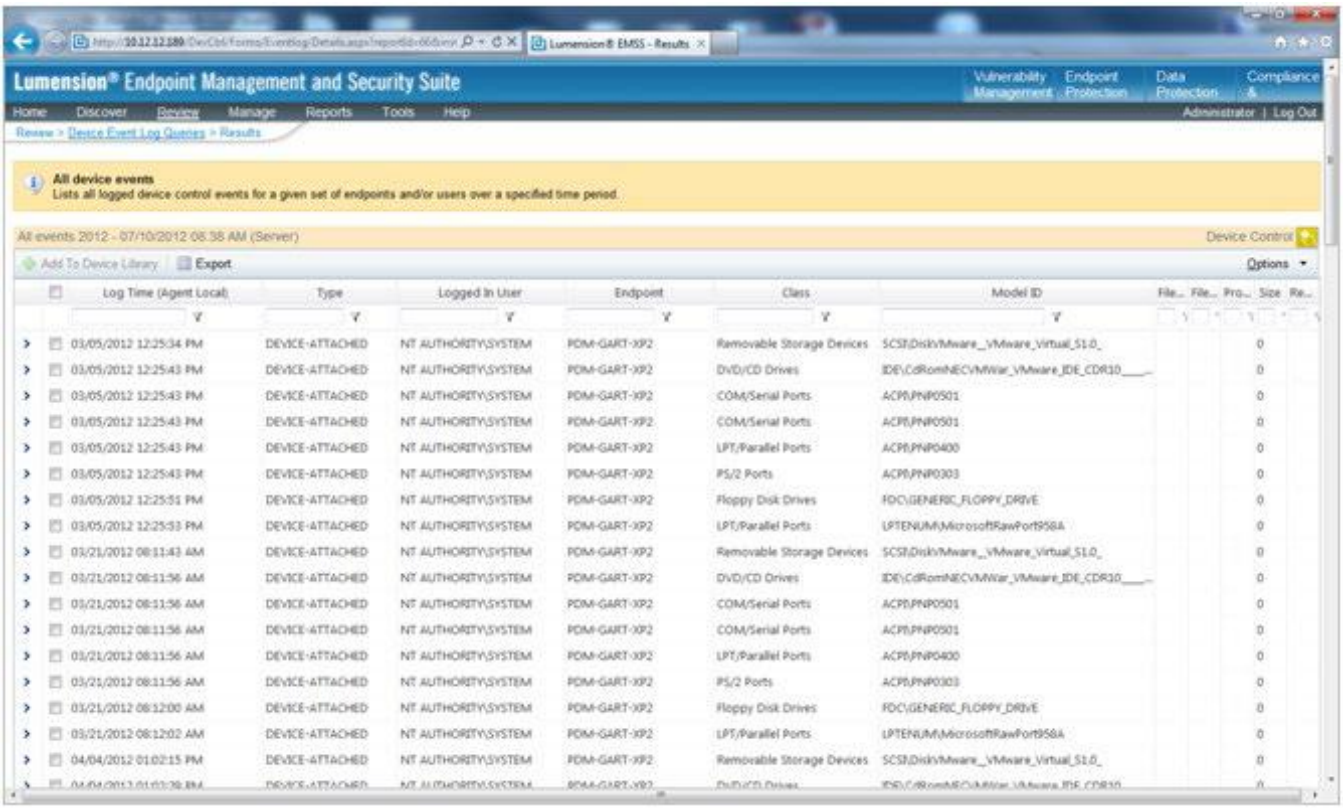


Figure 6 – Sample Device Log Query results

Socialization

This step is key to the success of enforcing your data security policies. It is not product related, and is often overlooked.

Your users may be accustomed to relatively unfettered access to their personal devices on their endpoints. While not malicious, it may not fall into the legitimate usage category in your organization. If you plan to start blocking access to devices which users could previously use, you will be more successful if you complement the roll-out of enforcement with an informational campaign.

The first step is to have a clear policy. Users will want to know exactly what the rules are which are newly being enforced. Along with this, you need a reasonable explanation of why this enforcement is being put into place. This messaging may include:

- The protection of users from malware being introduced into the environment through unapproved devices.
- The protection of users and organization in case of loss or theft of a device in their possession by enforcing a device encryption policy.
- The protection of the organization from statutory fines and lawsuits by ensuring data are encrypted when copied to devices.
- The protection of personal data belonging to your organization's customers and employees.
- The need for the organization to comply with regulatory requirements.

There may a myriad of other reasons your organization has for enforcing its data security policy. Be sure to have messaging which explain these in beneficial terms.

Communicate your message via email, company newsletters, posters in common areas, and similar methods well in advance of enforcement. Allow users to ask their questions and have their concerns addressed before you start to enforce. And, as you start your enforcement program, be sure to keep the communication channels open so users are clear on your security policy, how it's being enforced, and how to handle any special cases they may encounter.

Another important element to a successful deployment is an executive sponsor. The change will be more readily embraced when users see that the executive team is behind the initiative. A supportive and positive message from the executive level has proven to increase the success of any new type of policy enforcement.

Prepare

Definition

Now is the time to start documenting the policies you need to create in the console in preparation for roll-out. If you used the worksheet provided earlier in this document, use this as your guide for creating policies.

Again, approach this in small steps. Plan your policies one device class at a time. There will be several classes which you do not need to allow access for, so your plan would be to have no policies present for those device classes. This is due to the default-deny nature of *Lumension*® Device Control (LDC). Unless you specifically permit usage, it will not be allowed.

Keep in mind that as you create policies, multiple policies will likely apply to a specific user logged into a specific endpoint. There may be policies assigned to one or more endpoint groups, user groups, or even the specific user and/or endpoint in question. For example, if User A is a member of the Active Directory (AD) user groups *Sales* and *Tokyo Office*, and Sales is restricted to read-only access for removable storage devices but the Tokyo Office group is allowed read and write, then how will User A's enforcement be determined? The answer is the order of precedence built into LDC. When multiple policies apply, they are resolved in this priority order:

Priority	Read / Write Permission
1 - Highest	Block All Access – a policy which specifies Permissions set to block all access. You are explicitly blocking this access by creating a policy, rather than implicitly blocking it by not creating a policy. See example below.
2	Read and Write
3	Read
4 - Lowest	No policy - access is blocked

Table 5 – Policy Enforcement Order of Precedence

In the example above, User A would have read and write access. Both the read-only and the read+write policy apply to the user, and read+write takes priority over read only.

The highest priority is a Block All Access permission. Normally to disallow use of a device, you do not need to create a policy to allow access, and access will be blocked by default. Block All Access policies allow you to override the built-in priority for exceptions cases. For example, if you grant read and write access to CD/DVD drives to a User Group such as *Tokyo Office*, but want to restrict usage by users who are in the Trainees user group, then you would create a policy allowing read and write for the Tokyo Office, and a policy with permissions set to block all access for the *Trainees* user group. If a user is in both groups, the Block All Access policy will take precedence and access will be denied.

There are other Permissions settings, such as Encrypt, Decrypt, Export to Media, Export to File and Import. These settings are logically OR'ed together. If any policy which applies to the user has one of those permissions settings, the user will have that permission.

Device Collections

Some classes, such as Removable Storage Devices, cover such a wide array of devices that policy design for these will be more complex. There may be certain devices you wish to allow for everyone, certain devices in that class which you want to allow only for some users, and some devices, including unknown devices, for which you want to block access. This is accomplished through the use of Device Collections.

