Lync Software Pty Ltd

LyncRMS Discover & Audit

&

Device & File Policy

Administrator Guide

Version 4.0

extend your information security
to removable media and mobile devices

Contents

Management Console

Licensing

Device & File Policy

How To……

Introduction

Lync Software has developed a range of network management and security solutions that extend your security reach to mobile devices. LyncRMS delivers an integrated removable media security solution. There are two modules:

LyncRMS – Discover & Audit
Audit all hardware and file transactional details of connecting devices

LyncRMS Device & File Security
Create policy rules regarding access to devices and file types, also implement file encryption to removable device and file shadowing.

LyncRMS is a compact Windows client based security solution, which controls access to different types of removable media devices and logs all files transfers that take place between a removable device and a PC.

LyncRMS has been designed to operate on computers running Windows XP and Windows 2000.

This document covers the use of the Management Console for Discover & Audit and Device & File Policy (including File Encryption)

LyncRMS Discover & Audit

On detecting a device, LyncRMS captures the connection date time, together with details of the storage device. When a file is subsequently transferred to/from the device, the details of the file and device are logged and this information is made available through the LyncRMS Management Console.

If a device is connected, with no subsequent file operation, then no logging is performed. Similarly, if a user attempts to connect a device and is blocked, no record of the attempt is logged to the database.

When the client is not able to make a connection with the server, eg in the case of a laptop working outside of the corporate network, LyncRMS will capture details of all file transfers and then update the server database when a network connection is re-established.

The primary purpose of LyncRMS is to identify, log and restrict files that users try to move from within the enterprise network to a removable device.

LyncRMS Management Console Version 4.0

The LyncRMS Management Console is the graphical interface that displays the audit trail of all activities associated with removable media devices that connect to the network or local PC, together with a Status tab containing details of LyncRMS installations and licensing status.

The console contains three tabs:

Audit

History - Displays a hierarchical tree view of users who have connected removable media devices to the network or local PC and the associated activities

Reports – provides a set of built-in reports.

Policy

Details on how to implement rules and policies are provided later in this document.

Status

The console has been designed to interface with Active Directory and this tab will display details of all computers in the Domain(s) and indicate whether LyncRMS has been installed, version # installed, together with details of the license status for each computer.

Computer license status can be ;

Unlicensed — The computer will be running in 'off-line' mode, where details of device connections with associated file transfers will be logged to a local database stored on the computer. Details of these 'transactions' will not be displayed in the history tree in the data tab, until the license is upgraded to Audit or Security. Following the license upgrade, all the local database 'transactions' will be automatically uploaded to the server database.

RMS Audit — Details of device connections with associated file transfers will be logged to the database and displayed in the history tree. If any rules have been applied at a domain, group, user or device level, they will not be applied unless the user has logged onto a computer which is licensed for Security.

MDA Audit — Details of PDA/MDA connections and a snapshot of the files existing on the removable device will be recorded on device connection. Rules defined and Auditing of the PDA/MDA file transfers would only be applied when the license for MDA Audit has been installed.

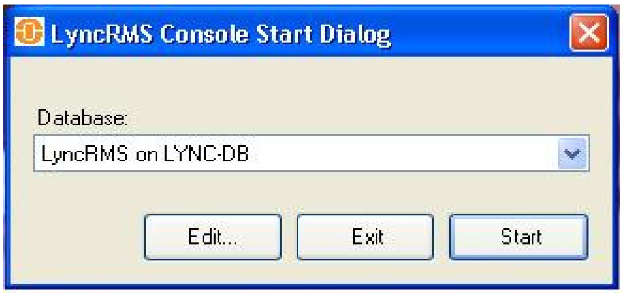
RMS Security — All rules have been applied at a domain, group, user or device level will be applied to the logged-on user. Also, if Shadowing has been enabled via the Policy tab, then it will be applied.

RMS Security & RMS Encryption — All rules which involve encryption being enforced are only applied to a user who has logged onto a computer that is licensed for Security & Encryption.

Installation

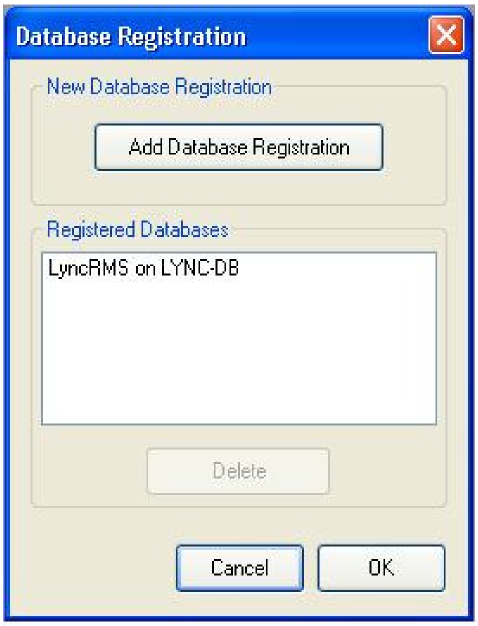
LyncRMS_Console.msi will install the Console on a local computer.

Note, the console has been configured to read data from the database that was configured during the initial install process. If the database is subsequently moved, or another database has to be added, this has to be done manually thru the Startup dialog window, using the Edit button to display the Database registration window. This feature allows the application to use multiple databases thru large networks.



Database: LyncRMS on LYNC-DB

Console Startup Dialog Window



LyncRMS on LYNC-DB

Database Registration Window

The Console requires .NET Framework Version 2.0 (22 MB) to be installed on the host computer

This can be downloaded from the Microsoft website at

http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en

How to use the Management Console

If the error "*Login failed for user lyncadmin*" is displayed when the console starts up, it is possible the SQL Server that is hosting the database has its authentication set to Windows Only, however it will require SQL Server & Windows (ie mixed mode) for LyncRMS to function correctly.

Use a valid Windows login to connect to SQL Server, then change the security authentication mode in SQL Server to **SQL Server and Windows**. To do this, follow these steps:

1. Start Enterprise Manager.
2. Expand **Microsoft SQL Servers**, and then expand **SQL Server Group**.
3. Right-click the server that you want to change to **SQL Server and Windows** authentication, and then click **Properties**.
4. In the **SQL Server Properties** dialog box, click the **Security** tab, click **SQL Server and Windows**, and then click **OK**.
5. When you are prompted to re-start the SQL Server service, click **Yes**.

Audit Tab -> Selecting Date Range

There are two methods of displaying data in the console in both the audit and reporting tabs:

Date range - Enter a from and to date range

Predetermined period - Select the period from a drop down list (e.g. Yesterday, Today etc)

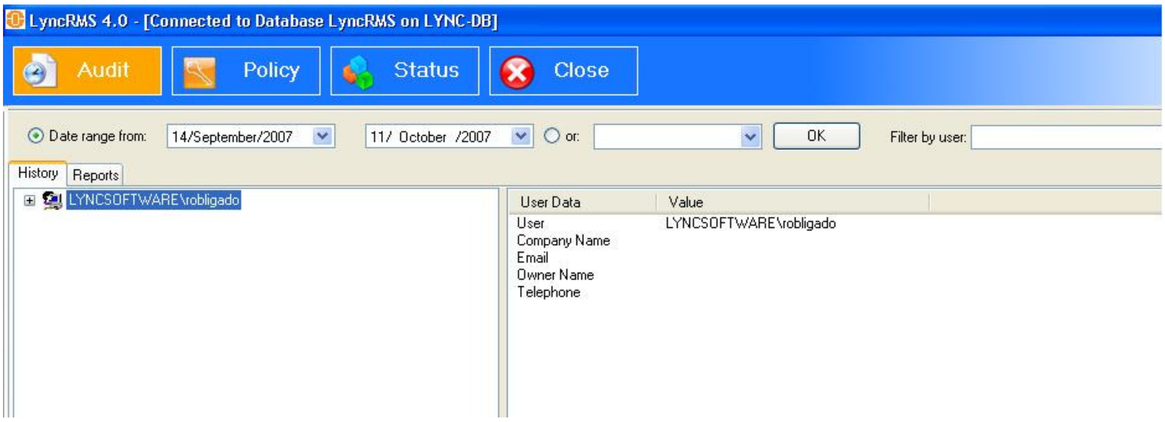
The history tree can also be filtered further by entering a User name into the Filter by User text box.

To generate a User report displaying details of all activity for the selected period, right-click on the User name in the tree and select Generate User Report.

A report will be opened in a separate window. Further information regarding reports is described later in this document.

Navigating The Hierarchical Tree

The console has a collapsible tree display. Double click on the user name to expand the tree to provide additional details about devices and associated file transfers. Select one of the items on the collapsed nodes to show the details in the display window.



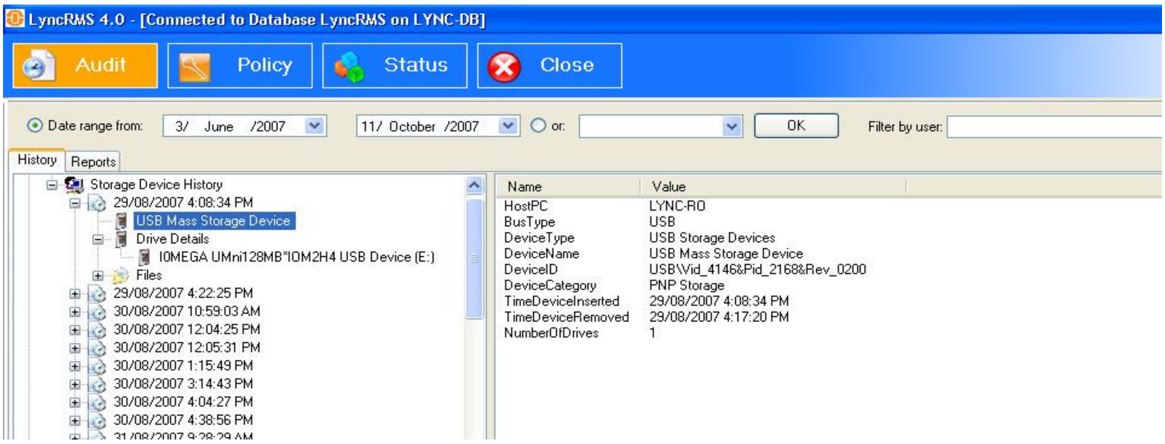
● Date range from: 14/September/2007 11/ October /2007 ○ or: Filter by user:

LYNCSOFTWARE\robligado

User Data	Value
User	LYNCSOFTWARE\robligado
Company Name	
Email	
Owner Name	
Telephone	

By expanding the User name, the tree will display details of all removable devices, which have been used to transfer files.

The tree displays details of the device, together with date/time of connection and disconnection.

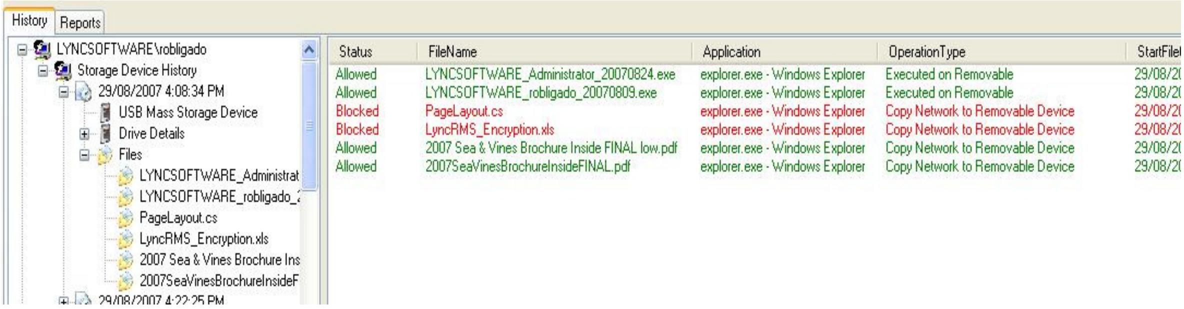


● Date range from: 3/ June /2007 11/ October /2007 ○ or: Filter by user:

- Storage Device History
  - 29/08/2007 4:08:34 PM
    - USB Mass Storage Device
    - Drive Details
      - IOMEGA UMni128MB*IOM2H4 USB Device (E:)
    - Files
  - 29/08/2007 4:22:25 PM
  - 30/08/2007 10:59:03 AM
  - 30/08/2007 12:04:25 PM
  - 30/08/2007 12:05:31 PM
  - 30/08/2007 1:15:49 PM
  - 30/08/2007 3:14:43 PM
  - 30/08/2007 4:04:27 PM
  - 30/08/2007 4:38:56 PM
  - 31/08/2007 9:28:29 AM

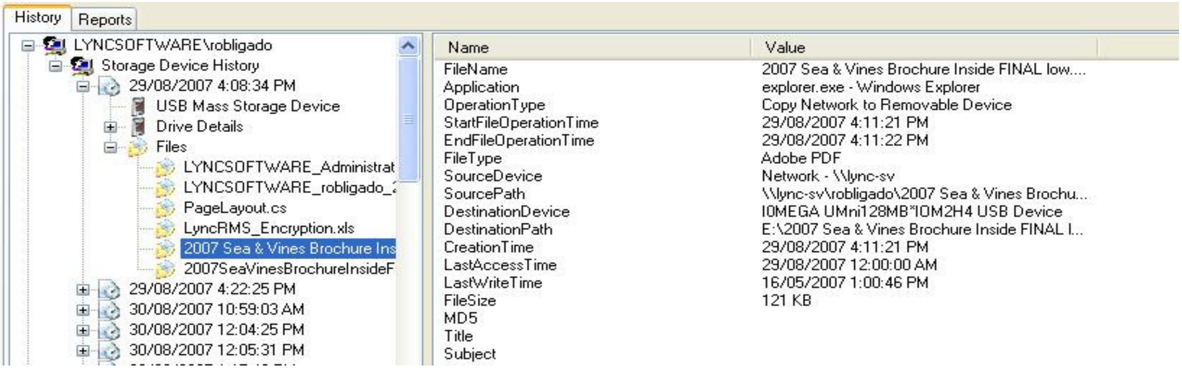
Name	Value
HostPC	LYNC-RO
BusType	USB
DeviceType	USB Storage Devices
DeviceName	USB Mass Storage Device
DeviceID	USB\Vid_4146&Pid_2168&Rev_0200
DeviceCategory	PNP Storage
TimeDeviceInserted	29/08/2007 4:08:34 PM
TimeDeviceRemoved	29/08/2007 4:17:20 PM
NumberOfDrives	1

By expanding the file nodes, the display window will show the list of files transferred, that can be sorted by clicking on the applicable column heading.



