

LFX Database of Managed Objects (DMO)

Copyright (C) CSO Lanifex GmbH

Paul Gillingwater

LFX Database of Managed Objects (DMO)

by Copyright (C) CSO Lanifex GmbH and Paul Gillingwater

This manual is copyrighted and all rights are reserved. It may not be copied, photocopied, translated or reproduced in any electronic or machine-readable form in whole or part without prior written consent from the manufacturer.

In general, the manufacturer will not be liable for any direct, indirect, special, incidental or consequential damages arising from the use or inability to use the product or documentation, even if advised of the possibility of such damages.

The manufacturer retains the right to change the contents of this manual without prior notice in order to improve the function, design, performance, quality or reliability of the product. The author assumes no responsibility for any errors or omissions which may appear in this manual, nor does it make any commitment to update the information contained herein.

Trademarks DMO® is a registered trademark of CSO Lanifex GmbH. Windows® is a registered trademark of Microsoft Corporation. Linux® is a registered trademark of Linus Torvalds. Check Point® is a registered trademark of Check Point Software Technologies Ltd. All other trademarks, products and or product names mentioned herein are for identification purposes only, and may be trademarks and/or registered trademarks of their respective companies or owners.

Revision History

Revision 2.1 24 Nov 2005 Revised by: PG

Added header pages.

Table of Contents

1. Introduction	1
What is the DMO?	1
How is it used?	1
System Requirements	2
DMO Licensing.....	2
Commercial Support.....	3
2. Installation Guide.....	5
Obtaining Installation Media.....	5
Configuring the Servers for Linux	5
Extracting the tar Archive	6
Adding Database Tables.....	6
Configuration Files.....	6
LFX_dbData.php.....	7
LFXlink.php.....	8
LFX_config.....	8
3. Starting and Provisioning the DMO.....	11
Starting DMO.....	11
Changing Administration Password.....	11
Beginning Navigation in the DMO.....	15
Provisioning Data.....	17
4. Definitions and their Attributes	19
What is a Definition?.....	19
What is a regular Attribute?	20
Core and Regular Attributes.....	21
Viewing Definition Details.....	23
Editing a Definition.....	24
Instance List in Definition Details.....	25
Editing Definition Attributes.....	25
5. Instances and their Attributes	27
About Instances	27
Instance Tree.....	27
Instance List	28
Instance Detail	29
Instance Selection	31
Instance Attributes	32
Pluggable Actions	33
6. Creating Reports	35
Selecting Report Objects.....	35
Choosing Report Type.....	35
Report Menu Items	36
7. Searching and Selection	39
Searching within DMO.....	39
Quick Search	39
Configuring Quick Search Attributes	40
Query Search.....	41
Advanced Search.....	41

8. DMO Administration	43
9. Access Controls	45
10. Inheritance	47
11. Modeling Dependencies	49
12. DMO within Event Horizon	51
13. DMO within Policy Compliance Manager.....	53
14. DMO within Crisis Manager.....	55
15. LFXlib	57
16. Customization and Development.....	59
17. DMO and Security Audits	61
18. DMO Operations	63

Chapter 1. Introduction



What is the DMO?

The Database of Managed Objects (DMO) is a software package that was developed by CSO Lanifex GmbH as part of its Security Consulting and Audit practice, in Vienna, Austria. First developed in 2001, the software was provided to customers who needed to build an inventory of all systems, applications and components within their IT infrastructure. Since then, the tool has grown extensively in capabilities, and now offers many features relevant to IT Operations and Security.

DMO provides an object-based view of information, and allows modelling of hierarchical and other non-relational or arbitrary relationships between its data elements. It can also be seen as a database in its own right, although internally it maps all operations to SQL syntax. Thus, it may be described as an Object-Relational layer on top of a traditional SQL RDBMS. For many of its data exchange operations it supports XML syntax, allowing for ease of import or export of information.

DMO deals with three major entities:

- Definitions -- descriptions of objects which might exist within the enterprise
- Instances -- specific objects which exist, i.e., instances of definitions
- Attributes -- defined as potential values for definitions, but become actual values for instances

All Definitions are defined into a single tree structure, with a single root, and each definition has one parent in the tree (which is another definition, the obvious exception being the root definition.) In addition, Instances may be organized into similar trees, however they may also exist without such a hierarchy, and there may be an unlimited number of such Instance Trees.

Definitions, Instances and Attributes are all user-defined, which means the system administrator can add new definitions, or change existing definitions according to their needs. In addition, instances may be associated with attributes which are inherited from their definitions. If a desired attribute does not exist, it may easily be added, and used immediately without reloading the data.

An important feature of the DMO is a comprehensive Access Control system, which means that definitions and instances may be assigned ownership (user and group), and users and groups may have access rights enforced, which can limit a user's view of certain objects, or their ability to change them.

How is it used?

The DMO can be used as a stand-alone application, or can be integrated within other products. For example, CSO Lanifex GmbH has developed two different products which incorporate DMO: the Event Horizon (EH) Security Monitoring system, and the Policy Compliance Manager (PCM), which verifies compliance with security policies such as ISO17799.

Generally, the DMO is used via a Web interface, which requires a standards-based browser, since it needs HTML 2.0, CSS, Javascript and AJAX techniques. It has been tested with Internet Explorer, Mozilla, Firefox, Safari, Opera and Konquerer.

The DMO is also distributed to some Lanifex customers as part of a Linux LiveCD, which may be booted in many PCs. This version is used with the results of our security audits, and is designed to provide read-only access to a large amount of structured data. It can also be used to generate PDF, CSV, HTML or XML reports based on data stored within the DMO.