In the *Lumension*® Endpoint Management and Security Suite (L.E.M.S.S.) console, navigate to Manage>Device Library. On the left you will see the device classes supported by LDC. Within each class, you can add Collections. Collections can contain specific device models and specific device instances. A policy can then be assigned directly to the collection, rather than to the entire device class.

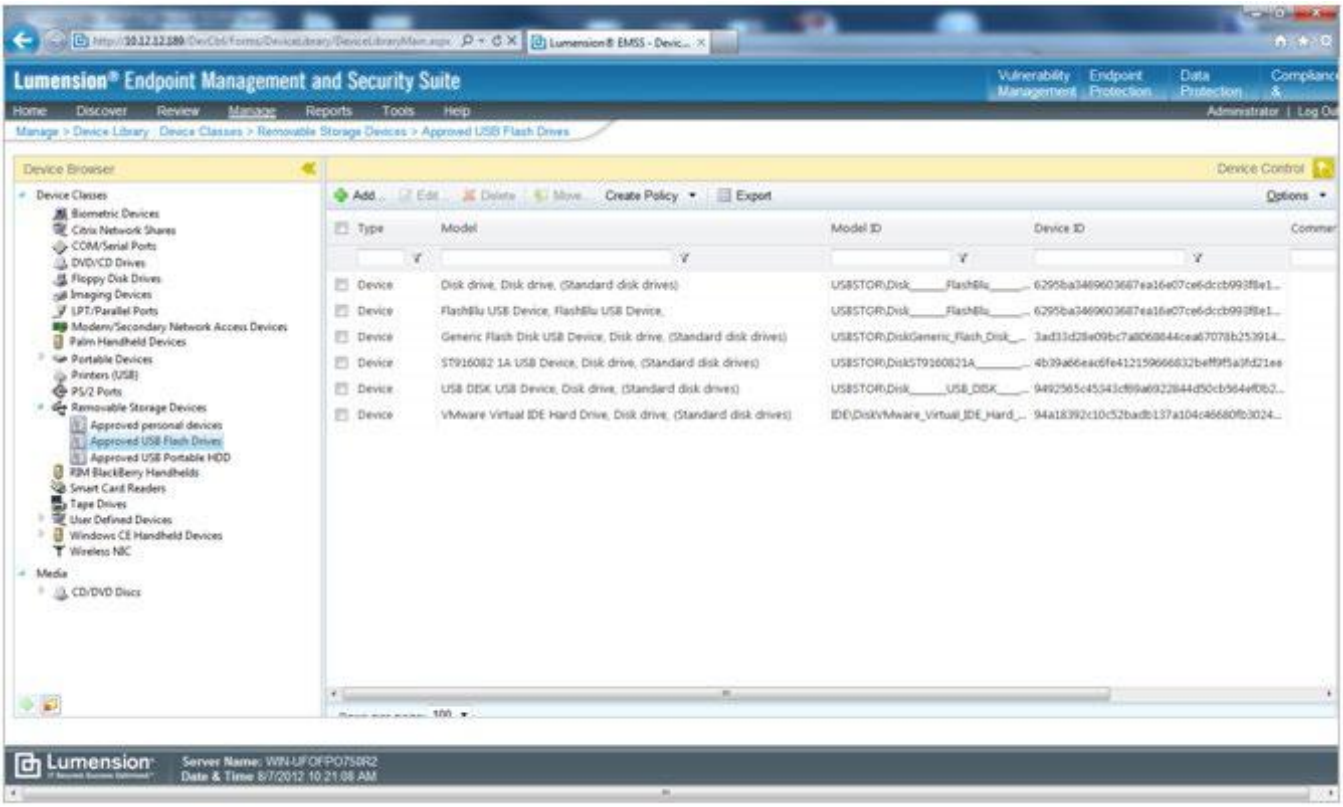


Figure 7 – Device Library and Device Collections

You add device models and device instances (IDs) to collections in one of two ways. You can identify an event related to the device in the device event log query, and add it to a collection from there by right clicking on it or by selecting it and clicking the Add to Collection button on the toolbar. Alternatively, from the Device Library, you can create a collection, select it, and then click the Add button on the toolbar. This will allow you to search the device event logs based on criteria such as user or endpoint and find the device, and then add it to the collection either by model or ID.

Given the example above, here is how you would handle the policy design:

- For those devices which you want to give everyone access, say read access to iPods, you would create a collection and add any iPod models you identified in our logs to that collection. You will then create a collection policy, allowing read permission, and assign it to the user Everyone.
- For those devices only certain people should access, you would create a collection and add the devices to the collection by model or unique ID, whichever method gives you the control you need. You then create a collection policy for that collection, allow read and write permissions, and assign it to the users who need access to those devices
- For the devices which you want no one to access, and devices you don't know about, you simply leave them without a policy. Access to them will be denied.

The idea of managing at the highest hierarchical level possible applies here too. Manage at the class level as much as possible. Use collections when you need to, managing at the model level when possible and unique ID level when you need to. This will substantially reduce the administrative effort required to manage enforcement after deployment.

Note that CD/DVD discs can be uniquely identified and grouped by collection as well, in Media Collections in the Device Library. This allows you to control access to specific media for specific users.

Consider adding an AD group which corresponds to each Device Collection to reduce future administrative workload. Here's an example. If you create a Collection Policy called "Approved USB External Hard Drives" and assign it to an AD user group called "Approved USB External Hard Drive Users", then ongoing management of the system will be simple. When a new user is approved to use external hard drives, add him to that group in Active Directory. He will have access by virtue of being a member of the group. If new hard drives are approved for use, add them to the collection. The policy will be updated with new device and access will be granted.

Policy Creation

Once you're satisfied you have designed the appropriate policies, it's time to create them in the console. Navigate to Manage>Device Control Policies. Click the Create... button and select the appropriate policy type, Class or Collection, and configure the proper settings in the wizard to create your policies.

Assuming the Global Device Control Policy is still in its default state of Audit Mode, none of the policies you are creating at this point will be transmitted to endpoints. You are free to create and experiment without impacting end users. As you roll these LDC policies out, you'll learn a couple of things:

- Some policies need to be modified to enable allowable behavior / usage.
- Some users will need to be "counseled" about unallowed behavior which will be blocked once enforcement is enabled.

Give your policies descriptive names so you and other administrators can easily identify the purpose of each policy.

One L.E.M.S.S. feature you may find useful in this process is the 'Group By' feature of the policy grid. On the right side of the toolbar, click the Options button, then select Show Group By Row. A blue row will appear above the grid. You can drag the Device Class column header into this blue row, and then the policy list will be grouped by device class. You can work one device class at a time, collapsing groups you are not working on to reduce what's visible in the grid.

It is recommended that you leave the Default Policy for each device class intact. Create new policies rather than editing these policies. This will help ease the move to enforcement later, and provide you with a quick method to revert to an all-access-allowed state in case policy enforcement inadvertently blocks critical devices later in the process.

Encryption Policy

The use of device encryption in your organization takes some additional planning. This section discusses aspects you need to consider.