Status	FileName	Application	OperationType	StartFile
Allowed	LYNCSOFTWARE_Administrator_20070824.exe	explorer.exe - Windows Explorer	Executed on Removable	29/08/2
Allowed	LYNCSOFTWARE_robligado_20070809.exe	explorer.exe - Windows Explorer	Executed on Removable	29/08/2
Blocked	PageLayout.cs	explorer.exe - Windows Explorer	Copy Network to Removable Device	29/08/2
Blocked	LyncRMS_Encryption.xls	explorer.exe - Windows Explorer	Copy Network to Removable Device	29/08/2
Allowed	2007 Sea & Vines Brochure Inside FINAL low.pdf	explorer.exe - Windows Explorer	Copy Network to Removable Device	29/08/2
Allowed	2007SeaVinesBrochureInsideFINAL.pdf	explorer.exe - Windows Explorer	Copy Network to Removable Device	29/08/2

File records are colour coded to see 'at a glance' which ones have been blocked by policies.



Name	Value
FileName	2007 Sea & Vines Brochure Inside FINAL low....
Application	explorer.exe - Windows Explorer
OperationType	Copy Network to Removable Device
StartFileOperationTime	29/08/2007 4:11:21 PM
EndFileOperationTime	29/08/2007 4:11:22 PM
FileType	Adobe PDF
SourceDevice	Network - \\lync-sv
SourcePath	\\lync-sv\robligado\2007 Sea & Vines Brochu...
DestinationDevice	IOMEGA UMni128MB*IOM2H4 USB Device
DestinationPath	E:\2007 Sea & Vines Brochure Inside FINAL l...
CreationTime	29/08/2007 4:11:21 PM
LastAccessTime	29/08/2007 12:00:00 AM
LastWriteTime	16/05/2007 1:00:46 PM
FileSize	121 KB
MD5	
Title	
Subject	

Select an individual file to display the file attributes and additional details of the file transferred

Reports

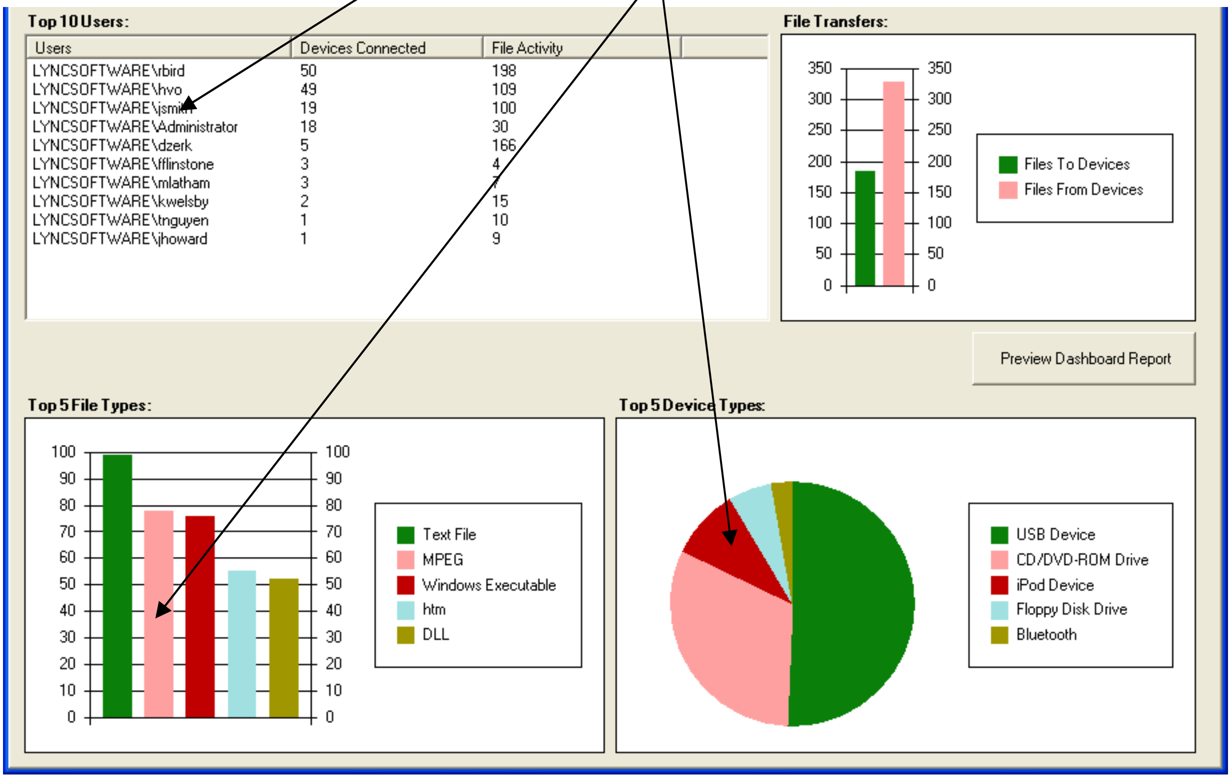
The LyncRMS Management Console also provides a suite of built-in reports to enable an administrator to generate removable device usage based on Users, File Types and Device Types.

The console displays a dashboard type report showing :

- Top 10 Users (by number of devices connected)
- Top 5 File Types transferred
- Top 5 Device Types connected or detected

This Dashboard Report can also be printed by clicking on Preview Dashboard Report button.

To generate a specific report, 'right click' on a User or within a section in one of the graphs and click 'Show Details'



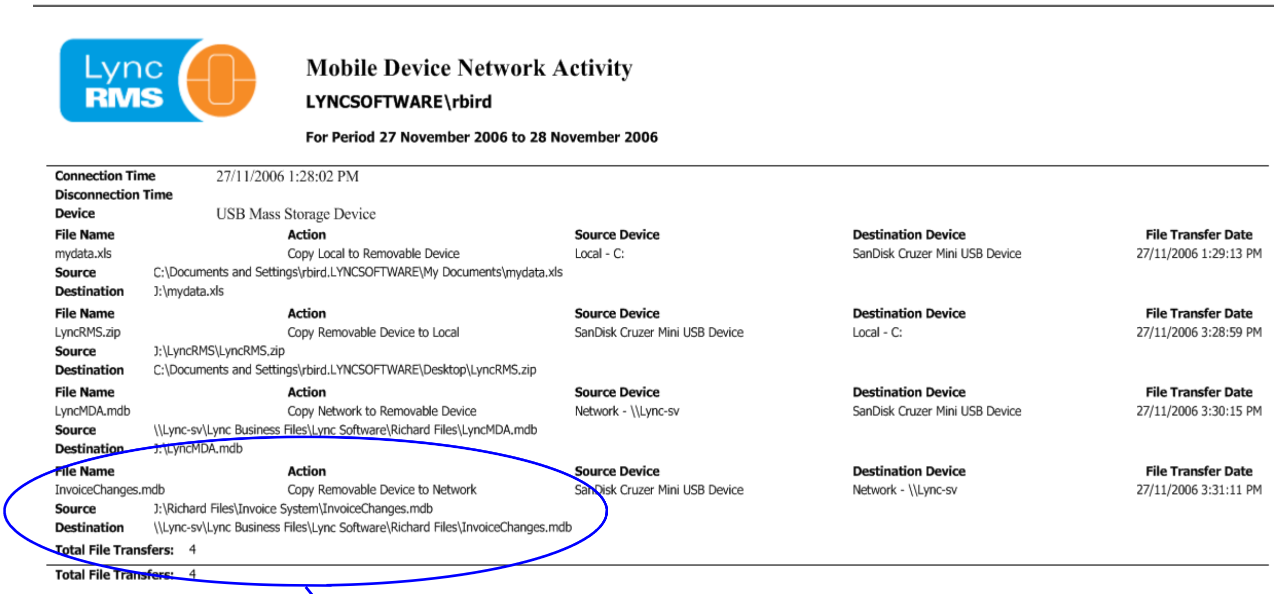
Top 10 Users:

Users	Devices Connected	File Activity
LYNCSOFTWARE\rbird	50	198
LYNCSOFTWARE\hvo	49	109
LYNCSOFTWARE\jsmith	19	100
LYNCSOFTWARE\Administrator	18	30
LYNCSOFTWARE\dzerk	5	166
LYNCSOFTWARE\fflinstone	3	4
LYNCSOFTWARE\mlatham	3	7
LYNCSOFTWARE\kwelsby	2	15
LYNCSOFTWARE\tnguyen	1	10
LYNCSOFTWARE\jhoward	1	9

The entered date range generates data for both the History tree and built-in reports.

User Report

To generate a report for a specific user, enter the date range and the user name in the Filter by User text box, then click OK button. Next right click on the User name in the **History** tree and select **Generate User Report**.



Mobile Device Network Activity

LYNCSOFTWARE\rbird

For Period 27 November 2006 to 28 November 2006

Connection Time 27/11/2006 1:28:02 PM
Disconnection Time
Device USB Mass Storage Device

File Name	Action	Source Device	Destination Device	File Transfer Date
mydata.xls	Copy Local to Removable Device	Local - C:	SanDisk Cruzer Mini USB Device	27/11/2006 1:29:13 PM

Source C:\Documents and Settings\rbird.LYNCSOFTWARE\My Documents\mydata.xls
Destination J:\mydata.xls

File Name	Action	Source Device	Destination Device	File Transfer Date
LyncRMS.zip	Copy Removable Device to Local	SanDisk Cruzer Mini USB Device	Local - C:	27/11/2006 3:28:59 PM

Source J:\LyncRMS\LyncRMS.zip
Destination C:\Documents and Settings\rbird.LYNCSOFTWARE\Desktop\LyncRMS.zip

File Name	Action	Source Device	Destination Device	File Transfer Date
LyncMDA.mdb	Copy Network to Removable Device	Network - \\Lync-sv	SanDisk Cruzer Mini USB Device	27/11/2006 3:30:15 PM

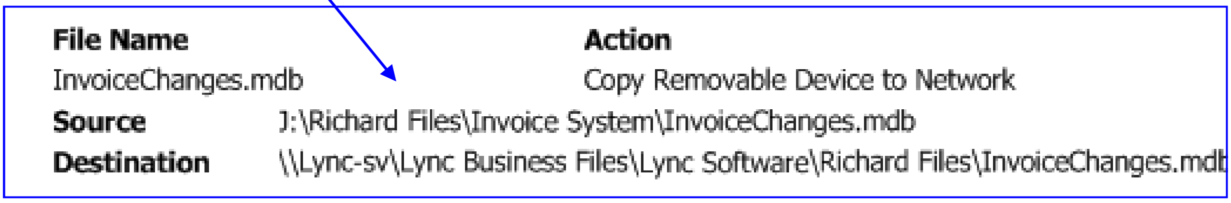
Source \\Lync-sv\Lync Business Files\Lync Software\Richard Files\LyncMDA.mdb
Destination J:\LyncMDA.mdb

File Name	Action	Source Device	Destination Device	File Transfer Date
InvoiceChanges.mdb	Copy Removable Device to Network	SanDisk Cruzer Mini USB Device	Network - \\Lync-sv	27/11/2006 3:31:11 PM

Source J:\Richard Files\Invoice System\InvoiceChanges.mdb
Destination \\Lync-sv\Lync Business Files\Lync Software\Richard Files\InvoiceChanges.mdb

Total File Transfers: 4

Total File Transfers: 4

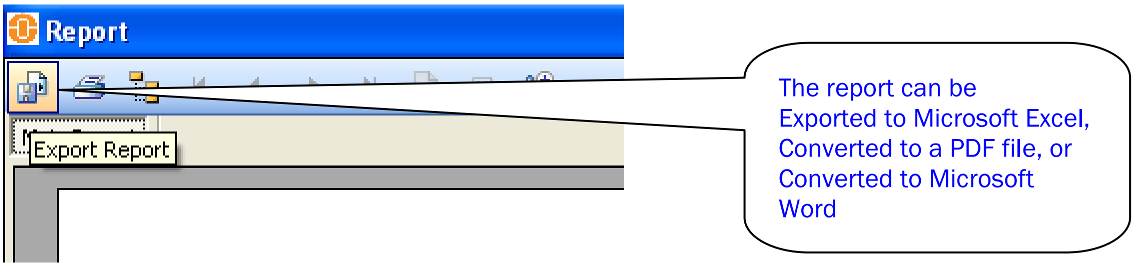


File Name	Action
InvoiceChanges.mdb	Copy Removable Device to Network

Source J:\Richard Files\Invoice System\InvoiceChanges.mdb
Destination \\Lync-sv\Lync Business Files\Lync Software\Richard Files\InvoiceChanges.mdb

Report contains full details of the 'file transaction'.

