Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

Lumension Data Security Partner Guide

Lumension®
IT Secured. Success Optimized.™

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted

Table of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2012 Cisco Systems, Inc. All rights reserved.

What's In This SBA Guide

About SBA

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

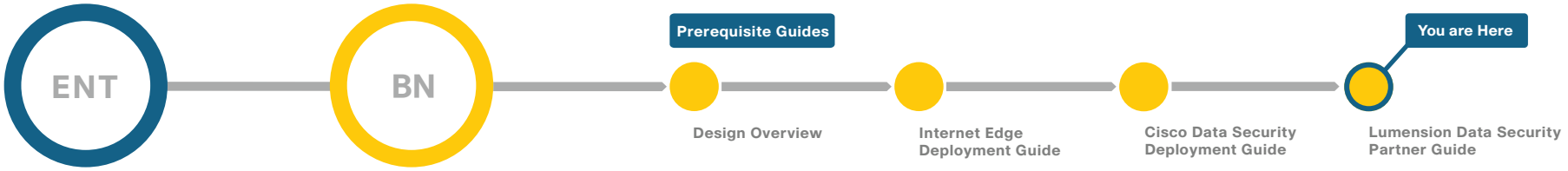
For more information, see the *How to Get Started with Cisco SBA* document:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *additional deployment guide* includes the following sections:

- **Business Overview**—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

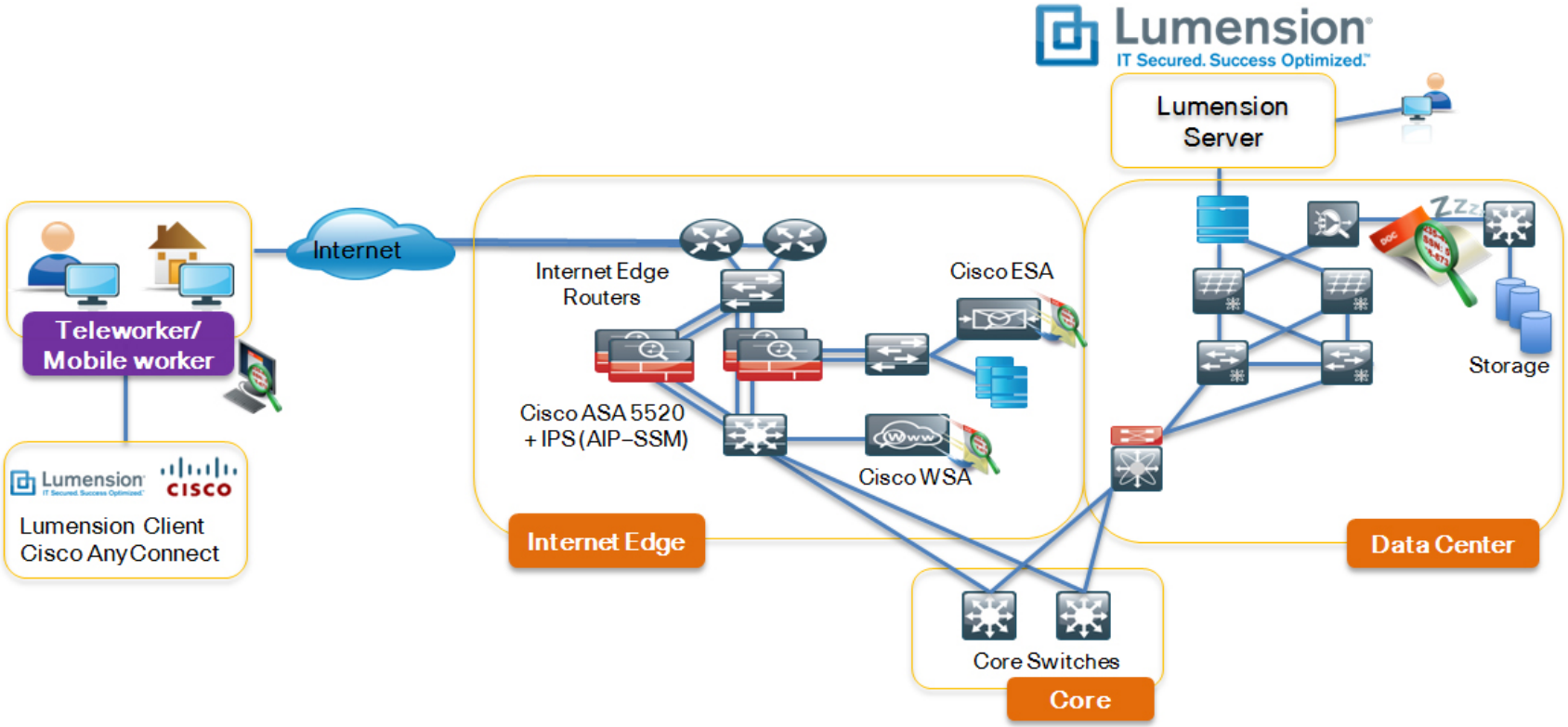
Overview of Cisco Borderless Networks

The Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations offers partners and customers valuable network design and deployment best practices; helps organizations to deliver superior end-user experiences using switching, routing, security and wireless technologies; and includes comprehensive management capabilities for the entire system. Customers can use the guidance provided in the architecture and deployment guides to maximize the value of their Cisco network in a simple, fast, affordable, scalable and flexible manner.

Modular design means that technologies can be added when the organization is ready to deploy them. Figure 1 shows how the Lumension data security solution integrates into the Borderless Networks architecture.

This guide is part of a comprehensive data security system designed to solve customers' business problems, such as protecting intellectual property and sensitive customer information assets, and meeting compliance requirements. The guide focuses on Cisco's partnership with Lumension to deliver affordable endpoint device control as a part of Cisco's broader data security system.

Figure 1 - Lumension Data Security Integrated into the Smart Business Architecture—Borderless Networks for Enterprise Organizations



Business Benefits

Data is an organization's lifeline and organizations have data stored everywhere. To enhance productivity, organizations allow employees and partners access to data from almost anywhere. In addition, many employees are working remotely, thus requiring access from outside the network. But the potential impact of data loss is a very real concern, be it accidental or malicious. And removable devices (such as USB flash drives) and media (such as DVDs/CDs) are among the most common data leakage routes, with no file copy limits, no encryption, no audit trails, and no central management.

In fact, the problem of data leakage due to the accidental or sometimes malicious use of removable devices and/or removable media has reached alarming levels: over 85% of privacy and security professionals reported at least one breach and almost 64% reported multiple breaches that required notification.[1] The costs for recovery of data and lost business are rapidly rising as well, with the average per incident cost now estimated to be $6.75 million.[2]

Lumension Device Control enforces organization-wide usage policies for removable devices, removable media, and data, including read/write access rights and encryption enforcement. The product features are summarized in Table 1.

Table 1 - Lumension Device Control Overview

Capability	Benefit
Centrally manages security policies for removable devices and media using a whitelist, default-deny policy approach	• Eliminates a major data leakage path through automated control of ports and removable storage • Enables business productivity while enhancing organizational security • Reduces management and maintenance needs in an ever-changing IT environment
Enforces encryption policies when copying data to removable devices or media	• Protects valuable corporate and customer data • Provides "safe harbor" protection in case of data exfiltration
Prevents malware intrusion via removable devices or media	• Adds a layer of protection to your network • Reduces threat of self-replicating, self-propagating malware (such as Conficker)
Provides in-depth reporting and alerting, including syslog integration	• Offers forensics and reporting tools to demonstrate compliance with applicable laws • Allows for real-time reaction to endpoint events • Improves understanding of inter-related events

1 Deloitte & Touche and Ponemon Institute, Enterprise@Risk: 2007 Privacy & Data Protection Survey, December 2007
2 Ponemon Institute, 2009 Annual Study: Cost of a Data Breach, February 2010

Lumension Device Control Deployment Overview

Step 1: Installing Lumension Device Control on Your Network

Lumension Device Control supports controls on any ports and devices recognized by Windows, including all Plug-and-Play and user-defined devices. Table 2 lists the supported ports and devices:

Table 2 - Lumension Device Support

Physical Interfaces	Wireless Interfaces	Device Types
• USB • FireWire • PCMCIA • ATA/IDE • SCSI • LPT/Parallel • COM/Serial • PS/2	• WiFi • Bluetooth • IrDA • Wireless NICs	• Removable Storage Devices • External Hard Drives • DVD/CD Drives • Floppy Drives • Tape Drives • Printers • 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