Encryption Permissions

When considering encryption policy there are three basic categories:

Users who will not be allowed to encrypt

This is the simplest group to address. Make sure no policies which apply to these users have the permission *Encrypt* selected. Users will not be allowed to encrypt devices. You can control whether they have access to encrypted devices or not using the *Encryption options* on the Permission Settings page of the policy

wizard. If the *Self contained encryption* option is checked, this policy will apply to encrypted devices, and users will have access to encrypted devices. If the *Unencrypted/Unknown encryption type* option is checked, this policy will apply to unencrypted devices, and users will have access to unencrypted devices. You can allow one, the other, or both.

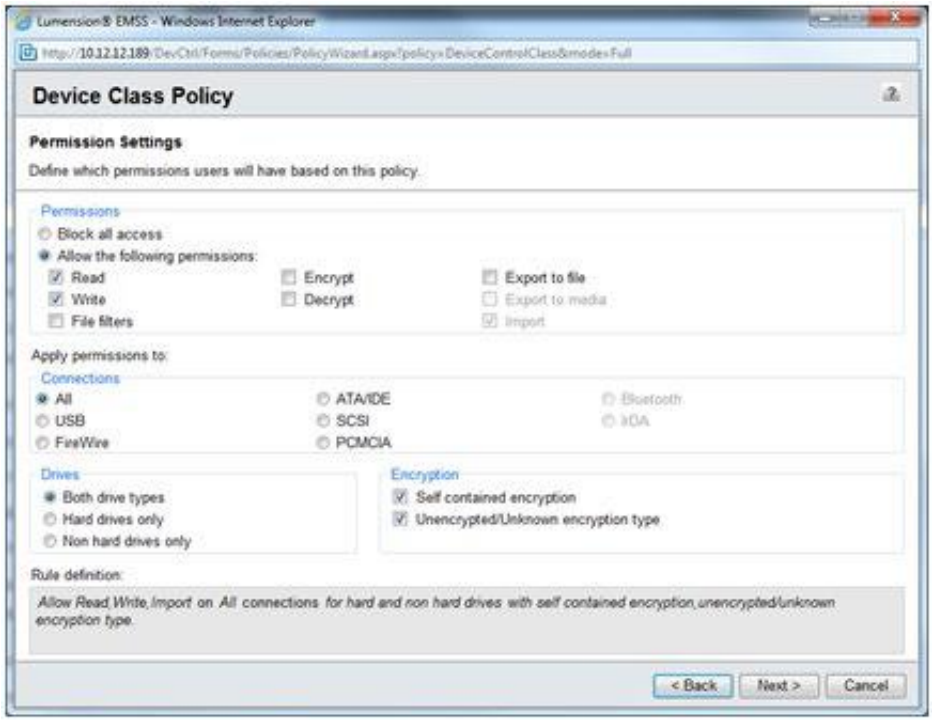


Figure 8 – A device class policy which does not allow encryption

Users who must encrypt devices prior to using them

In this case, you configure two policies: One policy for unencrypted devices, and another for encrypted devices.

- Create a policy with Permission settings; select the Unencrypted/Unknown encryption type option, unselecting the Self contained encryption option. In the Permissions section, select Allow the following permissions, and check the Encrypt box. The Export to Media box will be automatically selected. This allows the user to add a password to access the device after encryption. Assign this policy to the appropriate user group.

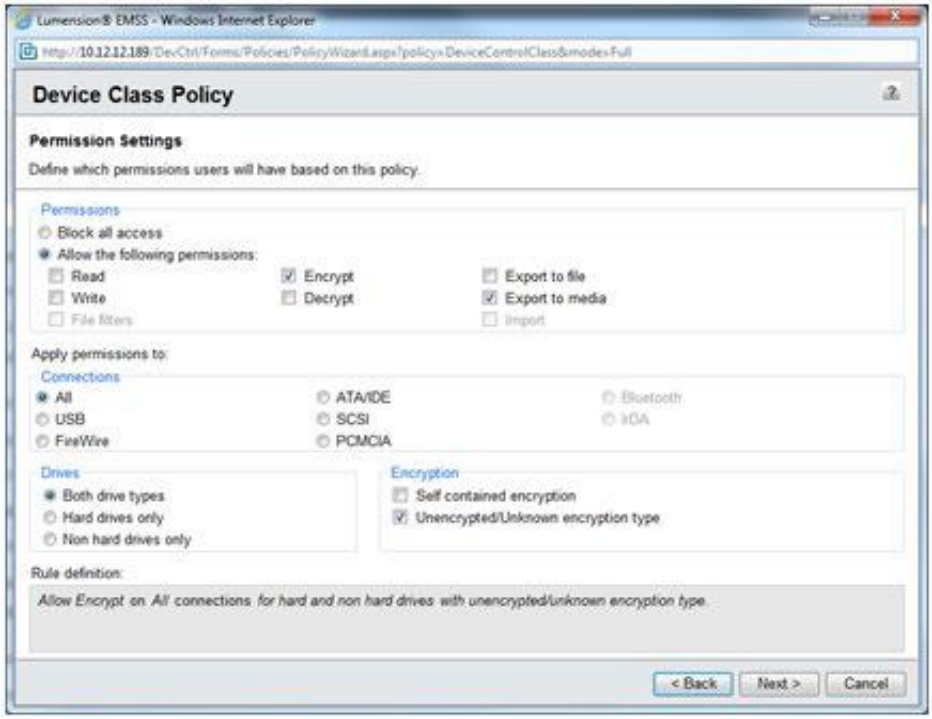


Figure 9 – A device class policy which only allows encryption of unencrypted devices

» Create a policy with Permission settings; select the Self contained encryption box, unselecting the Unencrypted/Unknown encryption type box. In the Permissions section, select Allow the following permissions, and allow read and/or write as appropriate. Assign this policy to the same user group.

The two policies above state that (1) when an unencrypted device is connected, the only thing the user can do is encrypt it, and (2) when an encrypted device is connected, the user may read and write to device.

Users who are permitted, but not required, to encrypt devices

In this case you configure a single policy. Create a policy with Permission settings. Select both encryption options, Self contained and Unencrypted. Allow permissions for read, write (if desired), and encrypt. The Export to media option should be selected automatically. Assign this policy to appropriate user group. This policy states that users have the ability to read from (and optionally write to) both unencrypted and encrypted devices.

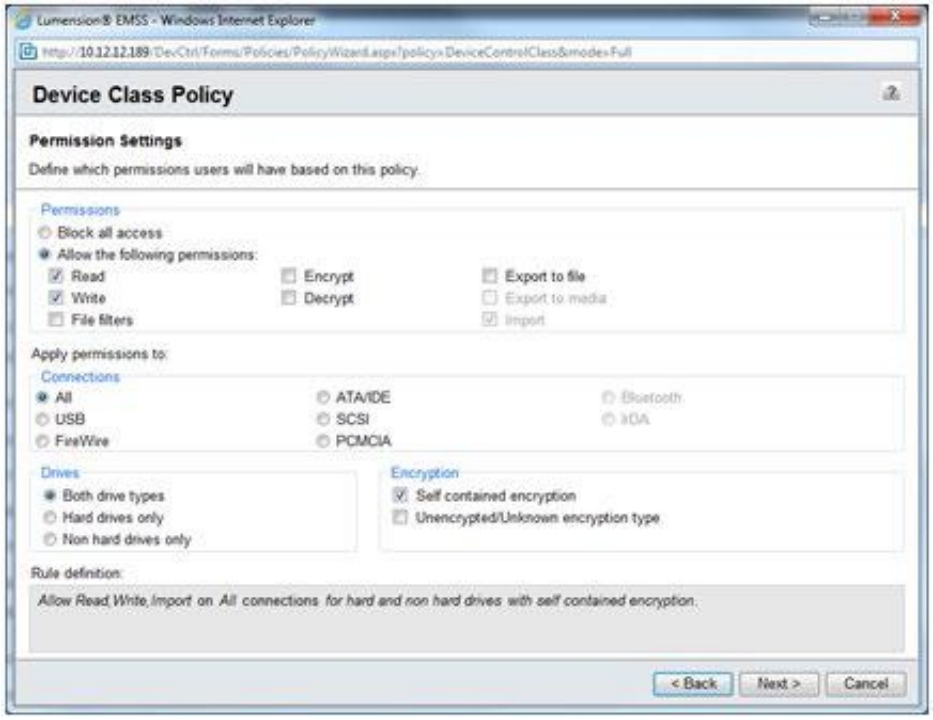


Figure 10 – A device class policy which allows read and write access to encrypted devices