When used as part of the Lanifex Crisis Manager, DMO operates from a DVD-ROM Live CD, and allows modification of its data to be stored on a USB memory stick, for later integration with the original DMO database which generated the DVD.

Some additional documentation on DMO is available at our Wiki: <http://opt.lanifex.com/cgi-bin/wiki.pl?DMO>

System Requirements

The DMO is written using the PHP language, and stores its information within a MySQL database. It is a Web application, which uses the Apache Web Server, and most often runs under Linux (but will also run under most UNIX systems, including AIX, Solaris and HP-UX.) It also runs under Windows. The Open Source version uses XAMPP as a convenient bundle of these prerequisites, however it will run on other systems with a little work.

The DMO depends on a number of other components, which include the following:

- LFXlib -- the Lanifex Library is an infrastructure library which is bundled within DMO. It provides user and group access management, plus the programming interface and various administration utilities.
- PHP -- the programming language on which DMO is based
- pdflib -- a library for the production of PDF documents. This library is commercially available, and requires a license fee to be paid for commercial use, like DMO.
- MySQL -- a database which is available in both commercial and non-commercial forms.
- Apache -- a Web server.

For ease of installation, we recommend using XAMPP, from Apache Friends, which provides a convenient bundle of the prerequisites that is easy to install and use.

DMO Licensing

The DMO, and its underlying infrastructure library LFXlib, is released as Open Source with a GNU General Public License v2. See <http://www.gnu.org/copyleft/gpl.html> for details of this license. The software remains fully under the Copyright of CSO Lanifex GmbH. We permit non-commercial use of the software without any payment of license fees, however we require any commercial user of the DMO software to pay us a license fee for each implementation, and request any third-party that wishes to sell products based

on the DMO to offer us a fixed percentage (5%) of the fees that they charge for DMO-based products.

As we recognize economic conditions are different in various countries, we use The Economist magazine's "Big Mac Index." Thus, the one-time license fee for DMO is 200 Big Macs, which may be converted based on the local price, as shown in The Economist at the following URL: <http://www.economist.com/markets/Bigmac/Index.cfm>

Note that for customers within the European Union, we are required to add Value Added Tax (VAT), which in Austria consists of 20%. Alternatively, for customers outside Austria we can deduct this Tax if the customer can provide a valid VAT Tax ID on an Order Form.

We are pleased to provide commercial Pro Forma Invoices based on the results of your local Big Mac calculation. (Our Accountants unfortunately prefer hard currency, rather than restaurant hamburgers. We regret that we cannot accept actual hamburgers for the payment of this license fee, nor gift tokens.) Simply send us the amount you have calculated via e-mail, and we will send you a PDF with the Pro Forma invoice, payment for which can then be transferred to our Bank via traditional electronic funds transfer mechanisms.

Commercial Support

The DMO is a fully commercial product, which is used by many customers around the world. As such, we are pleased to offer commercial-grade support, bug fixing and consulting services, based on an annual support contract. Our Support Contract offerings are as follows:

- Silver Support (200 Big Macs): Online access to our commercial Bugzilla tracking system for one year, with guaranteed 48 hour initial response during European working days.
- Gold Support (300 Big Macs): Online access to our commercial Bugzilla tracking system for one year, with guaranteed 24 hour initial response during European working days. Telephone support (up to 20 incidents per year) during European working hours.
- Platinum Support (500 Big Macs): Online access to our commercial Bugzilla tracking system for one year, with guaranteed 12 hour initial response during European working days. Telephone support (up to 50 incidents per year) during European working hours, with extended coverage (12 hours per day, and 7 days per week.)

Notes

1. <http://www.gnu.org/copyleft/gpl.html>
2. <http://www.economist.com/markets/Bigmac/Index.cfm>

Chapter 2. Installation Guide

Obtaining Installation Media

Commercial licensees of DMO will usually receive the installation media as a CD-ROM, which is part of another product, such as Event Horizon or the Policy Compliance Manager. With these products, DMO is automatically bundled and installed when the base product is installed, therefore this section may be skipped.

Open Source users are more likely to download the software, in which case they will receive a file, which may be a compressed tar archive, or an operating-system specific installation package, such as RPM, DEB or PKG. This document will focus on how to install based on the tar archive format. Assuming that this has been downloaded from Sourceforge, or copied from a CD-ROM, the next step is to satisfy the dependencies.

Installing of the required packages to support LAMP (Linux Apache MySQL PHP) applications is not always simple for people who are new to Linux, therefore we found a simple package which combines all of these into one easy installation. We recommend that you visit the Web site www.apachefriends.org/en/xampp.html¹, and download the XAMPP package for your operating system from Apache Friends. This has been tested for Ubuntu, SuSE, RedHat, Mandrake and Debian versions of Linux, as well as with Windows XP. Note that as an open source project, it is possible that some people may wish to develop their own packages for DMO, which support the dependencies of PHP, Apache and MySQL. We certainly encourage such efforts, but cannot support them if they fail.

There are also versions of XAMPP for MacOS X, Solaris and a Windows. Follow the instructions for installation of XAMPP, and continue here when you are complete. Make a careful note of the passwords you use during the installation, as you will need them when configuring DMO. We recommend following the standard installation location of `/opt/lampp/` for XAMPP. (For Windows, use `C:\Program Files\XAMPP`.)

Due to our recommendations on installation locations, it is highly likely that you will need root (Administrator) access rights on the system where you are installing DMO. We do not support users who do not have root access.