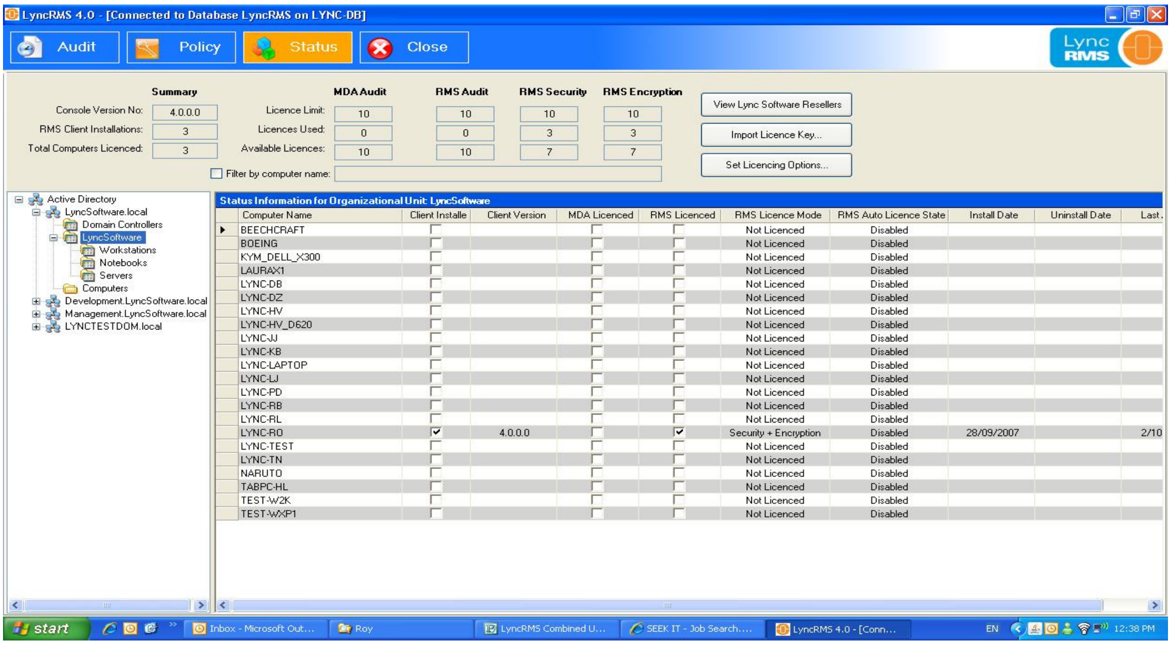
The report can be converted to different formats for emailing or converted into an Excel spreadsheet for further analysis, by clicking on this icon



The report can be Exported to Microsoft Excel, Converted to a PDF file, or Converted to Microsoft Word

Status & Licensing

This tab displays details of the status of LyncRMS installations and numbers of licenses purchased and available for install.



Summary

Console Version No: 4.0.0.0

RMS Client Installations: 3

Total Computers Licenced: 3

	MDA Audit	RMS Audit	RMS Security	RMS Encryption
Licence Limit:	10	10	10	10
Licences Used:	0	0	3	3
Available Licences:	10	10	7	7

☐ Filter by computer name:

Status Information for Organizational Unit: LyncSoftware

Computer Name	Client Installe	Client Version	MDA Licenced	RMS Licenced	RMS Licence Mode	RMS Auto Licence State	Install Date	Uninstall Date	Last.
BEECHCRAFT	☐		☐	☐	Not Licenced	Disabled			
BOEING	☐		☐	☐	Not Licenced	Disabled			
KYM_DELL_X300	☐		☐	☐	Not Licenced	Disabled			
LAURAX1	☐		☐	☐	Not Licenced	Disabled			
LYNC-DB	☐		☐	☐	Not Licenced	Disabled			
LYNC-DZ	☐		☐	☐	Not Licenced	Disabled			
LYNC-HV	☐		☐	☐	Not Licenced	Disabled			
LYNC-HV_D620	☐		☐	☐	Not Licenced	Disabled			
LYNC-JJ	☐		☐	☐	Not Licenced	Disabled			
LYNC-KB	☐		☐	☐	Not Licenced	Disabled			
LYNC-LAPTOP	☐		☐	☐	Not Licenced	Disabled			
LYNC-LJ	☐		☐	☐	Not Licenced	Disabled			
LYNC-PD	☐		☐	☐	Not Licenced	Disabled			
LYNC-RB	☐		☐	☐	Not Licenced	Disabled			
LYNC-RL	☐		☐	☐	Not Licenced	Disabled			
LYNC-RO	☑	4.0.0.0	☐	☑	Security + Encryption	Disabled	28/09/2007		2/10
LYNC-TEST	☐		☐	☐	Not Licenced	Disabled			
LYNC-TN	☐		☐	☐	Not Licenced	Disabled			
NARUTO	☐		☐	☐	Not Licenced	Disabled			
TABPC-HL	☐		☐	☐	Not Licenced	Disabled			
TEST-W2K	☐		☐	☐	Not Licenced	Disabled			
TEST-WXP1	☐		☐	☐	Not Licenced	Disabled			

Licensing Principles

LyncRMS is licensed through a purchase of a license key, which is imported either at the time of initial installation (see LyncRMS Installation Guide for details), or using the **Import License Key** button on this screen.

There is no limit to the number of computers that LyncRMS can be installed on, however the full audit/security functionality will not be enabled until the client computer is licensed. Licensing takes place either automatically, when LyncRMS is installed on the client computer, or are manually licensed either by selecting individual computers, or by selecting a Group from the tree.

Note—Automatic Licensing is turned on by default

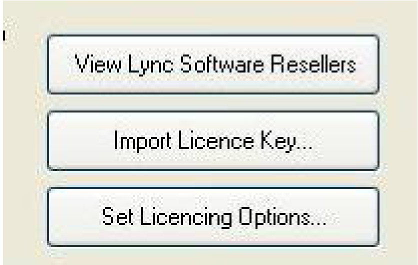
With manual licensing, if insufficient licenses are available to be assigned to the selected group of computers, then **none** of the computers in the group will be licensed. An information message saying 'Insufficient Licenses" will be displayed, however the unlicensed computers will continue to provide Audit functionality in off-line mode and once they become licensed, the off-line data will be uploaded.

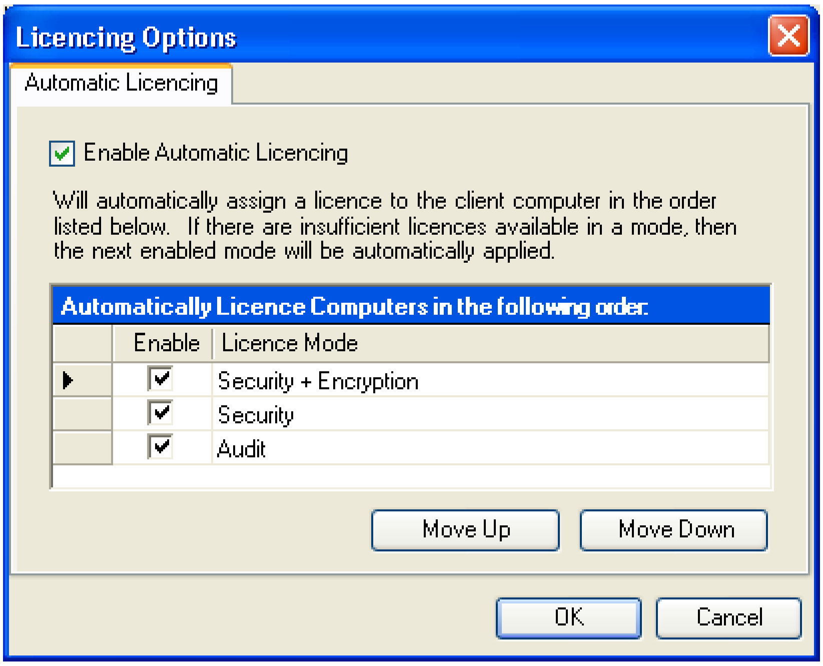
Further licenses can be made available either by removing a license from a computer/group of computers or purchasing further licenses from your vendor.

Licensing is very flexible and allows you to have a mixture of different licenses for different groups or even different computers within a group. Also licenses can be swapped between different machines to provide immediate security cover, ie in cases where a breach has occurred and security rules need to be applied immediately.

Automatic Licensing

In order to simplify the licensing process, Automatic Licensing is **enabled by default** and will apply licenses determined by the priority listed in Automatic Licensing configuration screen, accessed by clicking on the Set Licensing Options button





Licencing Options

Automatic Licencing

☑ Enable Automatic Licencing

Will automatically assign a licence to the client computer in the order listed below. If there are insufficient licences available in a mode, then the next enabled mode will be automatically applied.

Automatically Licence Computers in the following order:

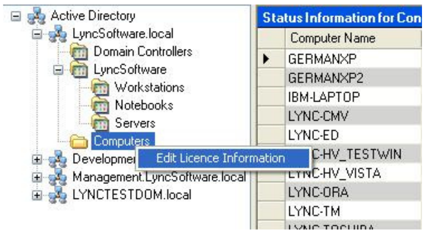
	Enable	Licence Mode
▶	☑	Security + Encryption
	☑	Security
	☑	Audit

In cases where there are insufficient licenses available for the 'preferred' License mode, the next priority is then applied. If there are insufficient licenses available for any mode, the client computer will be classified as Unlicensed and this status will be displayed on the Status screen.

With Automatic licensing, the first mode listed will be applied only if the license key is valid for that mode.

For Enterprise licensing, licenses will be applied automatically to the highest enabled level, assuming the license key is valid for that level.

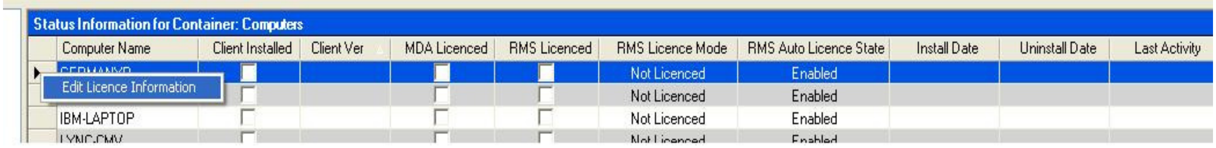
Manual Licensing



Status Information for Con

Computer Name
GERMANXP
GERMANXP2
IBM-LAPTOP
LYNC-CMV
LYNC-ED
C-HV_TESTWIN
LYNC-HV_VISTA
LYNC-ORA
LYNC-TM

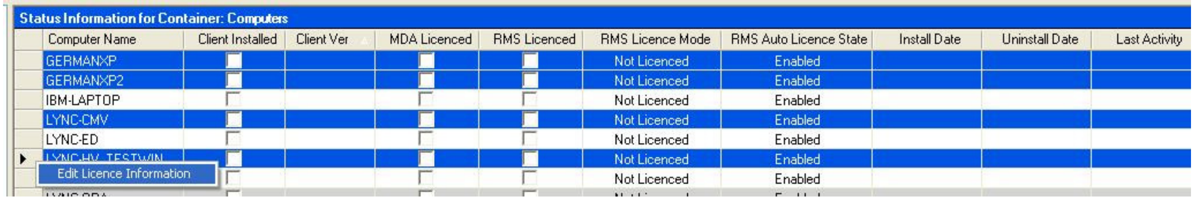
You can apply licenses at a Group level by right clicking on the organizational unit, and on the “Edit License Information” window and assign licenses for the entire group.



Status Information for Container: Computers

Computer Name	Client Installed	Client Ver	MDA Licenced	RMS Licenced	RMS Licence Mode	RMS Auto Licence State	Install Date	Uninstall Date	Last Activity
	☐		☐	☐	Not Licenced	Enabled			
	☐		☐	☐	Not Licenced	Enabled			
IBM-LAPTOP	☐		☐	☐	Not Licenced	Enabled			

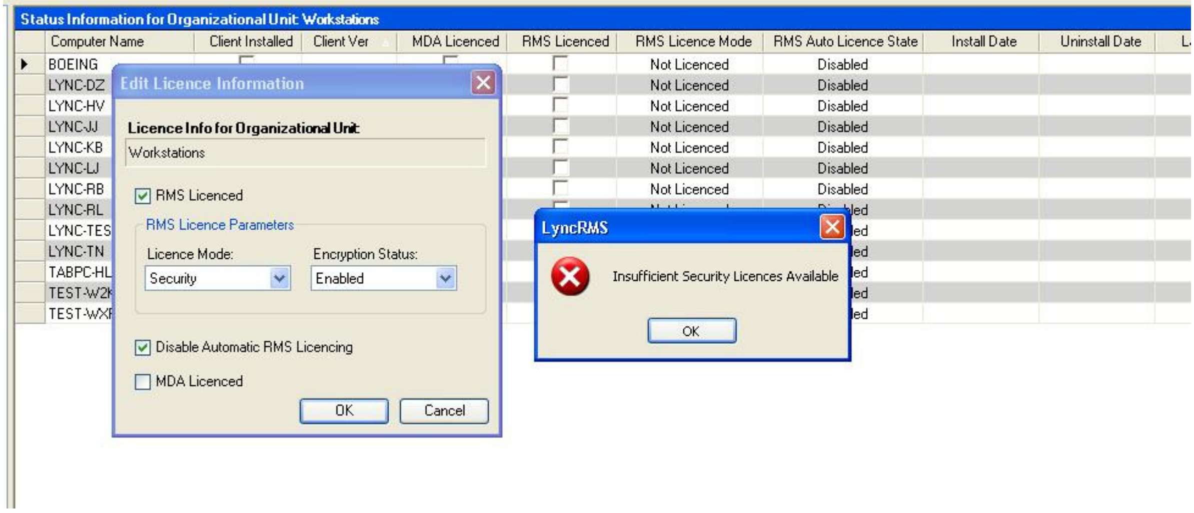
Individual computers can also be licensed by selecting the row or record and right clicking on the left most column of the selected record to display the License information window.



Status Information for Container: Computers

Computer Name	Client Installed	Client Ver	MDA Licenced	RMS Licenced	RMS Licence Mode	RMS Auto Licence State	Install Date	Uninstall Date	Last Activity
GERMANXP	☐		☐	☐	Not Licenced	Enabled			
GERMANXP2	☐		☐	☐	Not Licenced	Enabled			
IBM-LAPTOP	☐		☐	☐	Not Licenced	Enabled			
LYNC-CMV	☐		☐	☐	Not Licenced	Enabled			
LYNC-ED	☐		☐	☐	Not Licenced	Enabled			
	☐		☐	☐	Not Licenced	Enabled			
	☐		☐	☐	Not Licenced	Enabled			

The option to edit two or more records/users/computers (as shown above) is done by selecting several records, holding down the Shift or Ctrl key and right clicking on any selected record to display the edit license information window.