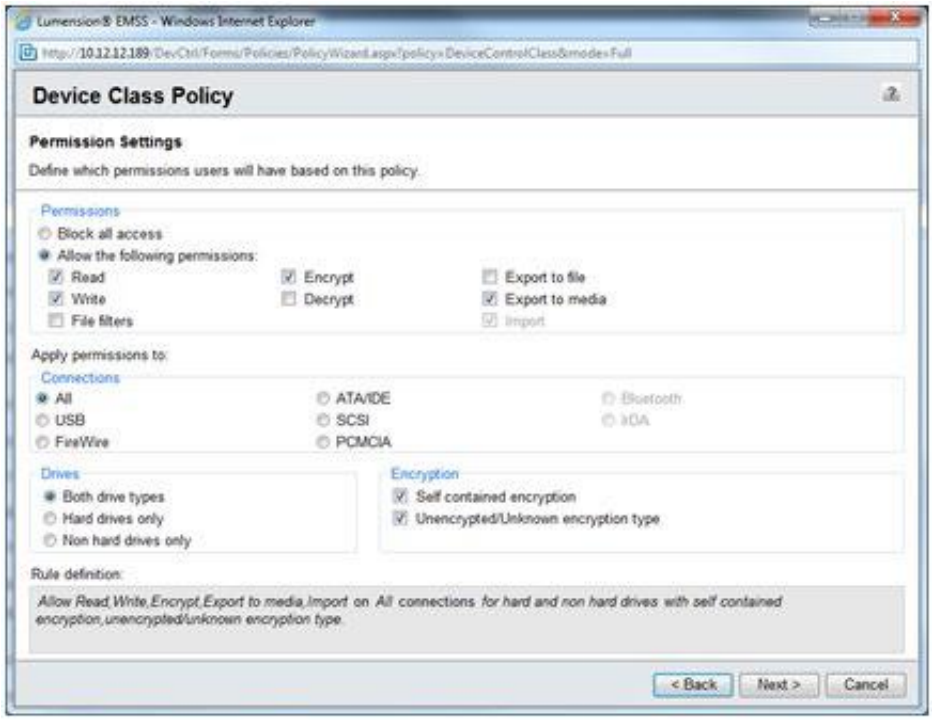


Figure 11– A device class policy which allows users the option to encrypt devices

Recall that these users can be reminded of their ability to encrypt when they connect an unencrypted device. This is configured on the Tools>Options page, Device Control tab under the Encryption settings group.

Accessing Encrypted Devices

You have two options for managing how users can access encrypted devices. The password option allows your devices to be accessed on any computer in or out of your organization. The certificate option limits access to managed endpoints in your network can access encrypted devices.

- **Password based access**: A password is chosen by the end user when the device is encrypted. The password requirements are governed by the options configured on the Tools>Options page, Device Control tab. The encryption key is placed on the device outside of the encryption container, and is itself encrypted with the password. To allow users to encrypt a device which is accessible with a password, they need the Encrypt and Export to media permissions in a policy which applies to them.
- **Certificate based access**: If you have a Microsoft Certificate Authority (CA) in your organization, and you provide certificates to users which are valid for encryption, there is a second option for device access. Users can choose Windows Users who are allowed access to the device after encryption. They can add a number of users from AD, all of which will have access to the device when on an LDC-managed endpoint in your organization. When the device is connected to an endpoint, LDC will compare the logged in user's encryption certificate to those added to the device. If the user is listed on the device, the device will be unlocked using the certificate. No password is required. The device cannot be unlocked in this manner on unmanaged machines, or machines outside of your organization since the certificate is needed. To provide this capability, you must have a Microsoft CA in your environment, and you must set the Microsoft CA key provider option on the Tools>Options page to Enabled (Decentralized).

Secondary Hard Drives

If your organization has endpoints which use secondary internal hard drives, you need to have a policy which allows access to that secondary hard drive.

The most common endpoint configuration designates the C: drive as the primary Operating System (OS) drive, and any other drive(s) for user and/or application data.

Secondary hard drives are considered by the OS to be in the Removable Storage Device class. They are not displayed this way, in My Computer for example, but LDC will treat them as Removable Storage Devices. They will be blocked if not allowed by policy.

To restrict the applicability of a policy to these drives, you have some choices. One option is to add all of the models of secondary hard drives into a Collection, and then create a collection policy which allows Everyone read and write access to those drives, not just an AD user. This is the most restrictive, but requires the connection of these drives to a managed endpoint in order to log the device-attached event so the device model can be added to a collection.

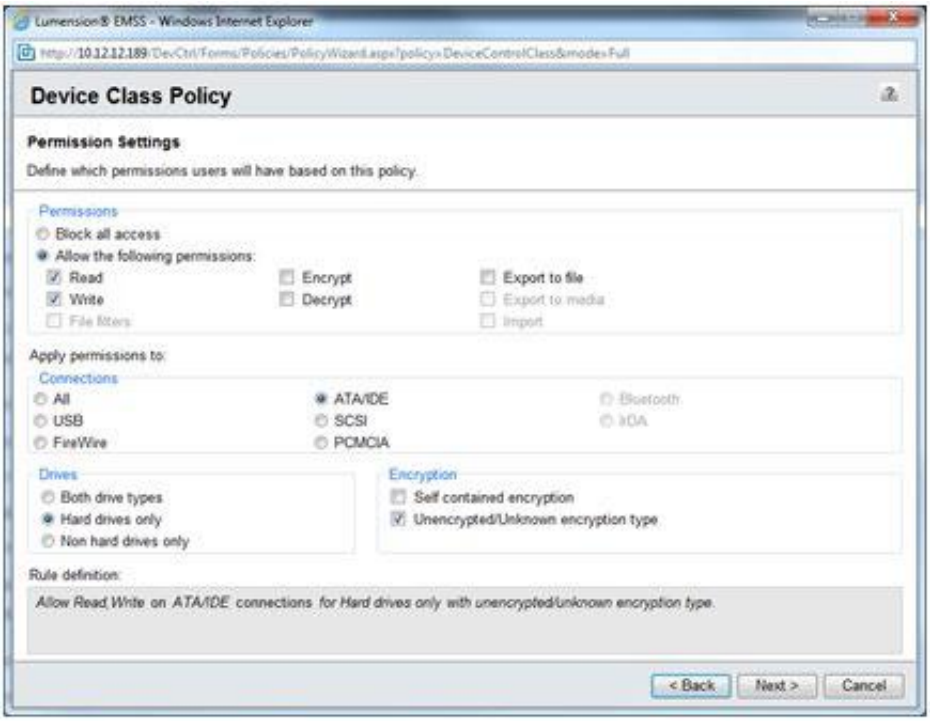


Figure 12 – Allowing access to secondary hard drives

Another option is to create a Device Class policy for the Removable Storage Device class. On the second page of the policy wizard, allow read and write permissions. Do not allow Encrypt permissions in order to prevent accidental encryption of this drive by the user. In the Connections group, select ATA/IDE, and in the Drives group, select Hard drives only. Assign this policy to Everyone. This policy requires less effort, but is not quite as restrictive. The OS has no way of differentiating between IDE and EIDE connected drives. They are actually the same bus, but the connector is on the outside of the case instead of the inside. A user could connect an EIDE drive and have access to that drive. Also, if you have SCSI connected drives, you will need to create a second policy, identical to this example except for the bus connection setting.