Configuring the Servers for Linux

DMO is currently based on PHP4, and will not function with PHP5. Therefore, it is necessary to enable use of PHP4, which can be done for XAMPP using the following command:

```
# /opt/lampp/lampp php4
```

Next, we recommend that the memory available for PHP processes be increased. Edit the file: `/opt/lampp/etc/php.ini`, changing the resource limit for memory from 8 Mb to 32 Mb as follows:

```
memory_limit = 32M      ; Maximum amount of memory a script may consume (8MB)
```

The next change is within the Apache configuration, and is used to configure Apache to ignore the ".php" ending for PHP scripts. This change is made in the file `/opt/lampp/etc/httpd.conf`, and consists of adding the option `MultiViews` in the `Directory` section for `/opt/lampp/htdocs`:

```
Options Indexes FollowSymLinks MultiViews
```

After these changes, it is necessary to restart XAMPP with the following command:

```
# /opt/lampp/lampp restart
```

Extracting the tar Archive

Make a note of the full path where you downloaded the DMO archive. For example, it may be in `/tmp/dmo-2.0beta.tar.gz`. Then extract the archive into your home directory (you can delete it after installation if you wish.) Extract the archive file using this command:

```
# cd /root
# tar xzvf /tmp/dmo-2.0beta.tar.gz
# cd /root/DMO/
```

This will create five folders, inside a directory DMO:

- `dmo_new` -- directory containing the DMO script files
- `LFXlib` -- directory containing the LFXlib script files
- `sql` -- directory containing scripts used to populate the database
- `etc` -- directory containing a file to be installed in `/etc`
- `docs` -- directory containing documentation on the DMO system

In addition, you will find other files, including a README. Please take some time to review that document now, as it contains the release notes and installation instructions, which may have changed since this documentation was written. Now you need to copy files into appropriate locations. The example below assumes you are using XAMPP; if you are not, then you might use a different Web root.

```
# cd /root/DMO
# cp -rv dmo_new/ /opt/lampp/htdocs/
# cp -rv LFXlib/ /opt/lampp/htdocs/
# cp -rv docs/ /opt/lampp/htdocs/
# cp htaccess /opt/lampp/htdocs/.htaccess
# cd /root/DMO/etc
# cp -rv LFX /opt/lampp/etc/
# mkdir /opt/lampp/data
# chown -R nobody.nogroup /opt/lampp/data /opt/lampp/htdocs/
```

Adding Database Tables

The Open Source version of DMO stores important data in the MySQL database. This data needs to be loaded, so that the required tables will be created. Change into the `/opt/lampp/htdocs/sql/` folder, and use the MySQL command line program to load the files. Note that you will require the password you specified earlier for the MySQL database administration.

```
# cd /root/DMO/sql/
# /opt/lampp/bin/mysql -u root -p < dmo_new.sql
Password:
# /opt/lampp/bin/mysql -u root -p < lfxlib.sql
Password:
```

The above commands create two new databases, and pre-load necessary data into tables.

Configuration Files

There are three important configuration files, which may need to be edited. These files are in /opt/lampp/etc/LFX (assuming you copied them as mentioned above.)

- /opt/lampp/etc/LFX/LFX_dbData.php -- edit to change the password(s) used for MySQL access
- /opt/lampp/etc/LFX/LFXlink.php -- edit if necessary to change path to dmo_new
- /opt/lampp/htdocs/LFXlib/LFX_config -- verify this points to /opt/lampp/etc/LFX

Note that the third file, LFX_config, specifies where the first two files should be found. By default, it points to /opt/lampp/etc/LFX, but this may be changed if required.

LFX_dbData.php

This file is used to specify the user names and passwords which should be used to connect to the MySQL database. These should match the user name and password you specified earlier when you installed MySQL as part of the XAMPP package. Typically, the default user name is "root". Assuming you chose the password "secret", the configuration file should be changed as shown below:

```
<?
/**
 * LFX database credentials
 * Bogdan Stancescu<bogdan@lanifex.com>, May 2002
 *
 * Contains sensitive information
 * $Id: DMO_UserGuide.xml,v 1.21 2005/11/28 21:09:48 paul Exp $
 */

$_LFX['global']['dbData']=array (
  'LFX' =>
  array (
    'host' => 'localhost',
    'db' => 'lfxlib',
    'uname' => 'root',
    'pwd' => 'secret',
  ),
  'dmo_new' =>
  array (
    'host' => 'localhost',
    'db' => 'dmo_new',
    'uname' => 'root',
    'pwd' => 'secret',
  ),
  'mysql' =>
  array (
    'host' => 'localhost',
    'db' => 'mysql',
    'uname' => 'root',
    'pwd' => 'secret',
  ),
);
$_LFX_dbData=&$_LFX['global']['dbData'];
?>
```

Note that the above file uses the same credentials for each database, however best practice means keeping these separate, and creating a different user for each database. In any case, because the file contains sensitive information, it should

be restricted using the Linux "chmod" command, so that only the Web server has permission to read it. This is usually done with the following commands, assuming that Apache is configured to run as user nobody:

```
# cd /opt/lampp/etc/  
# chmod -R 700 LFX  
# chown -R nobody.nogroup LFX
```

Note that it is possible to run an external MySQL server, by replacing "localhost" with the fully qualified domain name of the Database server.