Successful installation requires you to install the following components:

1. Install the Database. Lumension Device Control uses Microsoft SQL Server 2005 (standard or Express editions) or Microsoft SQL Server 2008 (standard or Express editions).
2. Generate and save a public and private key pair. Lumension strongly recommends the use of a public-private key pair to provide the highest level of security.
3. Install the Application Server(s). Lumension Device Control is designed to use one or more Application Servers. Each of these acts as an intermediary between the endpoint client and the database, and distributes the list of devices and software permissions for every endpoint on your network.
4. Install the Management Console, which is used to configure Lumension Device Control and enables administrators to perform a range of day-to-day administrative tasks.
5. Install and deploy the endpoint client (SK), which is a low-level kernel driver that controls access to devices on the protected endpoint. The SK supports Microsoft XP Professional, Vista, Windows 7, Server 2003, Server 2008, Server 2008 R2, and many others, including virtual platforms.

Step 2: Setting up Lumension Device Control

Lumension Device Control grants device access by applying permissions rules to each device type, including floppy disk drives, CD and DVD drives, serial and parallel ports, USB devices, hot swappable and internal hard drives,and so on. Based on the Least Privilege Principle, access to any device is prohibited by default for all users. To grant access, the administrator associates users or user groups to specific devices or complete device classes. This approach is unlike traditional security solutions that use blacklists to specify devices that cannot be used.

Setting up Lumension Device Control requires you to perform the following tasks through the management GUI:

1. **Discover:** Identify all removable devices that connect to your endpoints using learning mode to collect information without disrupting business.
2. **Assess:** Define rules at both global and machine-specific levels for groups and individual users to define device access by class, model or specific ID, and uniquely identify and authorize specific media. These permissions can be linked to user and user group information from Microsoft Active Directory or Novell eDirectory.
3. **Implement:** Enforce device and data usage policies, and centrally enforce the encryption of data being moved onto removable devices and/or media; apply these permissions to specific endpoints, ports, devices and users, or entire groups.
4. **Monitor:** Continuously monitor the effectiveness of device and data usage policies in real time and identify potential security threats by logging all device connections, recording all policy changes and administrator activities and tracking all file transfers by file name and content type. You can even keep a copy of every file that is transferred to or from a removable device using Lumension's patented bi-directional shadowing technology.
5. **Report:** Create both standard and customized reports on all device and data activity showing allowed and blocked events, which can be saved into a repository, shared via email, or imported into third party applications. Detailed forensic reports and comprehensive auditing capabilities enable organizations to demonstrate compliance with government requirements (such as SOX, GLBA, HIPAA, HITECH, and others), industry regulations (such as NERC, PCI DSS and others) and their own internal security policies.

Reader Tip

Implement Lumension Device Control in "learning" mode first, and collect information on device usage in your network without blocking, until you have a good idea of who is using what and why. Be sure to collect information over a sufficient length of time, one which covers important periods of high activity, such as month-end close in the accounting department, or increased sales activity at the end of a quarter.

Reader Tip

Deploy any new enforcement policy in phases. Start small, then test, monitor and adjust. After things have stabilized, move on to the next phase.

Working with Cisco AnyConnect and RSA DLP Endpoint

Lumension Device Control works seamlessly with RSA data loss prevention (DLP) products and the Cisco AnyConnect client to provide policy-based control for sensitive data on removable media. A combination of RSA DLP Endpoint and Lumension Device Control policies allows organizations to control data in use. Through partnership with RSA, Lumension will use the robust classification technology and comprehensive policy libraries contained in the RSA DLP SDK to scan documents and compare them against RSA policies, and then restrict or encrypt the sensitive data based on user access and corporate policy. Cisco AnyConnect provides the secure transmission of data in motion from the endpoint.

This combination of Lumension Device Control with Cisco AnyConnect VPN and RSA DLP Endpoint allows organizations to effectively control sensitive data transferred to removable media, encrypt data on removable media, and secure delivery of data in motion.