Monitoring

As you create your policies you will have a more definite idea of what will be enforced in your environment. Continue to monitor the Device Event Logs and determine if your policies will adequately allow for legitimate usage in your organization. Remember that the Audit Mode and Default Policies are still preventing any restrictions on the endpoints, so you are free to adjust your policies based on what you find in the event logs without impacting users. In addition, maintaining your socialization efforts will minimize the disruption because users will understand why these policies are necessary and how to abide by them.

Enforce

The *Lumension*® Endpoint Management and Security Suite (L.E.M.S.S.) server settings are configured, the policy strategy has been planned and communicated to end users, and policies have been created. It's time to start enforcing your policies using *Lumension*® Device Control (LDC).

User Communication

When you plan to start enforcement, communicate to end users that the enforcement of device usage policies is beginning. Users may see some changes on their endpoint, and this could generate a number of helpdesk calls from curious (concerned) users. You can address this through communication in advance of enforcement.

Users may also see some change in their ability to access devices. You can solicit and direct their feedback on this by communicating in advance. You will want to hear from anyone who was unintentionally disrupted by a policy setting so that you can adjust the policies as needed.

Audit to Enforcement

The first step in moving to enforcement is to switch the Global Device Control policy from Audit mode to Enforcement mode.

When the system is moved to Enforcement mode, all of the Device Control policies will be calculated, combined, and sent out to the endpoints. The endpoints will continue to log events, and they will begin to enforce the policies they receive.

Recall that there are Default Policies in the system for each device class. If you left these intact, then this move should be minimally disruptive. These policies allow Read and Write permission for all classes, and are assigned to the highest level user, Everyone. Also recall that read+write permission takes priority over read only and no permissions, so users will have read+write access when these policies are in place. The only exceptions will be in cases where you have configured policies which explicitly Block All Access. These will override the Default policies, in accordance with the priorities table presented earlier.

Navigate to the Manage>Device Control Policies page. Select the Global Device Control Policy, and change the setting from Audit mode to Enforcement mode, and click OK. This sends all policies in the system to the endpoints. As noted elsewhere, you will want to do this slowly: by device class, by user groups, *et cetera*.

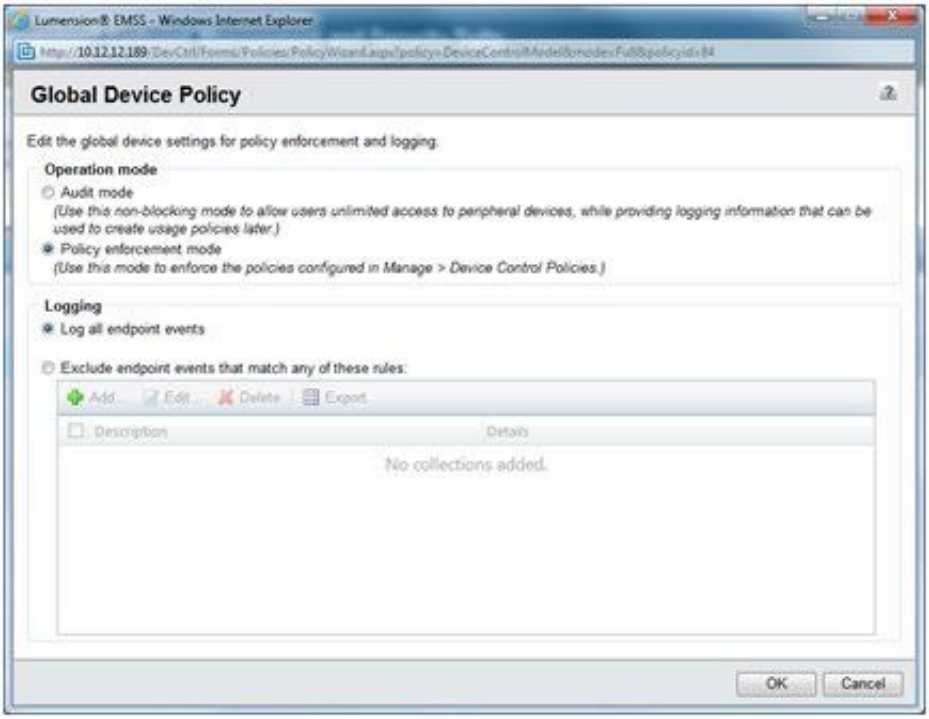


Figure 13 – Setting the Global Device Policy to Policy enforcement mode

On the endpoints, monitor the system tray for the notification "Settings have changed" or watch the Status dialog available from the system tray icon. This dialog shows what permissions the endpoint is enforcing, which may change based on policies you have configured in your environment. These events show that the policies have successfully been communicated to the endpoints.

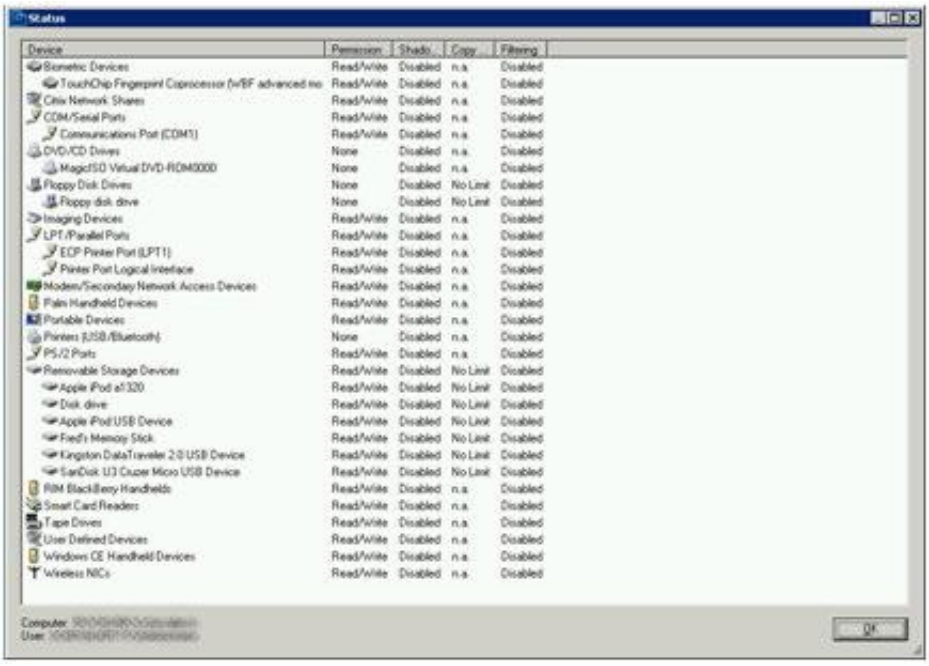


Figure 14 – The Status window on the endpoint, accessible from the tray icon

Initial Roll-out

You will want to take a phased roll-out approach, taking a step, verifying the result, and then taking another step. This helps avoid chaotic troubleshooting of unexpected results in an environment where there may be many contributing factors simultaneously.