LFXlink.php

This script defines which additional applications are installed with DMO. Normally, the standard installation of DMO does not require changes to this file. However, whenever DMO is installed with other applications, such as Event Horizon, Policy Compliance Manager, Help Desk, Crisis Manager, etc., this file should be updated to reflect each installed application. For DMO, it may be necessary to change the path which tells LFXlib where to find DMO in the file system.

```
<?  
/**  
 * The Lanifex link  
 * Bogdan Stancescu <bogdan@lanifex.com>, November 2002  
 * $Id: DMO_UserGuide.xml,v 1.21 2005/11/28 21:09:48 paul Exp $  
 */  
  
/**  
 * This file links the LFX_lib with all the other LFX  
 * applications on this server.  
 */  
  
$_LFX['global']['applications']=array (  
    'LFX' =>  
        array (  
            'app_code' => 'LFX',  
            'app_name' => 'LFX Library',  
            'app_url' => '/LFXlib',  
            'app_dbdata' => 'LFX',  
            'app_ver' => '1.0',  
        ),  
    'DMO' =>  
        array (  
            'app_code' => 'DMO',  
            'app_name' => 'Database of Managed Objects',  
            'app_url' => '/dmo_new',  
            'app_lib' => '/opt/lampp/htdocs/dmo_new/include/DMO_lib.php',  
            'app_dbdata' => 'dmo_new',  
            'app_ver' => '1.0',  
        ),  
);  
?>
```

LFX_config

This file should be found in /opt/lampp/htdocs/LFXlib/LFX_config. It contains a single line, which points to the location of the previous two files, as shown in the example below:

```
systemdir=/opt/lampp/etc/LFX
```

Notes

1. <http://www.apachefriends.org/en/xampp.html>

Chapter 3. Starting and Provisioning the DMO

Starting DMO

Assuming that installation is completed, DMO may be started by using the Web interface. Begin a Web browser on your system, and point it to the following URL:

`http://localhost/dmo_new/`

Note that the host name may be different, if you have installed the Web server on a machine different than your Web browser. If this is the case, you should verify that XAMPP is also reachable from the external interface. If all is well, you should see something like the following screen shot:



Note the very first time you login to DMO, it should be with user "admin", and password "secret". It is essential that you change this password as soon as possible.

Changing Administration Password

We strongly recommend that the password for the "admin" user be changed as soon as possible. This is done using LFXlib, which is accessed with the same credentials. The URL for LFXlib is:

`http://localhost/LFXlib/`

Note that if you have already logged in to DMO, you will not see the following LFXlib login screen:



Please identify yourself with a username and a password

Username:


Password:

Language: English

[Login now](#)

CSO Lanifex Website Contact Administrator Support

After logging in to the LFXlib, you will see the following screen:


LFXlib
 The CSO Lanifex Generic PHP Library

System and Configuration ▾
 Development and Audit ▾
 Applications ▾
 Change Password
 Log Out


Access Manager ▾
 Subscriptions ▾
 Translations ▾
 Globals ▾
 Reporting
 Report Settings ▾
 Document Types ▾
 Calendar
 SQL Operations ▾
 LFXlib Backup
 Synchronization ▾

Main Page

LFXlib Modules	LFXlib Applications
System and Configuration	Event Horizon
Document Types Management	Database of Managed Objects
Calendar	Outreach Project Tool
SQL Diff Tool	HelpDesk
SQL Structure Dump	
LFXlib backup	
Package Creation Manager	
Upgrade Manager	
Synchronization	
Development and Audit	
Class Consistency Checker	
Groups Cycles Check	
SC Data Dumper	
Email Sender	
Debug Level Settings	
PHP Information	
Audit Log	
Message Log	
LFXlib Feature Demonstrations	
Log out of LFXlib and all modules	

The menu item "System Configuration" contains the item "Access Manager", which

contains the sub-item "Users." This item is also available as a link from the Main Page. Choosing the "//System Configuration//Access Manager//Users" will produce the following screen:


LFXlib
The CSO Lanifex Generic PHP Library


System and Configuration ▾
Development and Audit ▾
Applications ▾
Change Password
Log Out

Users List

Members				
Users				
Groups				
Miscellaneous				
My User's Details				
Import Groups From XML				
Synchronize groups with external export				

Users List				
Show deactivated <input type="checkbox"/> Total 15 items Show 20 per page				
ID	First Name	Last Name	E-mail	Date Created
6	EH	Admin	admin	Jan 1, 2004
9	Andrei	Tinca	andrei@lanifex.com	Jan 1, 2004
10	Oliver	Van Assche	oliver@lanifex.com	Jan 1, 2004
12	Paul	Gillingwater	paul@lanifex.com	Jan 1, 2004
13	Bogdan	Stancescu	bogdan@lanifex.com	Jan 1, 2004
14	Andreas	Floriani	andreas.floriani@oenb.at	Jan 1, 2004
16	Dieter	Herndlhofer	dieter@lanifex.com	Jan 1, 2004
23	Matthias	Wolfframm	matthias@lanifex.com	Jan 1, 2004
28	bogdan	[n/a]	bogdan@moongate.ro	Mar 24 13:40
29	HelpDesk requestor	(temp)		Mar 24 14:06
30	harvester	subsystem		Apr 8 16:53
31	Michael	Krausz	mkrausz@coltcust.at	May 9 9:51
32	Peter	Perdich	peter@lanifex.com	May 27 11:55
33	Demo	User	root@lanifex.com	Jun 7 15:16
34	Olivier	Van Assche		Jun 28 14:16
Show deactivated <input type="checkbox"/> Total 15 items Show 20 per page				




Within the Users List, there is a link that says "My User's Details". Click on that link, and you should see the following screen:



LFXlib
The CSO Lanifex Generic PHP Library

System and Configuration ▾
Development and Audit ▾
Applications ▾
Change Password
Log Out


User EH Admin details

Members
[Users](#)
[Groups](#)
Miscellaneous
[My User's Details](#)
[Import Groups From XML](#)
[Synchronize groups with external export](#)






User Details


Name	EH Admin
Position	Administrator
Company	1
E-Mail	admin
Address	
Mobile Phone	
Work Phone	
Fax	
Home Phone	
Preferred Language	English
Notes	

List of groups in which this user is a member


Super Users	This is the Super Users group.	RW	Active
-----------------------------	--------------------------------	--------------------	--------