Getting Value from Lumension Device Control

Lumension Device Control provides deep, granular control of all port, device, and media usage on your network. Some of the capabilities which can be incorporated into your security policy include:

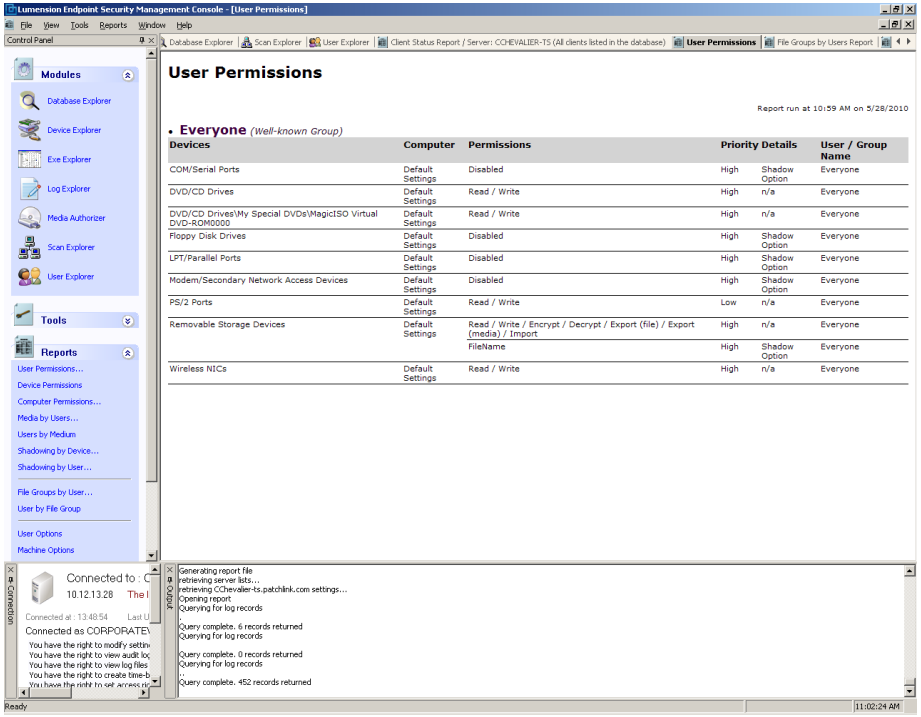
- **Per-Device Permissions:** Use granular permissions to control access at device class (for example, all USB flash drives), device group, device model or even unique ID levels; for instance, restrict access rights to a specific device of a company-approved model.
- **Default-Deny Whitelist:** Assign permissions for authorized removable devices, such as USB sticks, and media, such as DVDs or CDs, to individual users or user groups; by default, anything that is not explicitly authorized is denied.

- **Read-Only Access:** Define any device as read-only; other device permissions include write access, and encrypt/decrypt restrictions.
- **256-bit AES Encryption:** Use central security policy to force 256-bit AES encryption of all removable devices and media across all endpoints on network; options include: centralized (by admin only) vs. decentralized (by end-user), and non-portable (network accessible only) vs. portable (accessible outside the network).
- **Temporary/Scheduled Access:** Grant users temporary access to removable devices and media, for a limited period. Also, limit device usage during specific time periods.
- **Offline Enforcement:** Permissions and restrictions remain effective even when the endpoint is offline; these can be the same as when the device online, or different.
- **Uniquely Identify and Authorize Specific Media:** Authorize and manage DVD and CD collections by granting access to specific users or user groups and encrypting removable media with unique IDs.
- **Context-Sensitive Permissions:** Apply different permissions and restrictions depending on network connectivity status. For example, you can enable or disable wireless cards on laptops, depending on whether they are connected to a wired network or not.
- **Offline Updates:** Update permissions of remote endpoints that cannot establish a network connection. New permissions are saved to a file that is imported and installed onto the client computer.
- **Device Management:** Detect and manage all devices, including Plug-and-Play and non-standard devices, at the time they are inserted into the endpoint.
- **File Type Filtering:** Restrict and manage the types of files that can be moved to and from removable devices and media; combine with forced encryption for added protection.
- **Data Copy Restriction:** Restrict the daily amount of data copied to removable devices and media on a per-user basis; can also limit usage to specific timeframes and days (for example, only during normal working hours on weekdays).

Generating Reports from Lumension Device Control

Lumension Device Control comes with integrated reporting. Reports can be customized and saved into a repository, shared via email, or imported into third party applications. . Admins can log and create standard and customized reports on all device and data activity showing user permissions, for example. Figure 2 shows the report-generating interface.