Status Information for Organizational Unit: Workstations

Computer Name	Client Installed	Client Ver	MDA Licenced	RMS Licenced	RMS Licence Mode	RMS Auto Licence State	Install Date	Uninstall Date
BOEING				☐	Not Licenced	Disabled		
LYNC-DZ				☐	Not Licenced	Disabled		
LYNC-HV				☐	Not Licenced	Disabled		
LYNC-JJ				☐	Not Licenced	Disabled		
LYNC-KB				☐	Not Licenced	Disabled		
LYNC-LJ				☐	Not Licenced	Disabled		
LYNC-RB				☐	Not Licenced	Disabled		
LYNC-RL								
LYNC-TES								
LYNC-TN								
TABPC-HL								
TEST-W2k								
TEST-WXF								

Licence Info for Organizational Unit: Workstations

☑ RMS Licenced

Licence Mode: Security

Encryption Status: Enabled

☑ Disable Automatic RMS Licencing

☐ MDA Licenced

Insufficient Security Licences Available

The “Edit License Information” window has added options for assigning licenses for file encryption and PDA/MDA. It also has the option to disable Automatic licensing for the selected computers. Should there be no or insufficient licenses available then a message window will be displayed to inform users that there are “Insufficient Security or Encryption licenses available”.

Status

The left hand pane contains a hierarchical tree representing your Active Directory structure. You can then navigate through the hierarchy by opening and closing needs to display details of computers in the right hand pane.

To filter for specific computers, start typing the name of the computer into the "Filter By Computer name" text box and the tree will automatically contract/expand.

LyncRMS Installed & Client Version Columns

These indicate whether the LyncRMS client has been installed together with the version number.

Note – it is not an indicator that the client service is running on the computer. (This functionality will be provided at a later date)

MDA Lincensed — RMS Lincensed — RMS Lincensed Mode — RMS Auto License State

These columns indicate whether the client has been licensed for PDA/MDA, Audit or Security or both. It also indicates whether the client has auto licensing enabled or disabled.

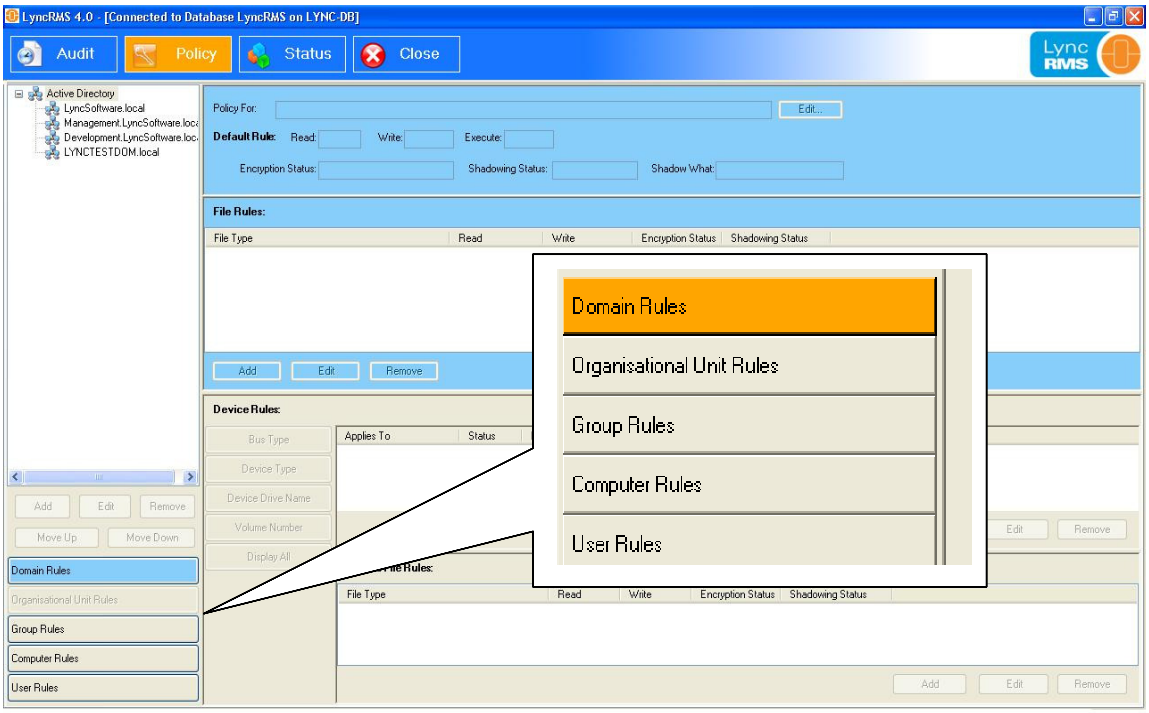
Install Date – Uninstall Date – Last Activity Columns

These provide a history of when the client was installed and the last date of any file transfer activities (in licensed mode only)

LyncRMS Device & File Policy Overview

Rules and policies can be implemented at varying levels of granularity (domain, groups users etc) and can apply to devices and file types, reflecting an organisation's own data security policies.

The rules engine within LyncRMS is a powerful and flexible tool to enable an administrator to implement device and file rules at various levels from Domain right down to an individual user's own USB device.



Device rules are implemented in a hierarchical structure, based on Active Directory levels and work upwards from User level.

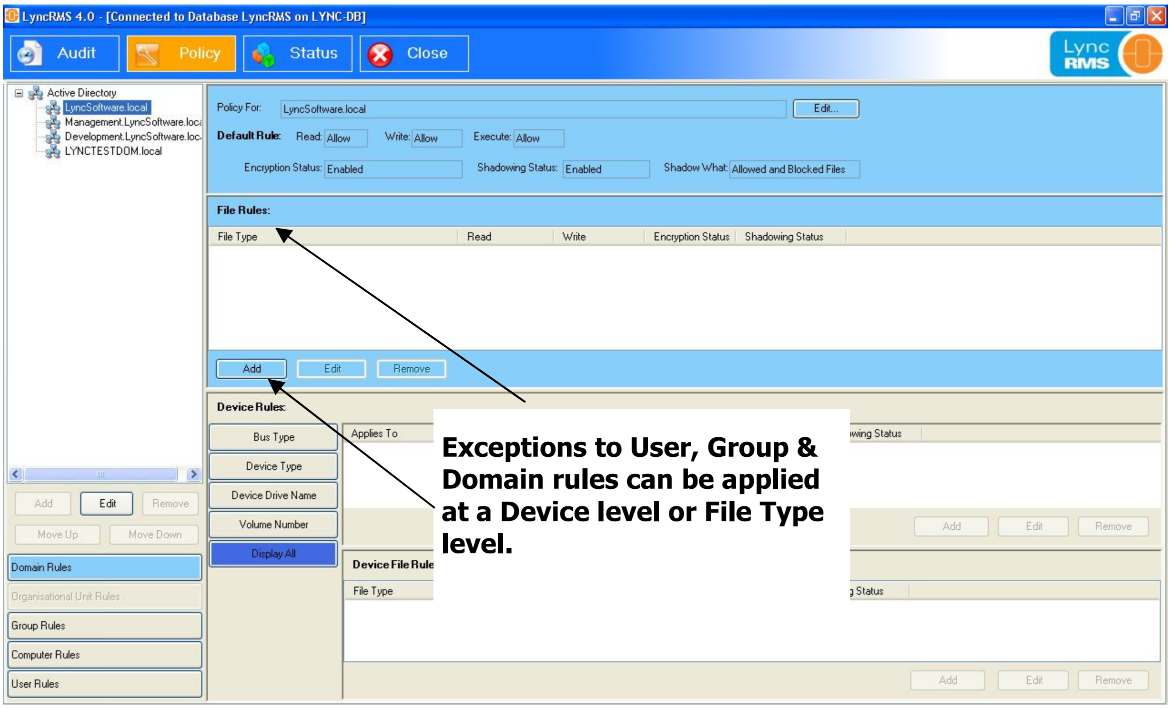
The application firstly checks if there are any User rules, if none then it checks if the Computer has any rules applied. This process continues until either a rule is 'found' or it reaches Domain level. At Domain level there is always a default rule, which will result in the device being blocked or enabled.

Exceptions to Device based rules can be implemented at Device level or File Type or File Group, for example all removable devices can be blocked with the exception of a specific brand/model. To allow a specific device to connect, you can configure a Device Rule to be Enabled or Disabled or Restricted.

Enabled – the device operates with no restrictions applied and the user can view contents and copy move files.

Disabled– the device is blocked and the user is not permitted to access any content.

Restricted – enables you to control whether files can be copied to/from the device.



Policy For: LyncSoftware.local

Default Rule: Read: Allow Write: Allow Execute: Allow

Encryption Status: Enabled Shadowing Status: Enabled Shadow What: Allowed and Blocked Files

Exceptions to User, Group & Domain rules can be applied at a Device level or File Type level.

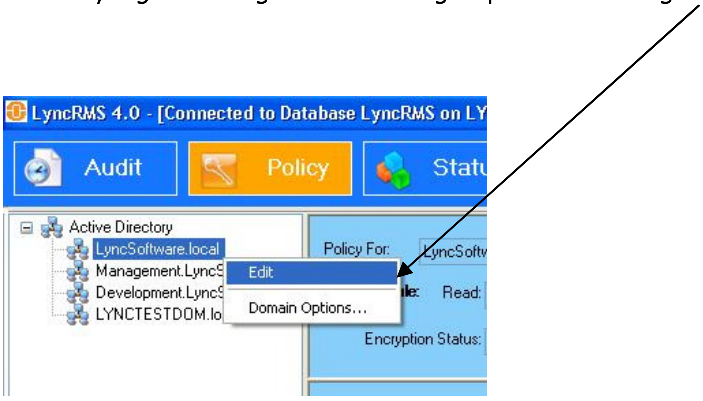
Exceptions can be applied to specific devices, by creating a Device Name Rule and selecting one of the devices from the list. The list contains details of all devices that have previously connected and had files transferred either to or from the device. (See Device Rules section for further details)

Exceptions can also apply to File Types, for example a rule can be configured to permit PDF files, but block all other file types. (See File Type Rules section for further details)

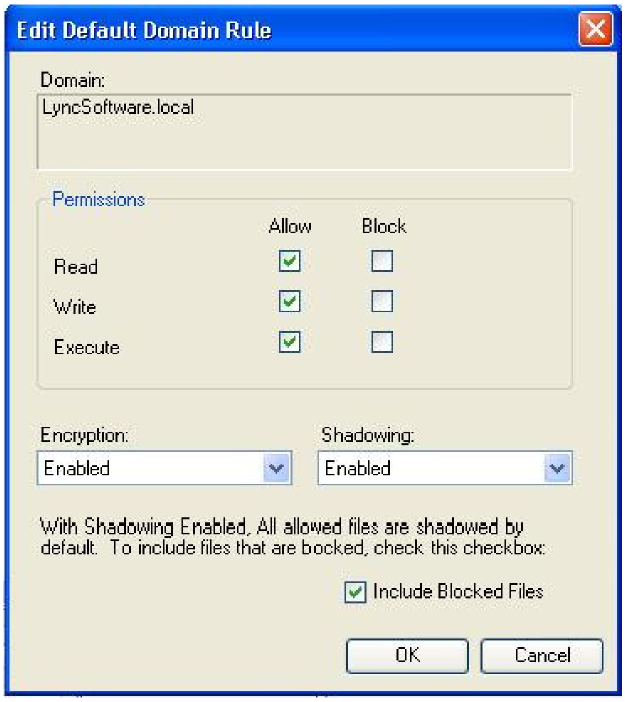
Additional rules can be applied to ensure that all files transferred to devices are automatically encrypted and/or shadowed.

Further details on file encryption and shadowing are provided later in this document.

Rules for Domain(s), Users, Groups and Computers can be edited/applied thru the rules definition window which could be accessed by right-clicking on the said group and selecting **Edit** from the popup menu.



Domain Level Rule



Edit Default Domain Rule

Domain:
LyncSoftware.local

Permissions

	Allow	Block
Read	☑	☐
Write	☑	☐
Execute	☑	☐

Encryption: Enabled

Shadowing: Enabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are bocked, check this checkbox:

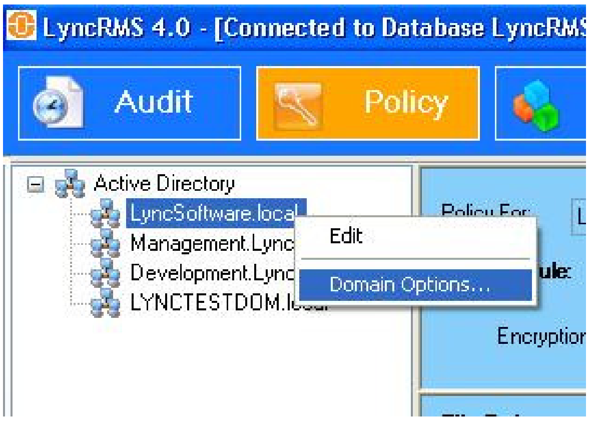
☑ Include Blocked Files

OK Cancel

LyncRMS supports domains and sub-domains, which means that different rules can be applied for different sub-domains. LyncRMS checks for the domain for the current logged on user and then applies rules according to this domain

Read— permits files to be copied **from** the device to the local computer/network location.
Write— permits files to be copied **to** a device from local computer/network location.
Execute – permits executable files to be executed on the device

Encryption — if set to Enabled, will automatically encrypt all files, when copied **to** a removable device.