Associated Files

Submit new file

Title	<input type="text"/>
File	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>

This screen shows the information for the currently logged-in user. Note the icons in the upper left part of the information panel. Click on the red pencil (✎) icon to edit this information, and the following image will appear:

LFXlib The CSO Lanifex Generic PHP Library	
System and Configuration ▼	Development and Audit ▼ Applications ▼ Change Password Log Out

Edit user details

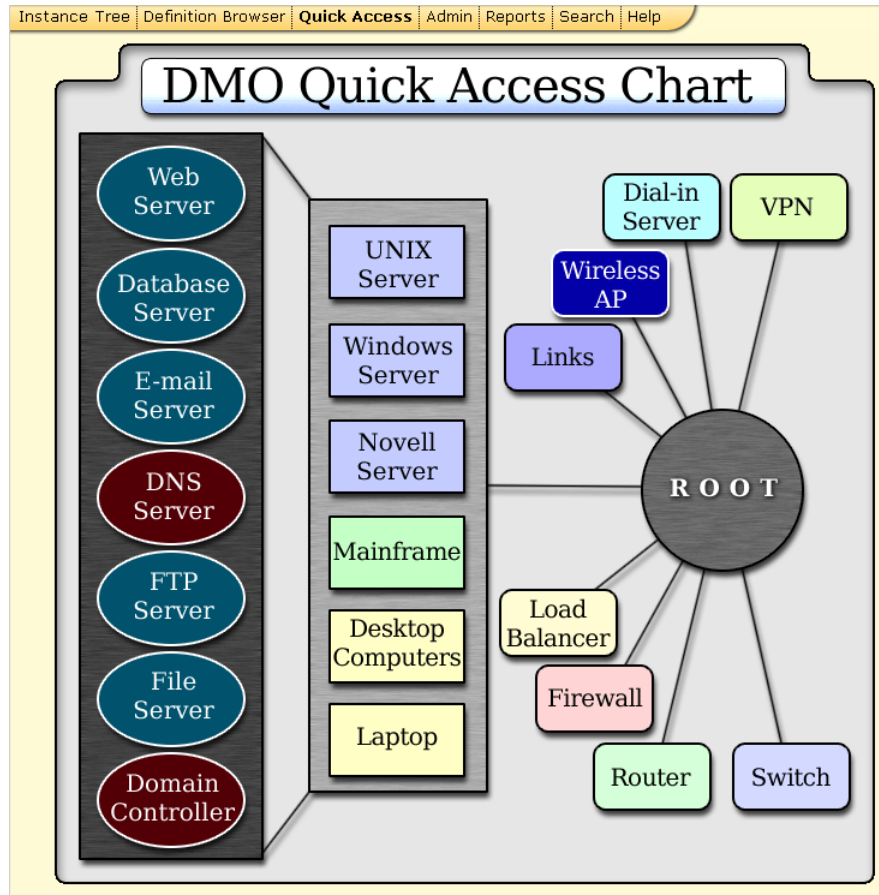
Members	User Details
Users	Salutation <input type="text"/>
Groups	First Name <input type="text" value="EH"/>
Miscellaneous	Middle Name <input type="text"/>
My User's Details	Last Name <input type="text" value="Admin"/>
Import Groups From XML	Position <input type="text" value="Administrator"/>
Synchronize groups with external export	Company <input type="text" value="1"/>
	E-Mail <input type="text" value="admin"/>
	Address <input type="text"/>
	Mobile Phone <input type="text"/>
	Work Phone <input type="text"/>
	Fax <input type="text"/>
	Home Phone <input type="text"/>
	Preferred Language <input type="text" value="English"/>
	Notes <input type="text"/>
	Username <input type="text" value="admin"/>
	Password <input type="text"/>
	Re-enter password <input type="text"/>
	<input type="button" value="Save User"/>

Enter your password twice at the end of this form, then click "Save User." It may be necessary to login again with the new password if you time-out from a session.

Further users may be added if you have administration rights, and these users should also have access to the DMO, depending on the access controls you have defined and the groups of which they are members. See Chapter 9 for more details on Access Controls.

Beginning Navigation in the DMO

Immediately after logging in to the DMO, one of two possible screens may appear, depending on how the DMO data has been provided. The first option assumes that no Location Definition has been instantiated, and the global option controlling this feature is disabled. It begins with the "Quick Access" screen, which appears as follows:



At the top of the browser window appears a menu bar, which includes the following choices:

- Instance Tree -- shows a tree of instances, based on the first Location, if available. Note that Instance Trees may not exist within the DMO data on your system.
- Definition Browser -- shows the single tree of Definitions, which exists in every DMO database, plus a view of the currently selected definition.
- Quick Access -- returns to the above graphic navigation image. Note this is a clickable image map, which will navigate to the Definition matching each name on the image.
- Admin -- the DMO Administration menus.
- Reports -- access to the DMO Report subsystem
- Search -- access to the complex Search facility
- Help -- access to online Help for DMO

The DMO Quick Access Chart is a convenient navigation tool for quickly selecting popular Definitions. This uses an image map, so that clicking on any of the Definition names will open the Definition List view. The ROOT object represents the root of the Definition Tree, which means the parent definition for all other objects. See the Definitions Section for more details on Definitions.