It is recommended that you start with a small group of endpoints and users. Once those are working satisfactorily, you can roll out to more and more endpoints and users with increasing confidence.

For the initial roll-out, select some endpoints in your organization representative of different configurations, such as desktop, laptop, and server. This will give you a more accurate prediction of issues you may encounter as the roll-out progresses. You can either install the Device Control module only on these endpoints, or disable the Device Control module on other endpoints if it is already installed until you are ready to expand enforcement to those endpoints.

For the first group, proceed one device class at a time. One class at a time, disable the Default Policy for that device class. This leaves only the policies you created for that class in place. Check with users to confirm your expected enforcement. Also check the Device Event Logs for those endpoints to validate that any read- or write-denied logs are expected. Users will not be aware of some device access, especially by built-in user accounts such as LocalSystem, or may not yet be aware of any issues which are present. If there are read- or write-denied events which should have been allowed, adjust your policies to allow for the desired access level.

Once the first class is working properly, continue the process with the remaining device classes, as outlined in your policy worksheet (table 3). Disable the Default Policy for that class, confirm operation, check the logs, adjust policy as needed, and proceed to the next class. When complete, the Default Policies will all be disabled, and only your policies will be enforced.

Validation

It's important to verify this initial group is working correctly. Over a period of time, continue to monitor the logs for access being unexpectedly allowed or blocked. Adjust your policies as necessary to get the enforcement you are targeting.

Also validate that this group of endpoints is representative of the remaining endpoints. For the remaining endpoints, enforcement will happen for all device classes simultaneously rather than class by class. If necessary, add a few more endpoints into the test group by installing or enabling the Device Control module on them.

Continuing to Full Enforcement

When you are satisfied with the initial test group, continue to roll LDC out to your remaining endpoints. You may want to do this location by location or one functional group at a time. Another option is to introduce Device Control as part of a hardware refresh cycle if the timing is appropriate.

Manage

As you start to deploy *Lumension*® Device Control (LDC) throughout your organization, certain maintenance activities will arise. This section describes the most typical of these.

Dashboard Widgets

There are two Device Control widgets which can be added to the *Lumension*® Endpoint Management and Security Suite (L.E.M.S.S.) dashboard.

The *Devices Connected to Endpoints* widget displays the number of devices connected to your endpoints over the last week, broken down by device class. You will notice a trend of relatively consistent numbers for each class. One purpose of this widget is to draw your attention to any inconsistencies. If you regularly see that no Tape Drives are ever connected in your organization, and suddenly you see that one is being used on a daily basis, this may merit investigation. You can click on the bar in the graph to see the log event data behind the total, including endpoint and user name.

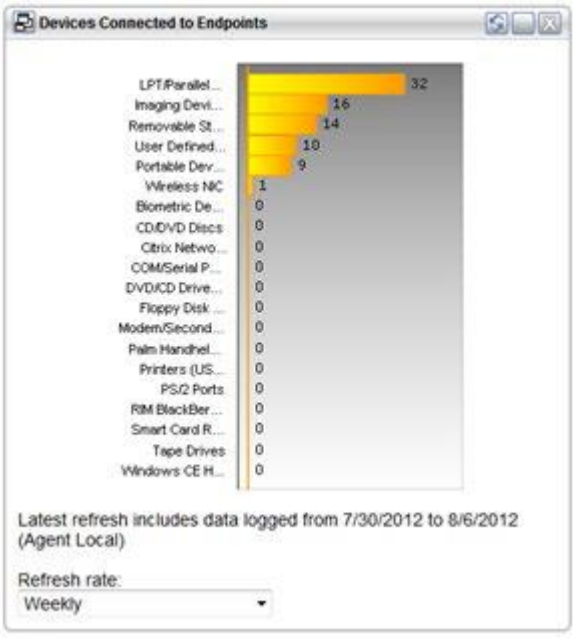


Figure 15 – Devices Connected to Endpoints dashboard widget

The *Device Control Denied Actions* widget totals the number of read-denied and write-denied events logged, and displays the users with the highest totals. This information alerts you that either a user is trying to legitimately use devices and a policy adjustment should be made, or that a user is attempting to connect prohibited devices and further investigation may be warranted.

Both of these widgets are driven by data from Device Event Log Queries which are permanently installed in the system. These queries are visible in the Device Event Log Query page, but cannot be edited or deleted.

Both of these widgets also filter out the list of Built-in Users and Groups when presenting their data. The intent is to present data which is driven by actual users rather than that of system accounts.

Reporting

You may be required to provide reporting to management or archive information for audit purposes. There are two types of reporting in LDC.

The first is Device Event Log Queries which show activity happening on endpoints. These are found under Review>Device Event Log Queries. Queries can be created to run one time, or on a recurring basis. For example, you can configure a query to run on a weekly or monthly basis. The system can alert you via email when the query is completed. A link in the email will take you to the query results. The results pages can be exported to a file for archival purposes if desired or required by regulation in your organization.

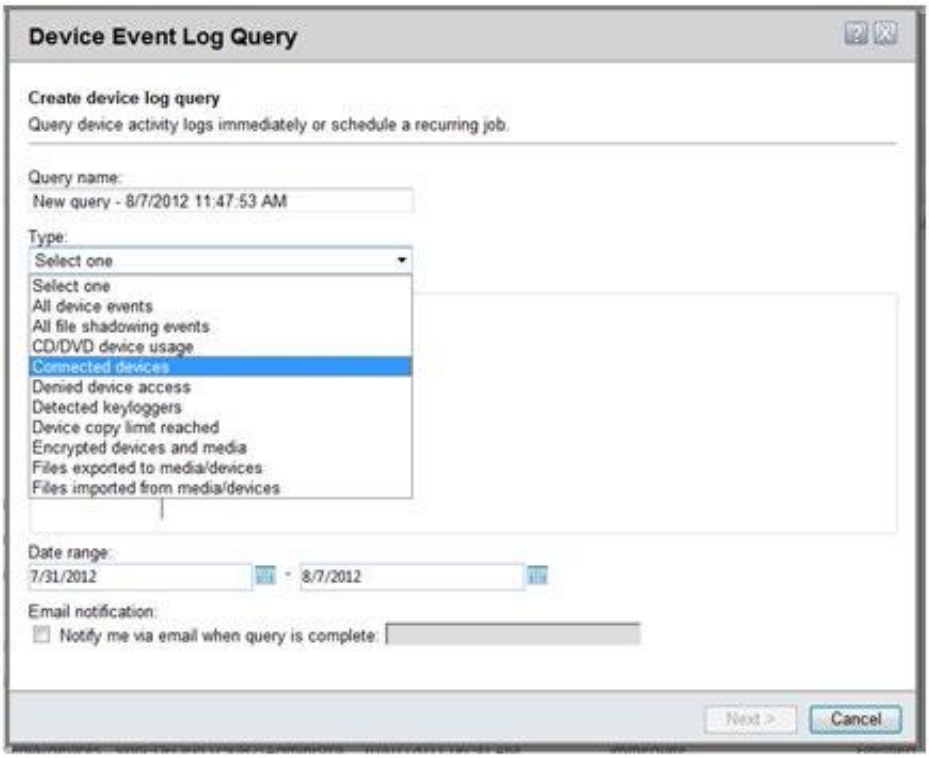


Figure 16 – Device Event Log Query types

There are several types of queries available, depending on the type of information you are looking for. You can further specify the date range for the query to use, and users or endpoints to filter the results.