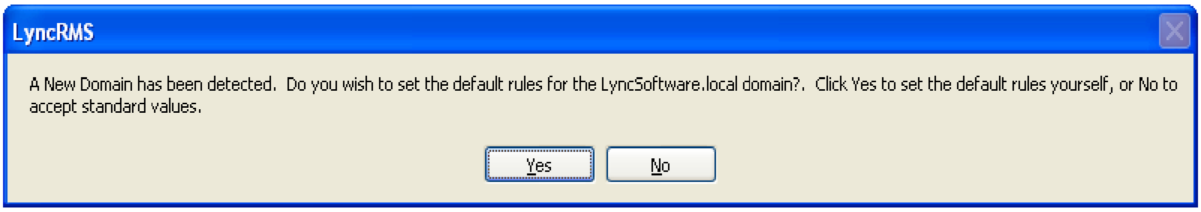


Shadowing — if set to Enabled, a copy of the actual file will be stored in the network Shadow location, specified by the Administrator, by right-clicking on the domain and selecting **Domain Options**

There is also an option to Shadow Blocked Files, so where there is an attempt to copy a file which has been blocked by a rule, the file(s) involved will be copied to the Shadow folder.

Domain Level Rule……..

When the Policy screen is opened for the **first time** following installation, it will prompt you to create a default rule for the domain.

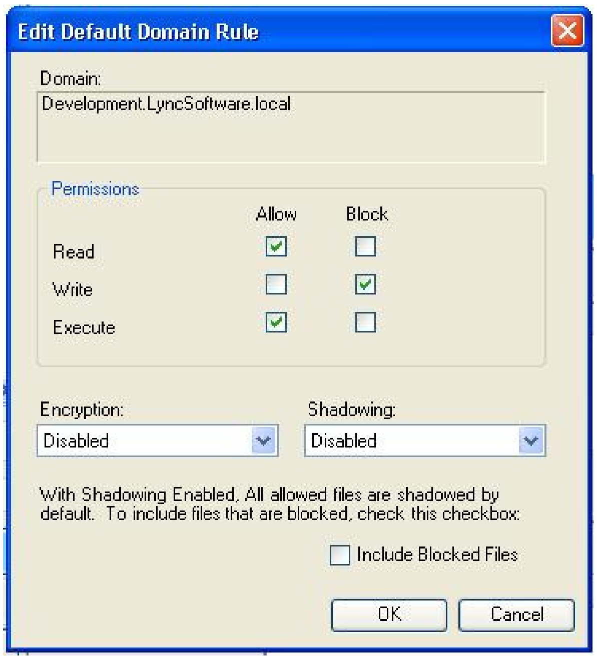


LyncRMS

A New Domain has been detected. Do you wish to set the default rules for the LyncSoftware.local domain?. Click Yes to set the default rules yourself, or No to accept standard values.

Note—if you have multiple domains, the same message will be displayed for **each domain**

If you select Yes, the following screen is displayed, to enable you to set your own default.



Edit Default Domain Rule

Domain: Development.LyncSoftware.local

Permissions

	Allow	Block
Read	☑	☐
Write	☐	☑
Execute	☑	☐

Encryption: Disabled

Shadowing: Disabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

☐ Include Blocked Files

If you select No, a default Domain level rule will automatically be created, as follows

Read – Allow, Write – Block, Execute - Allow

This will **allow** a user to copy files from the device to the local computer/network and **block** files being copied from the local computer/network to a device.

Block Access to All Devices—Black List

To implement a 'black-list' environment, that is **allow all** devices to be connected and **all** file types to be transferred to/from devices, and then **block** by exception, set the Domain policy to

Read – Allow, Write – Allow, Execute - Allow

Allow Access to All Devices—White List

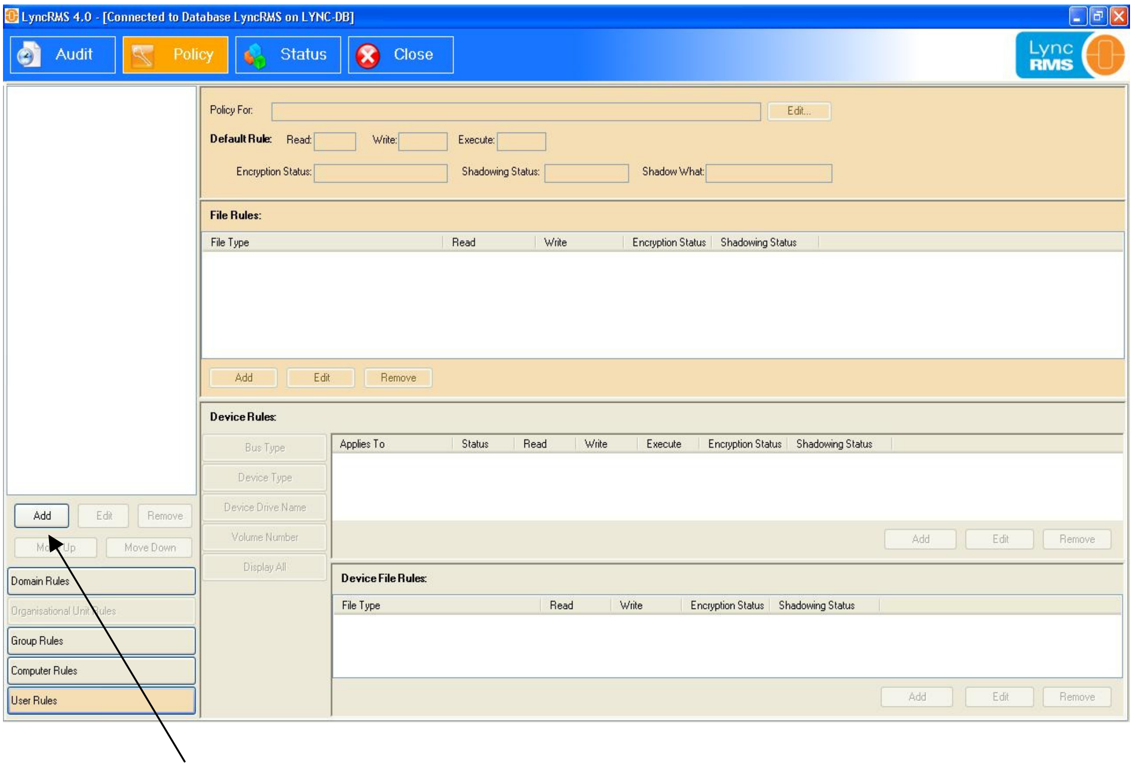
To implement a 'white-list' environment, that is **block all** devices to be connected and **all** file types to be transferred to/from devices, and then **allow** by exception, set the Domain policy to

Read – Block, Write – Block, Execute - Block

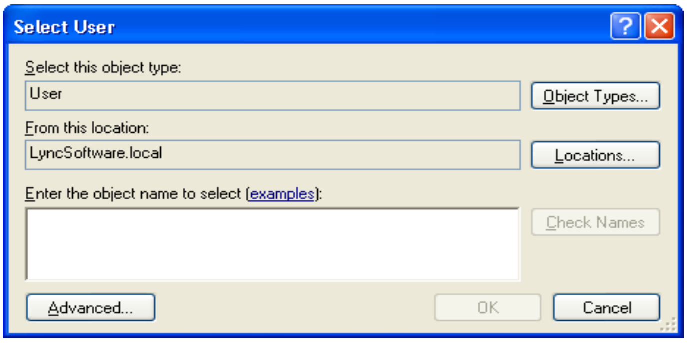
Note—This will prevent a user from accessing **all** removable and internal storage devices, including USB, CD/DVD, Floppy drives etc.

User Level Rules

To implement a User Rule, ensure the User Rule section is highlighted



Next, click the **Add** button, which will open a standard Active Directory dialog form, from which you can enter a user name.



Select this object type: User

From this location: LyncSoftware.local

Enter the object name to select (examples):

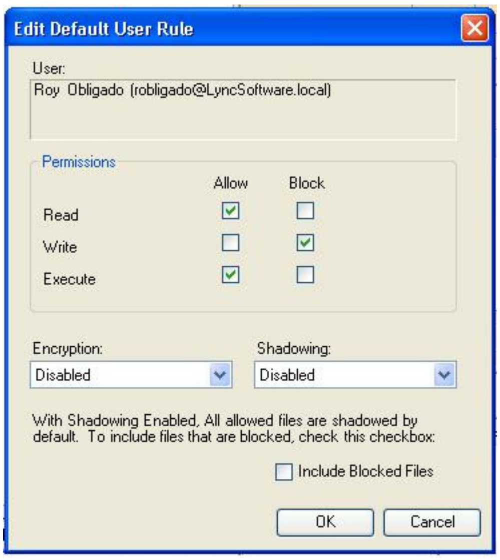
The default rule is :-

Read – Allow, Write – Block, Execute - Allow

Allows files to be copied from the device **to** the local computer/network and **block** files being copied **from** the local computer/network to a device.

If an exception to this rule is required, then a Device Rule or File Type rule can be implemented for this user.

For example, the user may be allowed to copy PDF files to a device, but block all other file types.



User: Roy Obligado (robligado@LyncSoftware.local)

	Allow	Block
Read	☑	☐
Write	☐	☑
Execute	☑	☐

Encryption: Disabled

Shadowing: Disabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

☐ Include Blocked Files

Device Rules

Device Rules can be implemented at 4 levels :-

Bus Type
Device Type (generic name for the device type)
Device Drive Name (name of the device model)
Volume Number (equivalent to a unique serial number for each device)

LyncRMS checks for Device Rules from Volume Number up through the list to Bus Type, which enables a fine level of granularity to be enforced. For example a user could be blocked from using any USB storage device, with the exception of one specific device identified by volume number.

Bus Type

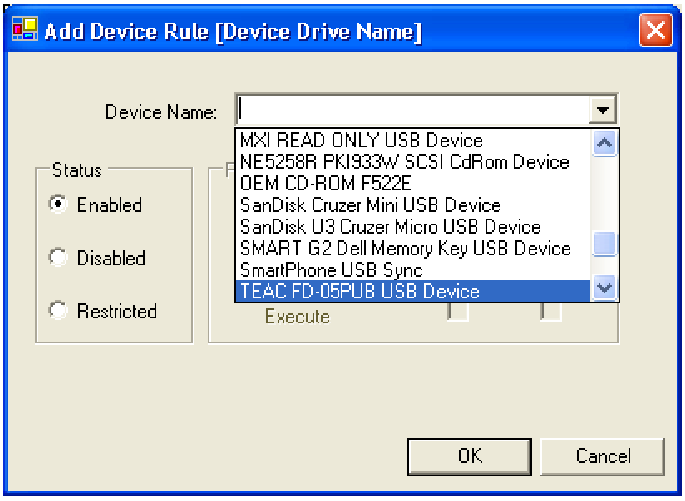
Controls connections for the User via the following ports (USB, Firewire, Infrared, Bluetooth, WiFi, PCMCIA)

Device Type

Control connections for a range of storage devices including (USB, iPod, SD Card, MMC, Palm, Windows CE, Floppy Disk, RIM Blackberry, digital cameras)

Device Drive Name

The interface presents a list of all Devices which have previously been detected or you can enter a 'new' name directly into the drop down list.


Add Device Rule [Device Drive Name]
Device Name:
MXI READ ONLY USB Device
NE5258R PKI933W SCSI CdRom Device
OEM CD-ROM F522E
SanDisk Cruzer Mini USB Device
SanDisk U3 Cruzer Micro USB Device
SMART G2 Dell Memory Key USB Device
SmartPhone USB Sync
TEAC FD-05PUB USB Device
Execute
OK
Cancel

Status
● Enabled
○ Disabled
○ Restricted

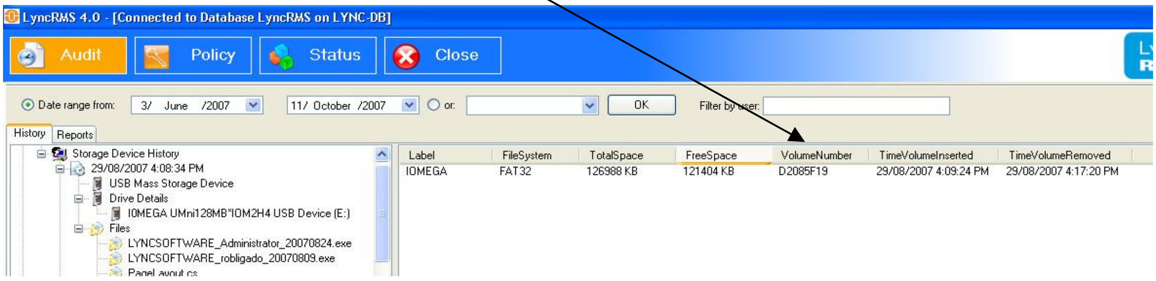
As with other rules, specific devices can be Enabled, Disabled or Restricted.

Volume Number

The interface presents a list of all Volume Numbers have previously been detected or you can enter a 'new' number directly into the drop down list.

Device Rules.......

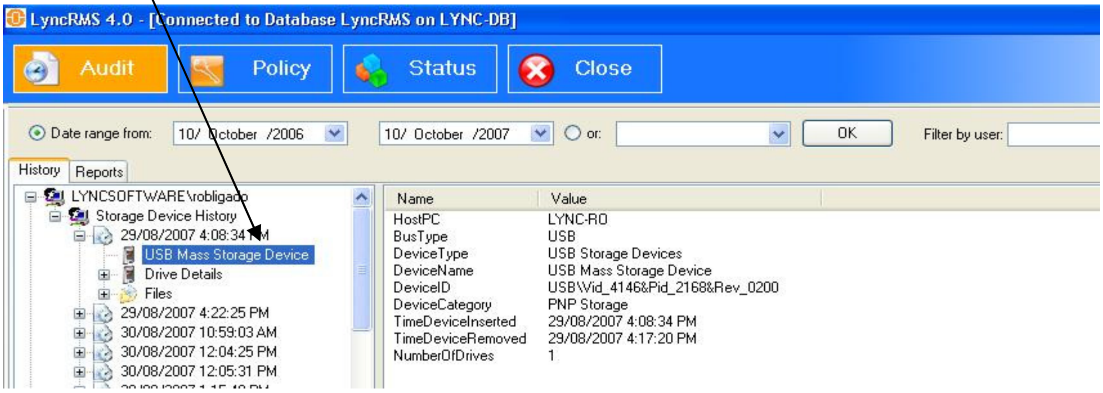
For individual users, the History tree in the Data tab contains details of all devices that have hosted file transfers and the **Volume Number** can be found by inspecting the Drive Details.