The second option that may appear when starting DMO is an Instance Tree. This will appear under two conditions:

1. There should be an instance of the Location Definition. The first one will be chosen.

2. The LFX Global "start_with_location" should be set to a value of 1 in the LFXlib Globals Management

If both conditions are met, a display similar to the following will be shown:

The screenshot shows the LFXlib Instance Tree interface. The top navigation bar includes 'Instance Tree', 'Definition Browser', 'Quick Access', 'Admin', 'Reports', 'Search', and 'Help'. The main content area is titled 'Location' and displays 'Vienna, Austria'. Below this, a tree structure shows the following items:

- Location : Vienna, Austria
 - Branch Office : Lanifex Office
 - Branch Office : Bartexim Office
 - Subnet : Subnet Test Eddie

On the left side, there are several search and selection panels:

- Quick Search:** Includes a search bar, a 'Go' button, and radio buttons for 'Definitions' (selected), 'Instances', '[By owner]', and '[By attribute]'.
- Query Search:** Includes a dropdown menu labeled '[select query]'.
- Advanced Search:** Includes a dropdown menu labeled '[select search]'.
- Instance Selection:** Includes buttons for 'Add Instance to Selection', 'Clear Selection', and 'View Selection'.

Note that this same display can be accessed by clicking on the menu at the top labelled "Instance Tree."

Please refer to the Chapter on Instances and their Attributes, for information about navigation through the instance trees.

Provisioning Data

This section describes how you should plan to provision data into the DMO. It's a good idea to understand the concepts of Object Design, and think about how you wish to model your data within the system, as there are many possible ways to do this--some of which can cause problems later.

Normally, users will explore the Definitions tree, and look for the names of Definitions that match information they already know about. For example, if an organisation wishes to create an inventory of all of its laptops, it will look for a definition called "Laptop", which already exists. There are over 200 definitions provided as standard with DMO, and more may be added if required.

Four approaches may now be used, which are described in more detail now:

1. Create Instance manually -- within the Definition, click on the green cube icon (🟩) to create a new instance. This will open a form, into which details for the Instance (i.e., a new Laptop) may be added. This process is slow, as it requires a form to be filled out for every item.
2. Create multiple new instances -- within the Definition, click on the cluster of green cubes (🟩🟩🟩). This opens up a form wherein it's a little easy to create multiple new instances, and easily copy information between them.
3. Import Wizard -- the Admin//Import Wizard menu item allows for the importing of an unlimited number of instances of a single Definition using a Comma Separated Value (CSV) file as input. This file might be exported from another database, or saved from an Excel file. See Chapter 8 for more details on the Import Wizard.
4. Automated Scanning -- this is the best and fastest technique for collecting large amounts of data. It involves using an external scanning tool (NMAP) to connect to the LAN, and determine the IP addresses of thousands of host computers and other network-connected devices. Note that this feature is only

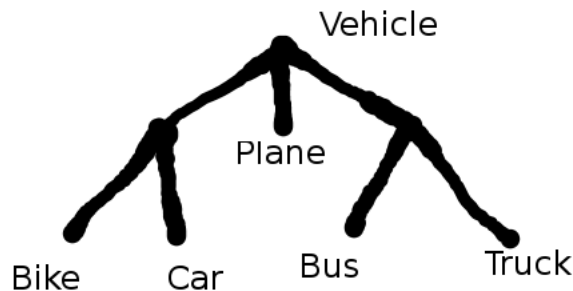
available as part of the Event Horizon Security Monitoring system, which is described in more detail in the Event Horizon Chapter.

A fifth method, involving integration with existing Inventory or Asset Management systems, is available as part of a consulting solution directly from CSO Lanifex GmbH. This would allow on-line periodic automated update of inventory items into the DMO, with synchronization of key data. We also support migration from existing inventory databases, which many customers decide to replace with DMO.

Chapter 4. Definitions and their Attributes

What is a Definition?

Within the DMO, a Definition is an Object's generic description, that is sufficiently specific as to distinguish it from an object of a different type. Generic means we are talking about classes of objects, rather than individual instances of the objects themselves. For example, a Definition might be "Vehicle", while a specific instance of a vehicle might be "Nissan 350Z, Blue, Chassis #34545755531". Reflecting on this definition however shows that it might not be sufficiently specific, if we have different types of vehicles. For example, we might need to distinguish between "Car", "Truck", "Bus", "Plane" and "Other." All of these are types of vehicles, but each is clearly of a different type. In that context, we are actually building a tree of definitions, where each more specific type constrains the class of objects which belong under that part of the tree.



The tree above shows one way to look at a hierarchy of definitions, but of course there are many others, and one of the design goals of DMO was to be totally flexible. Although we provide a set of more than 200 definitions by default, the user may completely replace them with their own tree design, which should map onto the real-world application they wish to solve. If you do make a definition, you need to keep in mind the following simple rules:

- Each Definition must have a unique name. Spaces may be used, but avoid punctuation or special characters (especially the "/" must not be used.)
- Every Definition should fit into a logical place in the hierarchy. If you can't find the right place, then create a new second-level category.
- The Definition tree has a single root, which is usually the name of the organisation which owns the tree.
- Every definition (with the exception of the root) MUST have a single parent definition. This defines its place in the tree. Note that it is possible to move definitions from one part of the tree to another, by changing its parent. (Beware that certain assumptions are made by Event Horizon and Policy Compliance Manager which may be broken if this is done, so take care. If in doubt, ask Lanifex.)
- One definition cannot exist in two different parts of the tree at the same time. If they share common characteristics, think about reorganising the tree to make them both part of the same branch.

For each definition you create, think about whether it is really the abstraction you are dealing with, or a specific instance. It's also possible to go too far in splitting things into types and categories -- for example, you might have a definition for "Cars", and then decide to make several sub-definitions such as "Sports Car", "Wagon", "SUV", "Coupe", etc. Instead, a better approach may be to simply have one definition, "Car", and then use an attribute called "Type" which can distinguish better between them.

What is a regular Attribute?