The second type of reports cover the system configuration and settings. This second group can be found under the Reports>Device Control menu item. It's useful to have a printed or exported version of these reports when your installation is stable and functioning as you desire. These can be a good reference if you need to revert future changes. They can also be used for audit purposes to demonstrate the policies you have in effect.

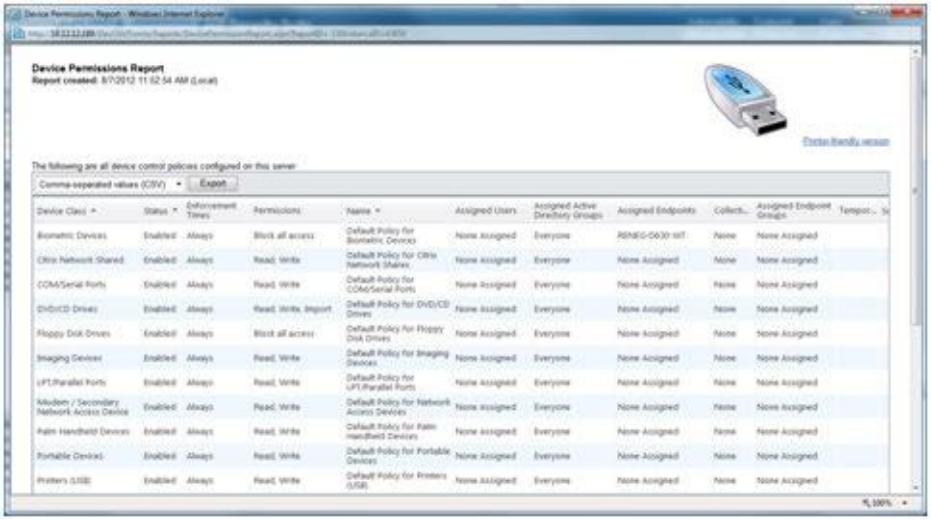


Figure 17 – Device Permissions Report

The Device Permissions Report is particularly useful when troubleshooting unexpected enforcement of policies. This report lists all policies configured in the system in detail.

These reports can be exported or printed for archival purposes if desired or required as well.

File Shadowing

If you implemented File Shadowing policies, you can review the activity shadowed in the Review>Device Event Log Queries screen. Create a query and select the type All file shadowing events. When the query completes, click on the query name on the Completed tab to view the results. You will see the names of files transferred to and from devices, depending on your policy settings, along with relevant details such as user name, endpoint name, and time of the transfer.

If you enabled Full File Shadowing, you can expand the row for an event, and click the disk icon. This will allow you to view the file which was transferred. You have three options for viewing the file.

- **View using Hex Viewer**: This option is the safest option, but possibly the least informative depending on the file. The actual file content is displayed in hexadecimal format, alongside an ASCII representation of the data. This is the safest option because the file is not sent to your browser. It remains in the shadow storage location and will not be executed.
- **Download the file to your computer through your browser**: This option leaves to your discretion the best option for examining the file.
- **Open the file in the browser using the browser's default action for that file type**: This is the fastest way of viewing the file, but introduces risk as the file may contain malware or have other unexpected content.

These are complete copies of the file which the user transferred, and can be saved for subsequent use in an audit or investigation.

Temporary Permissions

This feature allows you to grant permissions on a temporary basis to users who cannot connect to the L.E.M.S.S. server to receive an updated policy. If a user is in the field and has an unanticipated need for device access, this feature will allow you to grant specific permissions.

The process involves a challenge/response mechanism between the end user and the administrator. The user selects *Request Temporary Access Offline* from the system tray icon. The user completes a wizard specifying the access they are requesting. The wizard then provides them with a Client Key, which is a code they must read to the Administrator.

The Administrator accesses the feature from Tools>Device Control>Grant temporary permissions. The Administrator must make exactly the same settings the user made on the endpoint. These include the device class, the permissions requested, the duration of the permissions, and the user the permissions are for.

Note that the end user can only select 'Everyone' or the user's specific account. The Administrator is not limited to these selections, but since the settings must match, the Administrator must select 'Everyone' or the individual user in order to grant the permissions.

The user reads the client key to the Administrator, who enters it into the console. The Administrator then generates an Unlock code, which is read to the user, who enters that code on the client. The user is then granted the specified permissions.

The reason for including a challenge/response mechanism is so that the Administrator can validate the authenticity of the user and the validity of the request before granting permissions.

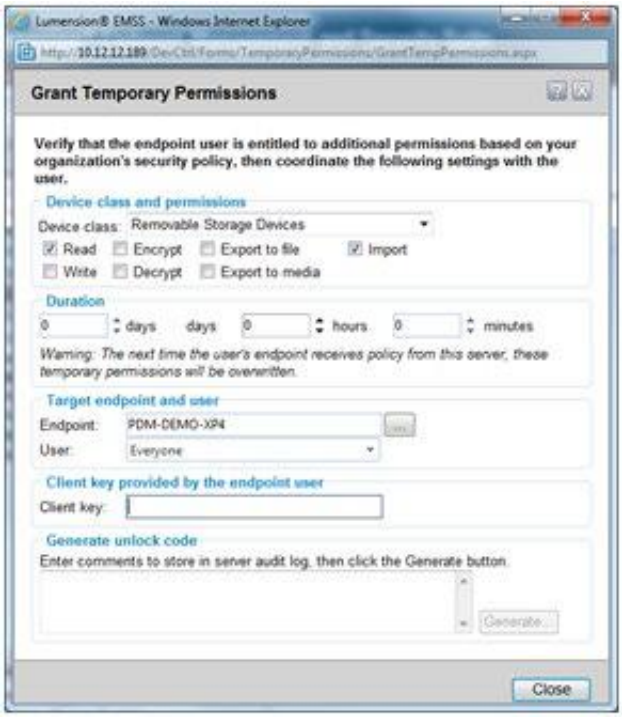


Figure 18 – Granting Temporary Permissions (offline endpoints)

Temporary Policy

Temporary Policies are different than the Temporary Permissions described above. These are actual policies configured in the L.E.M.S.S. console and delivered to connected endpoints.

Temporary Policies are typically used for one-time needs. These provide a way for you to grant permissions, which are then automatically revoked when they expire. These can be used to provide access to devices a common area computer, such as in a conference room, or allow for weekend work for a team working extra hours to meet a deadline. You can grant the permissions, and need not remember to revoke them later.