LyncRMS 4.0 - [Connected to Database LyncRMS on LYNC-DB]
Audit
Policy
Status
Close
OK
Filter by user:
History
Reports
Storage Device History
29/08/2007 4:08:34 PM
USB Mass Storage Device
Drive Details
IOMEGA UMni128MB*IOM2H4 USB Device (E:)
Files
LYNCSOFTWARE_Administrator_20070824.exe
LYNCSOFTWARE_robligado_20070809.exe
Panel avout cs

● Date range from: 3/ June /2007 11/ October /2007 ○ or:

Label	FileSystem	TotalSpace	FreeSpace	VolumeNumber	TimeVolumeInserted	TimeVolumeRemoved
IOMEGA	FAT32	126988 KB	121404 KB	D2085F19	29/08/2007 4:09:24 PM	29/08/2007 4:17:20 PM

The **Device Name** can also be found in the History tree.



● Date range from: 10/ October /2006 10/ October /2007 ○ or:

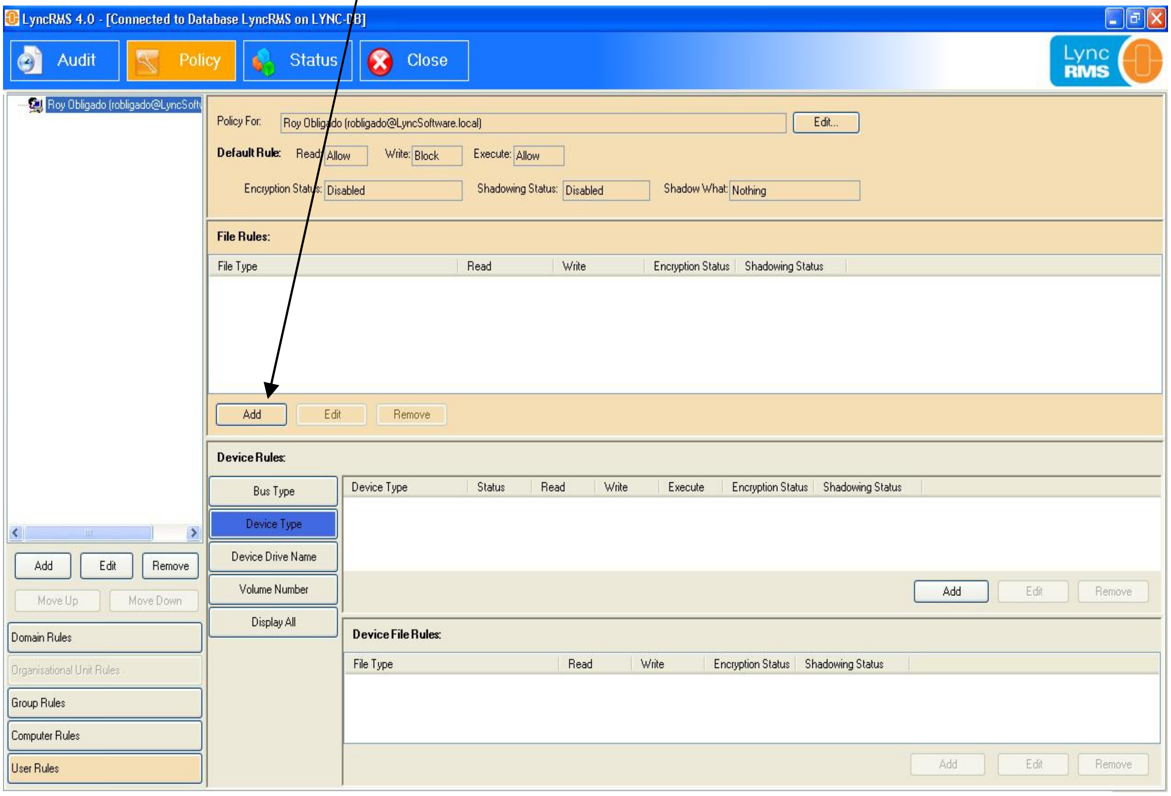
Name	Value
HostPC	LYNC-RO
BusType	USB
DeviceType	USB Storage Devices
DeviceName	USB Mass Storage Device
DeviceID	USB\Vid_4146&Pid_2168&Rev_0200
DeviceCategory	PNP Storage
TimeDeviceInserted	29/08/2007 4:08:34 PM
TimeDeviceRemoved	29/08/2007 4:17:20 PM
NumberOfDrives	1

File Rules

As with Device rules, File rules can be set at Domain level down through to individual Users

For example, if the User default rule is set to Read Allow, Write Allow and Execute Allow, and there are no Device rules implemented, you could block all Microsoft Excel files from being copied to/from any type of removable device, by configuring a File Rule exception for the Domain.

To configure a File Rule click **Add**

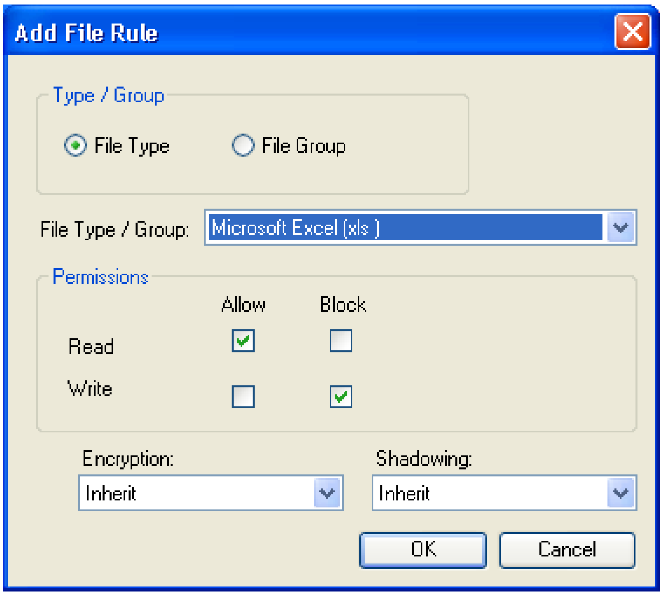


LyncRMS 4.0 - [Connected to Database LyncRMS on LYNC-DB]

Policy For: Roy Obligado (robligado@LyncSoftware.local)

Default Rule: Read: Allow Write: Block Execute: Allow

Encryption Status: Disabled Shadowing Status: Disabled Shadow What: Nothing



Add File Rule

Type / Group: ● File Type ○ File Group

File Type / Group: Microsoft Excel (xls)

Permissions

	Allow	Block
Read	☑	☐
Write	☐	☑

Encryption: Inherit

Shadowing: Inherit

Select the file type and set the Read & Write permissions to **Block**.

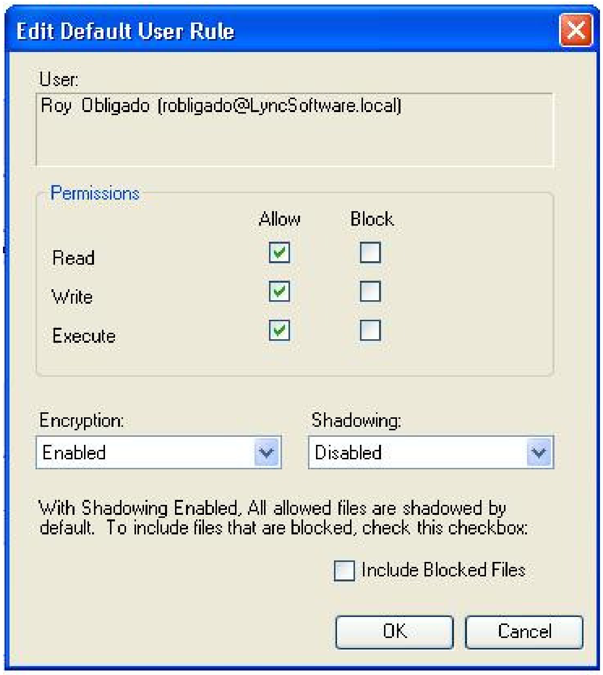
This will prevent any Excel file being copied to/from any device.

File rules can also be extended to include File Groups (Microsoft Office, Images etc) which controls files with the same characteristics.

The file type is determined by inspecting the internal properties, so if the extension is changed, the file is still blocked.

File Encryption

A further level of security has been introduced, which enables you to enforce rules to ensure that all files copied to removable devices are encrypted. As with Device rules, File Encryption rules can be set at Domain level down through to individual Users.


Edit Default User Rule

User:
Roy Obligado (robligado@LyncSoftware.local)

Permissions

	Allow	Block
Read	☑	☐
Write	☑	☐
Execute	☑	☐

Encryption: Enabled

Shadowing: Disabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

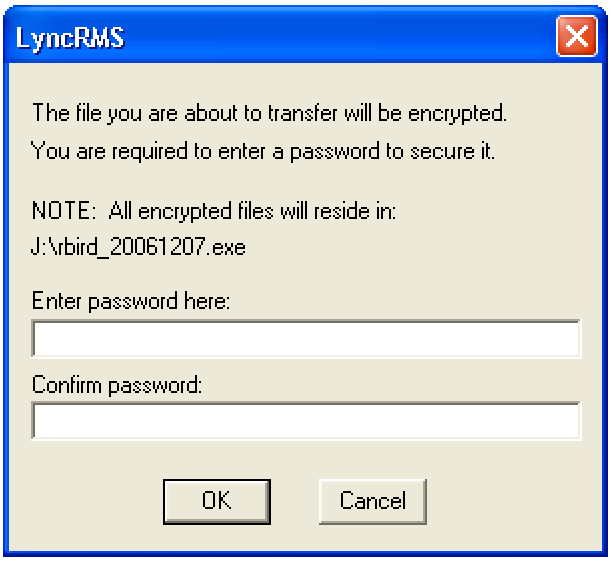
☐ Include Blocked Files

To set an Encryption Rule, open the User Rule admin screen and set **Write = Allow** and **Encryption = Enabled**

Read and Execute permissions do not affect the implementation of an Encryption Rule.

Device Rules and File Rules can also be extended to enforce encryption.

Encryption is enforced on computers with a License Mode = Security + Encryption.


LyncRMS

The file you are about to transfer will be encrypted.

You are required to enter a password to secure it.

NOTE: All encrypted files will reside in:

J:\rbird_20061207.exe

Enter password here:

Confirm password:

When a file is copied to a device, a dialog screen is displayed requesting the user to enter a password.

After entering a password, a secure 'container' will be created, which can only be opened by entering the same password.

If further files are then copied to a device, which already has a container, they will be added automatically, **without** the need to enter a password.

The container has internal properties to recognise the logged-on user, so different people using the same device will have different containers.

The container can be deleted at any time, in which case a new one will be created when a file is copied to the device. As there is no password administration, it is recommended that only **copies of files** are stored in the encrypted container and **NOT originals**. If a user forgets their password, they should delete the container and copy the files again

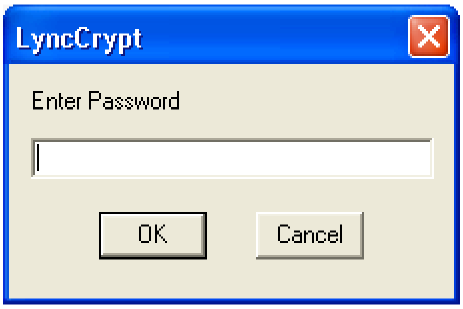
File Encryption ......

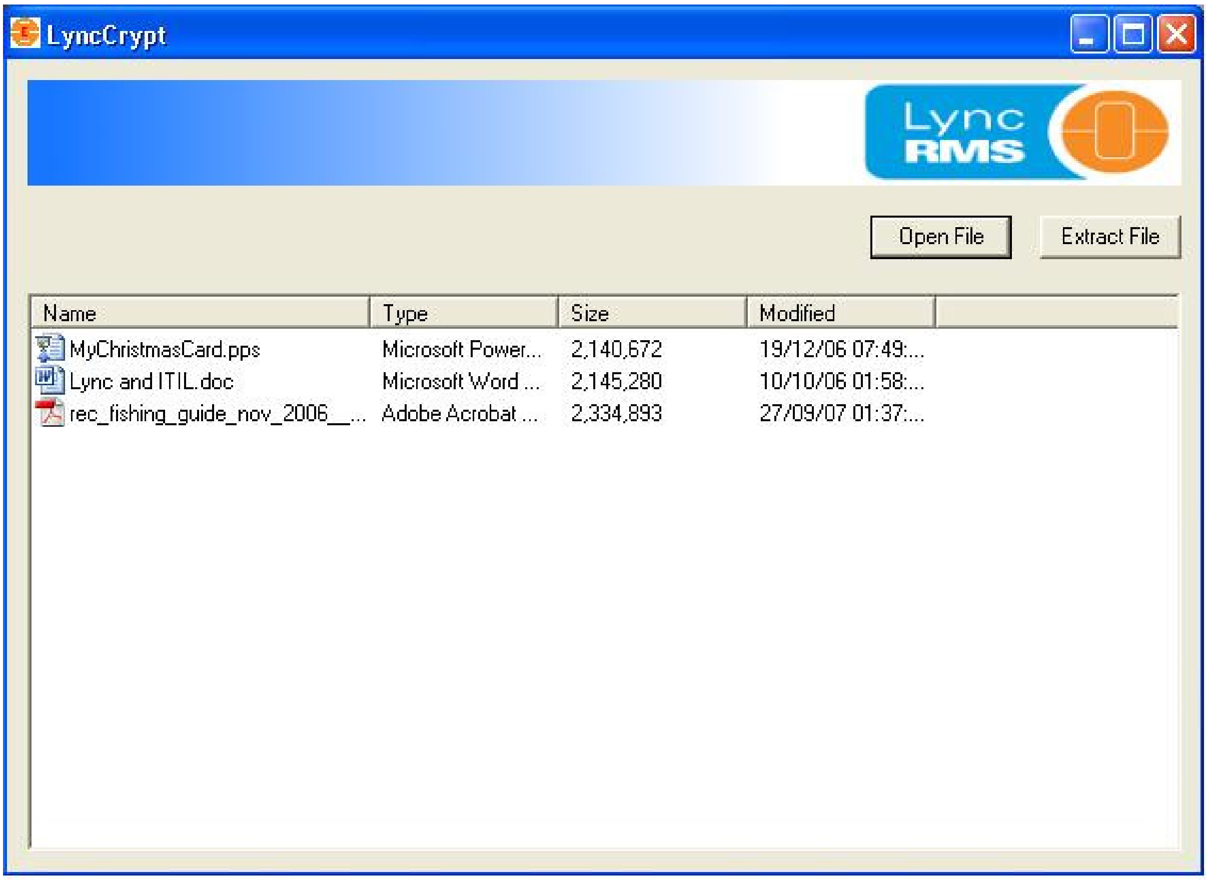
The container will be saved on the device as UserName + DateStamp .exe

IMPORTANT— The container must remain on the device in order to extract the files. If the container is copied from the device to another computer, the files **cannot** be extracted.