Figure 2 - Lumension Report Interface



Reports can show:

- Usage of ports, devices, and media across all endpoints
- All allowed or blocked events
- Policy changes and administrator activities
- File transfers by file name and content type

In addition, event, audit and diagnostic logs can be sent as syslog messages, allowing administrators to take advantage of existing infrastructure and integrated event management. This allows for event correlation with other system logs for centralized forensics, and adds more options for alerting and reporting.

Maintaining Lumension Device Control

Minimal maintenance is required for Lumension Device Control. The administrator can easily clean up old log files in the SQL database from the Management Console. In addition, all log entries can be easily managed and exported to comma-separated value (CSV) files, which can then be imported into third-party log analyzer tools.

Security policies also require occasional maintenance. As organizations monitor device usage and data flows over time, the list of allowed devices can be tightened, especially as new devices are introduced, as new people join and others leave, and business needs evolve. Lumension's whitelist-based policy approach allows new devices to be adjusted as the need arises.

Reader Tip

Start by creating as few generalized permission sets as possible. These should include as many high-level rules as possible, with as few exceptions as possible. Define rules at both Default (or Universal) and Machine-Specific levels for groups and individual users. The policy rules will grow more complicated over time, so start simply and add exceptions as needed

Lumension Device Control in Action

As USB devices grow larger in capacity, smaller in size, and cheaper in cost, a key question for many organizations is: How do I control what removable devices employees can use at work?

The first step in answering this is to use Lumension Device Control's learning mode to discover what devices are being used on your network. This can reveal a surprising number and variety of devices in use on the endpoints in your network. The devices are categorized based on how they register themselves with Windows, down to makes and models and even specific device IDs. Here are some examples of how this information can be applied:

- **The Device Class level.** You can assign read, read / write, or deny permissions to access a specific type of device (for example, all removable storage devices).
- **The Device Group level.** You can sub-classify devices, grouping them in coherent units and then adding specific permissions and rules to each device group (for example, all USB flash drives).
- **The Device Model level.** You can define a device model and apply permissions for it (for example, all SanDisk Cruzer Titanium 8 GB flash drives).
- **The device itself.** You can manage the use of unique devices (for example, Fred's Cruzer flash drive with serial number 1x23rty789).

The next step is to define permissions. Based on the data collected and your security policy, you can define permissions for the entire organization (global), for different groups (for example, you may want different permissions for the finance group and the sales group), or even for specific individuals (for example, the CEO might be afforded special rights). These permissions might include read/write access, forced encryption, or time-based access, and can be set for individual or groups of users, machines, ports and devices

After going through the education and activation phase, you will monitor device usage and data flows, and adapt your policies and procedures to accommodate the real-world needs of your end users without compromising security. You will want to publish periodic reports to audit compliance with internal security policy (and external regulation, if applicable), and to continue to understand the gap between where you are and where you want to be. This in turn should drive reassessments and updates of your overall security policy.

Products Verified with Cisco Smart Business Architecture

Lumension Endpoint Security V4.4. is validated across Cisco Smart Business Architecture with Cisco AnyConnect 2.5.0.217.

Summary

The trend towards greater mobility of workers is accelerating due to increased productivity, greater convenience, and reduced costs. With greater mobility comes the need for increased security and protection of data at all points in your network. Along with workforce mobility, organizations are facing a growing and rapidly evolving set of security challenges, including: IT outsourcing, cybercrime, Web 2.0, and data breaches.

Lumension provides operational endpoint management and security solutions that help protect your vital information and manage your critical risk across network and endpoint assets. Lumension delivers Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and IT Risk Management Solution. Lumension Device Control enforces organization-wide policies for removable devices, removable media, and data such as read/write and encryption.

Future integration between Lumension Device Control and Cisco AnyConnect VPN will bring additional benefits to endpoint security including adaptive security policy settings where the client will adjust security automatically based on threat detection levels provided to the client through the VPN connection.

How to Contact US

End Users

- Please contact Lumension, Inc. via endpoint.support@lumension.com for any questions.
- Submit an inquiry about Lumension and the Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations.

Resellers

- Please contact Lumension via partners@lumension.com for any questions.
- For more information on how to become a Lumension reseller, please visit the Partner Section of our website at www.lumension.com/partners.

For more information on the Lumension and Cisco Partnership, please visit the Cisco Resource Center.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C07-608508-03 02/12