An Attribute is some descriptive property of a Definition. It differs from Core Attributes, which are described in the next section. For example, when talking about the definition "Car", we might have several properties which can be recorded, including "Colour", "Size", "Horsepower", "Engine Displacement", "Owners", etc. Within the DMO, the most common attribute is a small piece of text (typically not larger than 250 characters in length), however there are many possible data types of attributes, which are listed below:

Table 4-1. Table of Definition Attribute Data Types

Attribute Type	Description
Text Line	This can be a single line of text, in any language. Typically no more than 250 characters in length.
Boolean	This requires a choice between True and False.
Large Text	This is a text area, which might have up to 65,000 characters in length. Of particular interest is the fact that multiple versions of this may exist, in different languages, for the same attribute.
File	For large documents, images or virtually any type of file, this attribute allows a file attachment to be assigned to a definition. Multiple files may be attached, but only if each attribute has a different name (see basic rules below.)
Instance	This is a powerful feature of the DMO, which allows any single instance to be made into an attribute for any other instance (except itself.)
User	Any person information stored in the LFXlib may be selected as an attribute for an instance.
Group	Any group information stored in the LFXlib may be selected as an attribute for an instance.
Select	This attribute allows selection from among a limited set of choices, which are presented in a pull-down list.
URL Link	The attribute will be treated as a URI, which allows selection of any Web page or other Internet-related media selector.
Helpdesk Escalation Preset	This is a specialized attribute which only applies when DMO is used with the LFX Process Desk, to specify what escalation preset should be used to apply to incidents that are created based on an object instance with this attribute.

There are several basic rules about Attributes which must be observed:

- Each attribute must have a name. Attribute names must be unique. Like defini-

tions, avoid special characters. While it is not essential to avoid a conflict between Definition and Attribute names, we recommend this anyway, to avoid confusion in the minds of users.

- If an attribute is shared between two or more different definitions, it must be assigned to the lowest definition which is superior to all of the others, i.e., which is above all the definitions in the tree which need to use that attribute.
- When an attribute is defined for a definition, it will be automatically inherited as an available attribute for all definitions below it in the tree. Note this does not mean the value of the attribute will be copied -- instead, it means that the attribute may have a value assigned.
- Attributes may not be repeated. This means that an attribute **MUST** be unique for that definition, and cannot be instantiated more than once within that instance. For example, "IP Address" is an attribute which could be repeated, however it means that the definition is incorrect -- instead of assigning an "IP Address" attribute to a multi-homed host, one should create a new definition called "Network Interface", each of which has one IP Address -- and the multi-homed host becomes then a parent instance for a set of logical or physical network interfaces.

Attributes themselves may have some options, besides their type. These options are:

Table 4-2. Attribute Options

Option	Description
Visible	This defines whether the attribute will be shown in forms which are presented to the user. Some attributes are for internal or program use only, and do not need to be displayed.
Is Password	When presented in a form, the contents of this attribute will be masked from the user. This is typically required for passwords, community strings or other sensitive information. Note that in the underlying database, this information is not hashed or otherwise encoded; this option only applies to the presentation layer.
Revision	This is a simple number which is incremented each time the attribute is changed.
Inheritable	This is NOT related to the inheritance of attributes by one definition from its parent definition. Instead, it means that whenever this attribute is assigned a value, it will be copied (both the attribute AND the value) to all of the Instances that exist as child instances of the current instance. This is typically used for attributes such as Security Classification.
Description	This is text which appears whenever an attribute is to be added or changed, as a guide to the user.

Core and Regular Attributes

There are two types of Attributes associated with Definitions and Instances. Core attributes are available for all definitions of every type, and are fixed by the DMO system (i.e., their type cannot be changed.) They include the following:

Table 4-3. Table of Core Attributes

Core Attribute Name	Description
Definition Name	This is the unique name for the definition. This is one of the two core attributes which are mandatory.
Child Of	This specifies the location of the definition within the Definition Tree, by indicating the parent definition. This is the other mandatory core attribute.
Revision	This is a revision number, which is incremented each time the definition is changed.
Number	This is a unique number used to identify the definition. By default, we use a variation of ASN.1 numbering, which identifies each node in the definition tree according to its relative place in the tree, starting from the second level definitions. For example, a LAN is 1.2.1.
Description	The description of the definition. Not required, but certainly recommended.
Lock Inheritance	This is a check box, which defines whether instances for this definition and their child instances will inherit so-called "inheritable attributes." See the Chapter on inheritance for more details.
Owner	A select box showing the list of persons who might own this definition -- this actually functions as a default, so that when instances are created, they inherit this owner information from the definition.
Group	A select box showing the list of groups who might own this definition -- this actually functions as a default, so that when instances are created, they inherit this group information from the definition.
Type	A general way of classifying definitions (now obsolete, but retained for backwards compatibility.) New types may be added --- this is usually selected from second-level definitions.
Hidden	This core attribute defines whether the definition will be hidden. Rather than deleting a definition from the tree if it is not being used, it is better to mark it as hidden, so it doesn't confuse users.

Core Attribute Name	Description

Regular Attributes are different from core attributes, in that their type, name and availability may be changed by the systems administrator. See the previous section on regular Attributes for more details.