The encrypted files are located on the device in a folder called Encrypted_Files, which should not be deleted.

To open the container, double-click on the .exe file and enter the password.



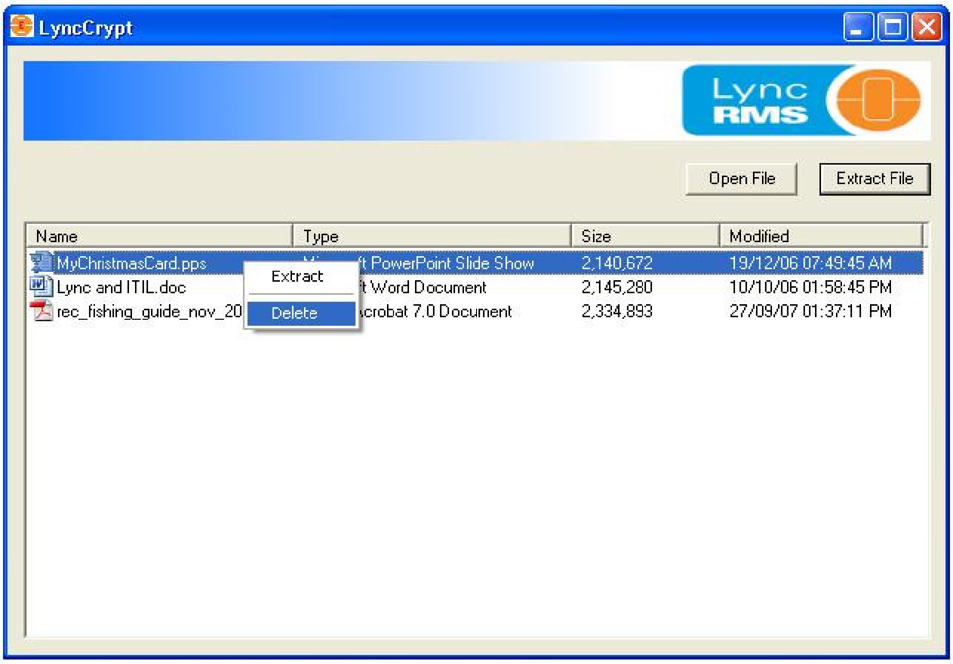


Name	Type	Size	Modified
MyChristmasCard.pps	Microsoft Power...	2,140,672	19/12/06 07:49:...
Lync and ITIL.doc	Microsoft Word ...	2,145,280	10/10/06 01:58:...
rec_fishing_guide_nov_2006_...	Adobe Acrobat ...	2,334,893	27/09/07 01:37:...

To extract a file, highlight the file in the list and click Extract File, which will display a Browse dialog screen to enable you to select a location to save the file. The extraction process will decrypt the file and enable it to be opened using the appropriate application. To view the file without extracting, select the file and click open file, the file will then be displayed using the appropriate editor.

To remove a file from the container, right-click and select Delete

To remove a file from the container, right-click and select Delete



Name	Type	Size	Modified
MyChristmasCard.pps	ft PowerPoint Slide Show	2,140,672	19/12/06 07:49:45 AM
Lync and ITIL.doc	t Word Document	2,145,280	10/10/06 01:58:45 PM
rec_fishing_guide_nov_20	crobat 7.0 Document	2,334,893	27/09/07 01:37:11 PM

Off-line File Encryption

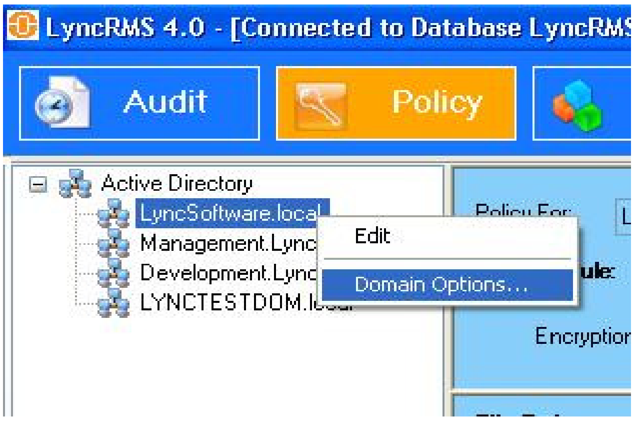
The encrypted container has the capability to encrypt files when the removable device is inserted into a non-secured or non-networked PC. New files can be added or updated simply by dragging and dropping the said files to the container.

NOTE: The policies or rules defined by the System administrators are not applied in off-line encryption.

File Shadowing

Although auditing provides details of the name, type, location etc of files that have been copied to removable devices, there is no indication of the file content that has moved with the file. File Shadowing is a simple form of content monitoring, which can be turned on/off when required to examine the details of specific file transactions.

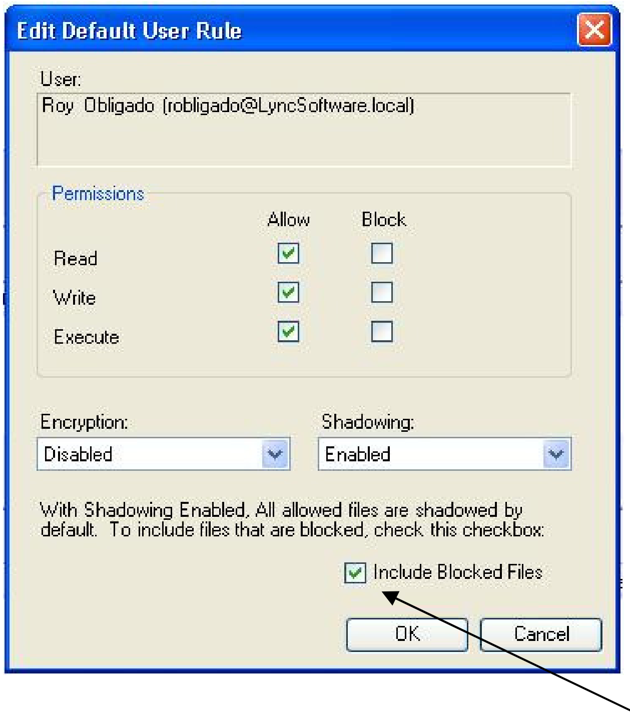
Shadowing is completely 'invisible' to the user and involves automatically taking a copy of the file and storing it in a network location.



The network location is controlled using the **Domain Options**, accessed by right clicking on the selected domain.

When Shadowing takes place, a separate folder for each user is generated automatically.

Also, each 'shadow file' has a date/time stamp appended to the file name, to ensure that multiple copies of the same file are captured.



User:
Roy Obligado (robligado@LyncSoftware.local)

Permissions

	Allow	Block
Read	☑	☐
Write	☑	☐
Execute	☑	☐

Encryption: Disabled

Shadowing: Enabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

☑ Include Blocked Files

To set a Shadowing Rule, open the User Rule admin screen and set **Write = Allow** and **Shadowing = Enabled**

Read and Execute permissions do not affect the implementation of an Shadowing Rule.

Device Rules and File Rules can also be extended to enforce Shadowing.

Shadowing is applied on computers with a License Mode = Security or Security + Encryption.

Shadowing can also be extended to take a copy of files where an attempt was made to copy the file, but was blocked by a rule. To extend Shadowing, check the **Include Blocked Files** check box.

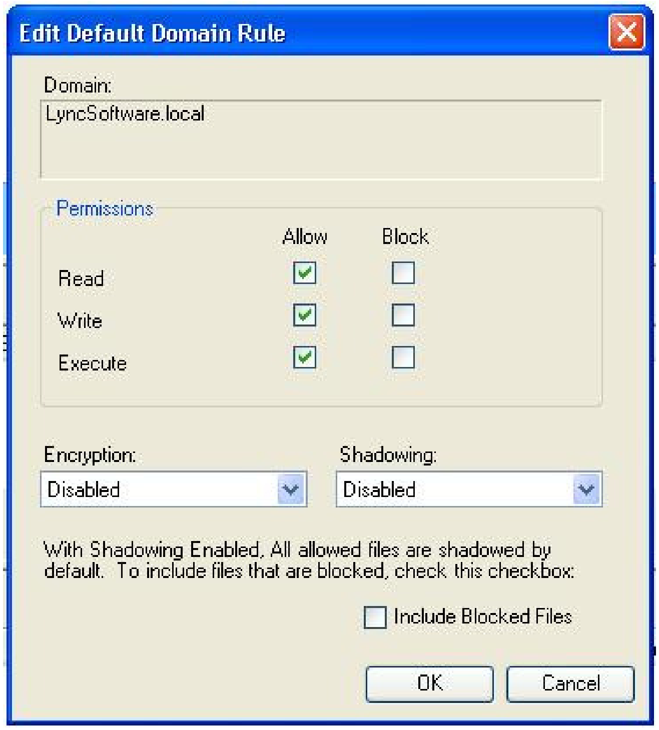
IMPORTANT— Recommend that Shadowing is applied only in limited cases, due to the amount of storage required to accommodate the network files. Files must be deleted/archived manually to reclaim disk space.

How To Create a Black List Environment

A 'Black List' environment is one where **all devices** are permitted to connect and **all file types** are permitted to be copied. Policies are then implemented to handle exceptions.

The main advantage of this type of environment is that policies can be implemented gradually once usage patterns have been established.

To implement this type of environment, the Domain level rule should be set as follows



Edit Default Domain Rule

Domain: LyncSoftware.local

Permissions

	Allow	Block
Read	☑	☐
Write	☑	☐
Execute	☑	☐

Encryption: Disabled

Shadowing: Disabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

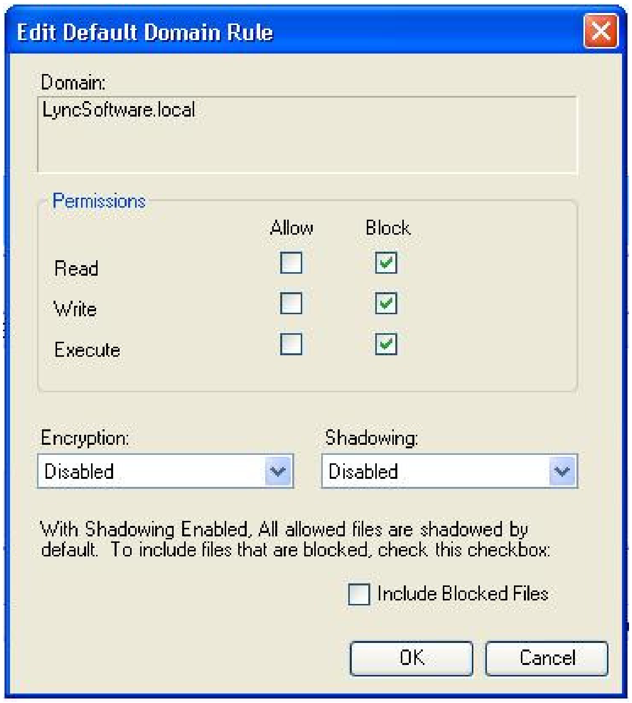
☐ Include Blocked Files

How To Create a White List Environment

A 'White List' environment is one where **all devices** are blocked. Policies are then implemented to allow specific devices to connect and/or specific file types to be copied.

This type of environment will immediately prevent any type of storage device being used, which includes USB devices, Floppy disks and CD ROMs.

To implement this type of environment, the Domain level rule should be set as follows



Domain:
LyncSoftware.local

Permissions

	Allow	Block
Read	☐	☑
Write	☐	☑
Execute	☐	☑

Encryption: Disabled

Shadowing: Disabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

☐ Include Blocked Files

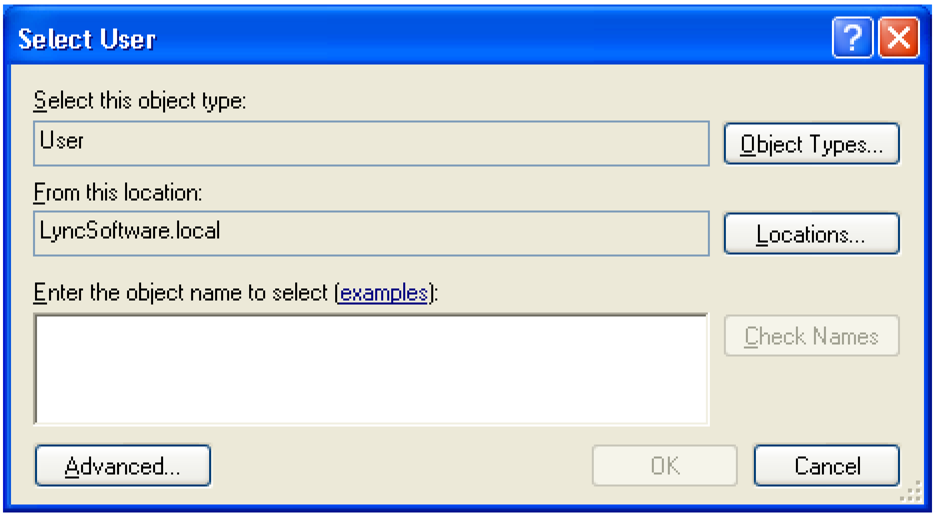
WARNING— This type of rule will block access to all types of removable devices and internal floppy drives and CD-ROM drives.