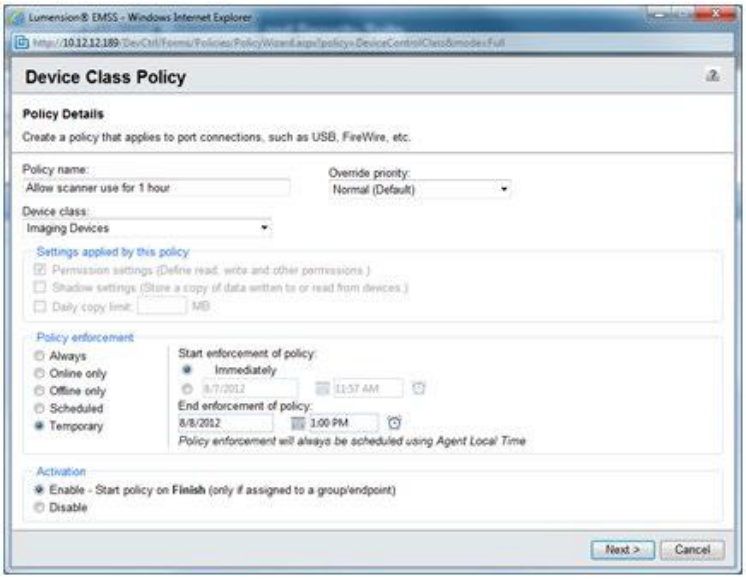


Figure 19 – Temporary policy

Password Recovery

If you use device encryption in your organization, you will likely need to help users recover forgotten passwords. Users are locked out from a device when they exceed the threshold for incorrectly entering the password to unlock the device. The Secure Volume Browser on encrypted devices provides a link for users to recover the password.

Password recovery is also a challenge/response tool. It is the Administrator's role to authenticate the user and ensure the request is valid before proceeding.

When the user clicks a Recover Password link, an Encrypted Medium ID and Security Code will be displayed. The Administrator accesses the Password recovery under the Tools>Device Control>Recover Password menu selection.

Figure 20 – Password recovery

The user reads the codes to the Administrator, who enters them into the console. The Administrator then generates another code which is in turn entered by the user into the Secure Volume Browser. The user is then able to enter a new password for the device.

Policy Maintenance

Policy maintenance requirements should be very minimal. If the majority of your policies are at the highest possible hierarchical level (Device Class, User Group) and exceptions are accounted for then policies will require no maintenance due to new devices on the market, new endpoints in your organization, or new users in your organization. The only policy changes you should need to make are those driven by changing business needs.

If you find that you frequently need to make changes to policies, there is likely a better strategy for your policy design.

Administrative Tasks

Adding Individual Users

You may need to add individual users to L.E.M.S.S. if a specific user needs a unique policy. This should be done on an exception basis. Do not try to add all of your users to L.E.M.S.S. individually and manage them at that level.

To add an Individual User, navigate to Manage>Users, select Individual User Policies in the hierarchy, and then click the Add button. Search for and select the user you wish to add and click OK. This user will now be available in the Policy wizards on the assignment page. You can also perform this task directly from the policy assignment page in the policy wizard.

Adding new devices

Over time you will need to add more devices into device collections to manage their access. You can do this using either of the methods described above in the Device Collections section.

When you add a device to a Collection, any policies which are related to that collection are updated with the new device information and the new policies are automatically updated on the endpoints. There is typically no need to alter policy or create a new policy, simply add the device to a collection with appropriate permissions and assigned to the appropriate users.

Frequently Asked Questions (FAQs)

Q: We want to disable the use of all USB ports.

A: It's usually not conducive to organizational productivity to universally block access to a port or ports. You can allow for productivity and manage access by managing the devices connected to ports rather than the ports themselves. If you wish to block access to a specific port, such as USB ports, create a Port Control policy from the Manage>Device Control Policies page. Select the Permission settings on the first page of the wizard. On the second page select Block all access, and select the desired port. On the last page of the wizard, assign the policy to Everyone from the Users panel. All access to that port, regardless of device, will be blocked.

Q: We want to allow our users the ability to encrypt devices when they need to.

A: Refer to the Encryption Permissions section in this document for details on configuring a policy this way.

Q: We want to force any data written to USB flash drives to be encrypted (users can read any USB flash drive).

A: Refer to the Encryption Permissions section in this document for details on configuring a policy this way.

Q: People need to take this data out of the organization to use it, how do I allow that while keeping the data safe from unauthorized access?

A: Allow for password-based access to encrypted devices. See the section Accessing Encrypted Devices in this document for details on the settings required to allow this.

Q: I need to know what users are copying to devices, how do I accomplish this?

A: Use Lumension's patented Shadowing technology. See the section on shadowing in this document for a detailed discussion.

Q: I need a secure solution which won't be easily bypassed. Can users with Administrative rights bypass LDC?

A: No, they can't. The agent is hardened from tampering from users, even those with Administrative rights. The enforcement kernel driver loads prior to the user logging on, so protection is in place for the entire user session.

Q: I only want my employees to use company issued (or approved) devices (makes and models).

A: Use Device Collections to allow the device models you want to allow. No policy or effort is required to block all other devices.

Q: What considerations might exist when considering the differences between laptops, workstations, and servers?

A: Consider what devices are appropriate on each of those endpoint classes. A Wi-Fi adapter is certainly present in a laptop, but is it needed on a workstation, or should it ever be allowed on a server? Likewise, you may have Tape Drives as backup devices on servers, but should they be permitted on workstations? Also, refer to the sections in this document on SK-NDIS and Reboot Options.

Q: I want specific devices to be used by specific people or a group of specific people.

A: This is accomplished using Device Collections in combination with Collection Policies. Place the permitted devices in a Device Collection, then create a Collection policy for that collection, and assign it to the appropriate user groups or users.

Q: I don't want permission changes to be seen or pop-up on the end user's machine.

A: These notifications can be suppressed with the Agent permission change notifications setting on the Tools>Options page, Device Control tab.

Q: I don't want to allow rogue / unmanaged devices (e.g., keyloggers, Wi-Fi adaptors, etc.) which shouldn't be present in the organization. How do I account for all possibilities?

A: Because LDC uses a default-deny approach, you need only manage the devices you want to allow. Any other device which is connected to your endpoints will be denied access.

Q: I want to monitor use, we'll decide whether or not to enforce later. Is that possible?

A: Yes. LDC includes an Audit mode, in which the system will log device activity on endpoints without enforcing any access policy.

Q: I need to block a specific device, NOW!

A: The device will be blocked by default unless it falls within the scope of an existing policy. In that case, you can disable the policy, or search for the device in the Device Library, add it to a new Collection, and create a Collection Policy which specifically blocks access to that device. This explicit blocking of access will take priority over any other policies.

Q: We only allow specific media on these machines, how can I limit the DVD's people can use?

A: Optical media can be added to Media Collections in the same way devices can be added to device collections. You then create a Media Collection policy which allows access only to those discs.

Q: I want to manage my permissions with AD instead of in your console, is that possible?

A: Yes, after initial configuration of the policies, many customers manage user's permission levels through the use of AD groups. See the section AD Sync for a more detailed description.

Q: I want to be able to define groups of machines and manage them that way. Does LDC allow that?

A: Yes, the L.E.M.S.S. console has very flexible endpoint group creation and management. You should create groups and apply Agent Policy Sets to control reboot behavior and the installation of the NDIS driver (see corresponding sections in this document). Servers, laptops, desktops, and unattended machines have different needs and can be handled differently.

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.

Lumension®
IT Secured. Success Optimized.™

Global Headquarters

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255 USA

phone: +1.480.970.1025

fax: +1.480.970.6323

www.lumension.com