How To Create a User Rule

A User Policy can be implemented by either using the Policy Wizard or manually using the main Policy screen as follows.

Click User Rules -> click Add

The standard Active Directory dialog box will be displayed



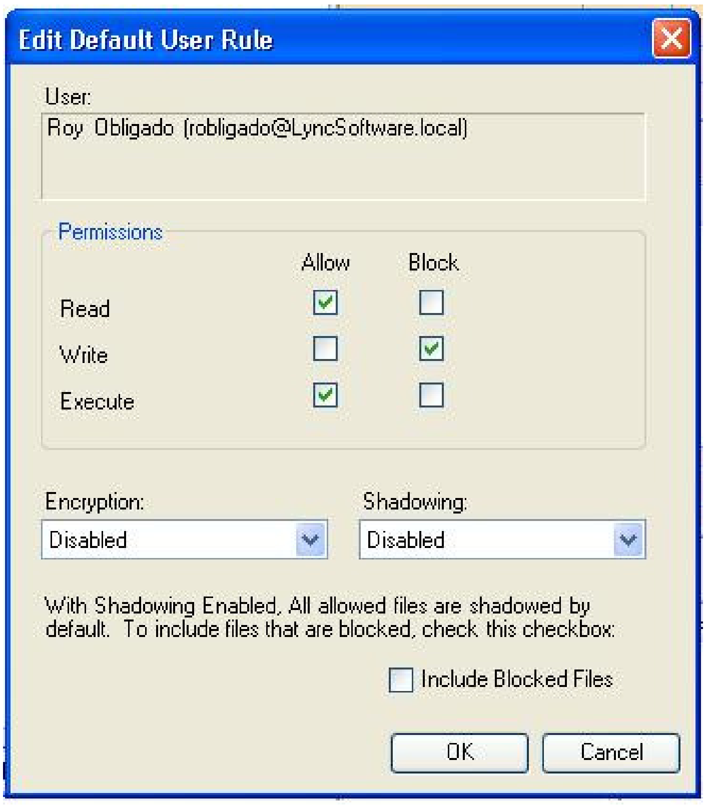
Select this object type: User

From this location: LyncSoftware.local

Enter the object name to select (examples):

Enter the user name or click the Advanced button to perform a search.

After entering/locating a user the following screen will be displayed:



User: Roy Obligado (robligado@LyncSoftware.local)

Permissions

	Allow	Block
Read	☑	☐
Write	☐	☑
Execute	☑	☐

Encryption: Disabled

Shadowing: Disabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

☐ Include Blocked Files

Defaults are set to permit files to be copied from a device (Read)) but blocked from copying to a device (Write)

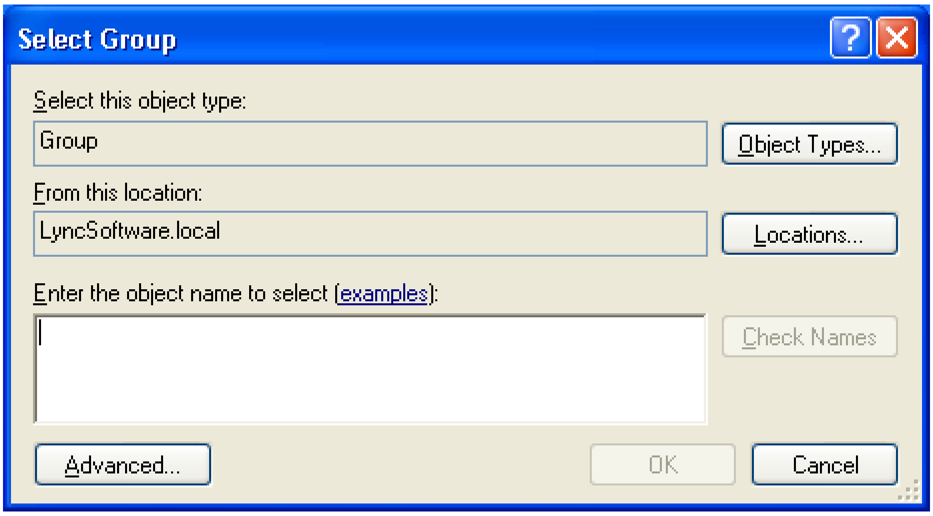
Encryption and Shadowing are also 'turned off' by default.

How To Create a Group Rule

A Group Policy can be implemented by either using the Policy Wizard or manually using the main Policy screen as follows.

Click Group Rules -> click Add

The standard Active Directory dialog box will be displayed



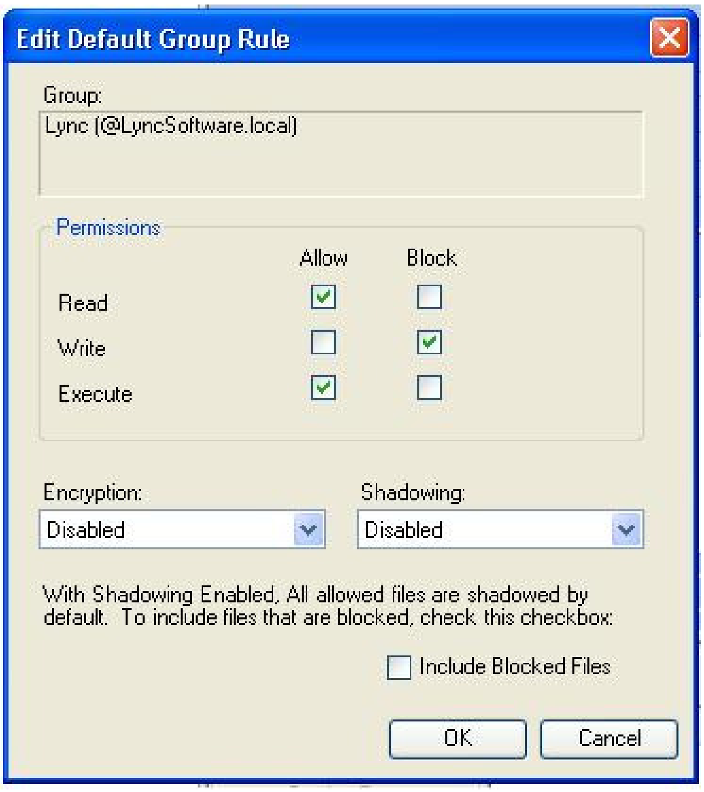
Select this object type:
Group

From this location:
LyncSoftware.local

Enter the object name to select (examples):

Enter the Group name or click the Advanced button to perform a search.

After entering/locating a Group the following screen will be displayed



Group:
Lync (@LyncSoftware.local)

Permissions

	Allow	Block
Read	☑	☐
Write	☐	☑
Execute	☑	☐

Encryption: Disabled

Shadowing: Disabled

With Shadowing Enabled, All allowed files are shadowed by default. To include files that are blocked, check this checkbox:

☐ Include Blocked Files

Defaults are set to permit files to be copied from a device (Read)) but blocked from copying to a device (Write)

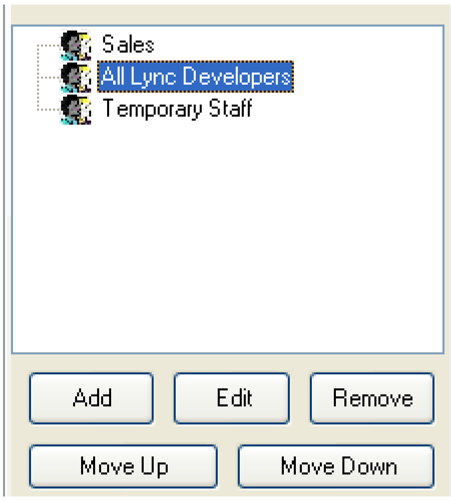
Encryption and Shadowing are also 'turned off' by default.

How To Create a Group Rule …….

If the logged on user belongs to the Group, the rule is enforced.

If there is already a User rule for the logged on user, the User rule takes precedence.

If the User belongs to more than one Group, then rules are enforced upwards through the list of groups for example if the user belongs to both Sales and Temporary Staff, then the Temporary Staff rules will be enforced before Sales.



The order in which Group rules are enforced can be controlled by moving Groups up or down in the list, using the Move Up or Move Down buttons.

How To Block USB Devices

If you want block USB devices from being used, but allow other types of data storage devices including CDROM, floppy disk, SD card etc) then a Device Type Rule must be implemented.

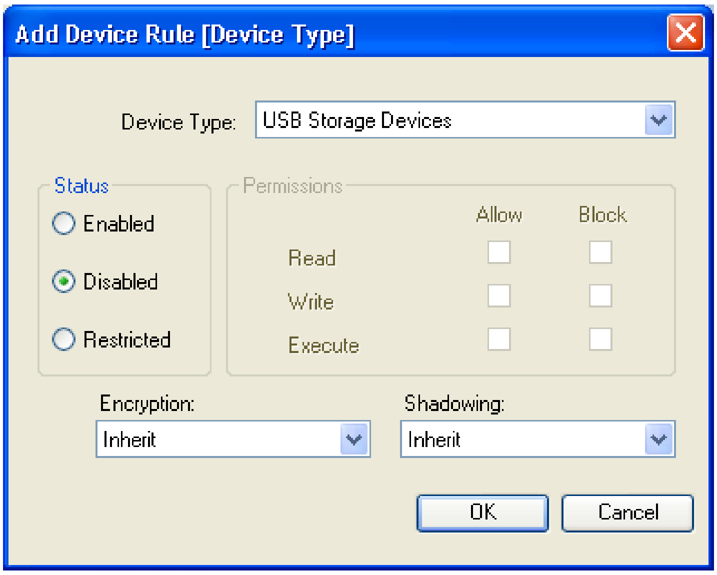
Firstly, you need to determine at which level you want enforce the rule :-

- Domain level
- Active Directory Group level
- Computer level
- User level

At the selected level, you need to set the rule to Read – Allow, Write – Allow, Execute – Allow

Then set a Device Type Rule on the main policy screen as follows

Click Device Type -> Click Add



Add Device Rule [Device Type]

Device Type: USB Storage Devices

Status

○ Enabled

● Disabled

○ Restricted

Permissions	Allow	Block
Read	☐	☐
Write	☐	☐
Execute	☐	☐

Encryption: Inherit

Shadowing: Inherit

Set the Status to **Disabled**, which will then block access to the device type.

How To Block Files Being Copied to USB Devices

If you want block certain File Types from being copied to a device, but allow other File Types then a File Type Rule must be implemented.

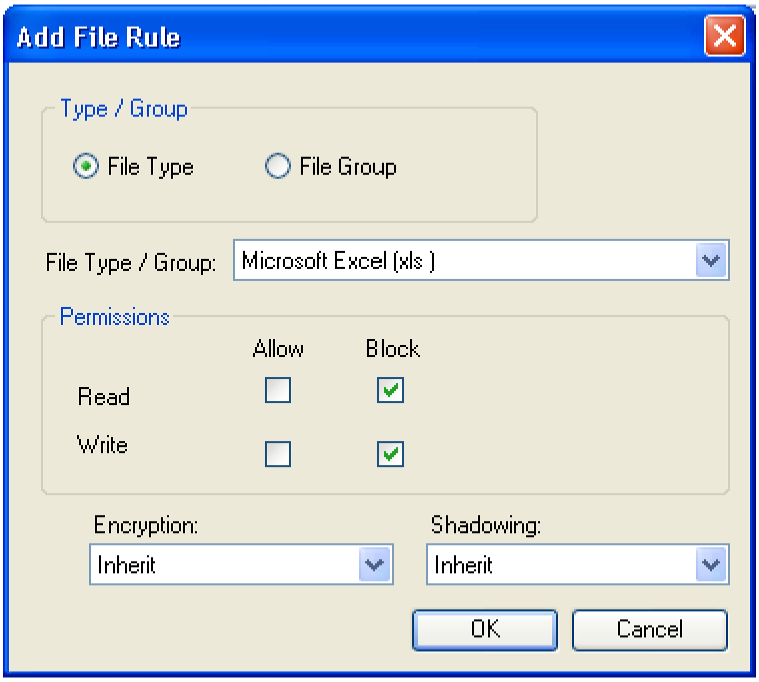
Firstly, you need to determine at which level you want enforce the rule :-

- Domain level
- Active Directory Group level
- Computer level
- User level

At the selected level, you need to set the rule to Read – Allow, Write – Allow, Execute – Allow

Then set a File Type Rule on the main policy screen as follows

In File Rules section Click Add



● File Type ○ File Group

File Type / Group: Microsoft Excel (xls)

Permissions

	Allow	Block
Read	☐	☑
Write	☐	☑

Encryption: Inherit

Shadowing: Inherit

Select the File Type and set Write = Block and Read = Block. This will prevent Excel files from being copied to or from a device.

File Type rules can also be implemented to manage groups of files as follows

Microsoft Office
Images
Audio/Video
Compressed Files (ie Zip)

Individual File Types take precedence over File Groups, so if a rule to block Microsoft Word documents was implemented, with another rule to allow Microsoft Office files, the Word document will be blocked.

Lync Software

http://www.lyncsoftware.com

Australia

15 Bentham Street
Adelaide SA 5000
Australia

Telephone: +61 8 8410 0277
Facsimile: +61 8 8410 1344

United States

1750 Montgomery Street
San Francisco
CA 94111

Telephone: (415) 835 9449
Facsimile: (415) 954 8598