Viewing Definition Details

Definitions are usually navigated in the form of a tree. Click on the menu "Definition Browser", or the ROOT object from the Quick Access, and a display similar to this will be shown:

The screenshot displays the 'Definition Browser' window. On the left is the 'Definition Tree' showing a hierarchy of definitions under 'CSO Lanifex System'. The tree includes categories like Application, Asset, Business Process, COBIT Processes, Dependency, Infrastructure Object, ITIL Process, Location, Network Object, Link, MIB, Node, Firewall, Host, NIC Interface, Probe, Alarm Ruleset, RMON, Sensor, Router, Switch, Unknown, Services, Subnet, VLAN, Policy Object, Processes, Responsibility, Risk, Security Classification, and Unassigned. Each node shows instance counts. The right pane shows 'Definition Details' for the selected 'CSO Lanifex System' definition. It includes a 'Core Attributes' table with fields like Revision (1.0), Number, Description, Lock Inheritance (No), Owner (EH Admin), Group (default), Type (Administrative), and Hidden (No). Below this are tabs for 'Child Definitions', 'List of Attributes', and 'List of Instances'. The 'Child Definitions' tab is active, showing a list of child definitions with their descriptions. At the bottom, there is a 'Quick Search' bar and a 'Definitions' section.






Core Attributes	
Revision	1.0
Number	
Description	This is the parent object for all other objects.
Lock Inheritance	No
Owner	EH Admin (admin)
Group	default [0]
Type	Administrative
Hidden	No

Child Definitions of CSO Lanifex System	
Application	All software systems and applications are defined by this object.
Asset	This is some type of Asset used as part of a Risk Assessment. Assets will be as
Business Process	This definition is used to describe the Business Services which are supported by network services and infrastructure objects defined within the DMO. This is the
COBIT Processes	This hierarchy of definitions is used to document the COBIT processes within th
Dependency	This is a special class of definition that is used to model a detailed dependency
Infrastructure Object	This object includes all parts of the infrastructure which are not computer-relat
ITIL Process	ITIL is the Information Technology Infrastructure Library. Two of its 40 volumes Delivery.
Location	The physical location of some object. This is usually a building of some type.
Network Object	All objects within the network are defined underneath this object
Policy Object	This definition and its children define the various Security Policies which are imp
Processes	All network and system-related processes that must be managed are defined he
Responsibility	Wer ist fuer etwas verantwortlich Who is responsible for the thing.
Risk	Risk relating to Information Security.
Security Classification	This definition is used to classify information assets according to their security
Unassigned	Objects which are unknown or otherwise unassigned will be placed here.

This display is complex, and has many elements, which we will review below.


- Definition Tree -- this is the swatch to the left of the screen, which shows a tree structure consisting of all definitions. This tree may be navigated by clicking on any of the definition names. Parts of the tree may be opened or closed by clicking on the plus or minus sign to its left. The definition tree includes counts of the number of instances associated with each node. There are two numbers: the first shows the number of instances of the currently selected definition, while the second shows the number of instances of all its child definitions. Note that the currently selected

definition is shown highlighted within the tree. Click on the magnifier to see the Definition Details for the currently selected definition, which is highlighted.



- Definition Details -- this swatch across the top of the right panel contains some icons which are used to perform actions on the current definition.
 - The green cube  means create a new instance for this definition;
 - the green sphere  means to create a child definition;
 - the red pencil  means to edit the current definition;
 - the eraser  means to delete the current definition (and all items below it);
 - the question mark  is used to request on-line help.

Immediately below this is the name of the current definition, in larger type.

- Core Attributes -- these are attributes which are associated with every definition in the system.
- Child Of -- this swatch identifies the parent definition for the current definition -- clicking on the name of the parent will navigate to it.
- Miscellaneous -- these are options relating to how the definition will be displayed.
 - Definition Reporting: If this box is checked then information about this definition will be included in the system reports separately from the global DMO reports. This way the system administrator can focus on chosen definitions for more detailed information, as well as keeping track of the number of instances for the respective definitions over time.
 - Show in Summary: If this checkbox is checked, this definition will be easily accessible on the system summary page.
- Child Definitions -- this is first of three tabs, which is the default. It shows a table of each of the child definitions for the current definition, along with their descriptions. Clicking on the name of any of the child definitions will navigate to that definition.
- List of Attributes -- the second of three tabs, this shows a table with each of the attributes which MAY be associated with instances of this definition.
- List of Instances -- the third of three tabs, this shows a table with each of the instances which may exist for this current definition. Some definitions have no instances, while some may have thousands. (A limit of 100 instances is placed on this list, to avoid overwhelming the Web browser.)
- Quick Search -- if the name of a definition is known, enter it here and click "Go" to navigate to that definition in the tree.

Note that you will usually see this view of a Definition only if there are no instances that exist for it. By default, the root object should not have any instances. To view this Definition Details page from a list of instances, click on the name of the definition at the top of the page (highlighted in blue), or click on the magnifier icon () in the top right of the Definition Tree swatch.

Editing a Definition

To add a new definition, click on the green sphere  icon for any other definition. The new definition will be created as a child definition for the currently selected definition. To edit an existing definition, select it, and click on the red pencil  icon. Doing so will show a form such as this:

Edit Definition	
Definition name <input type="text" value="CSO Lanifex System"/>	
<div> <div>Core Attributes</div> <div>Child Of</div> </div>	
Revision <input type="text" value="2"/>	Select Definition <input type="text" value="CSO Lanifex System"/>
Number <input type="text"/>	
Description <div>This is the parent object for all other objects.</div>	
Lock Inheritance <input type="checkbox"/>	
Owner <input type="text" value="Admin, EH (admin)"/>	
Group <input type="text" value="No owner"/>	
Type <input type="text" value="Administrative"/>	
Hidden <input type="radio"/> Yes <input checked="" type="radio"/> No	
<div>Save Definition</div> <div>Reset Form</div>	

The Definition Name should follow the rules outlined above. Use the Child Of swatch to specify the parent definition for the new one which you are creating. Attempting to create a definition which already exists will result in an error. As soon as you click the "Save Definition" button, the system will automatically open the form for editing the Definition Attributes (see below.)

Instance List in Definition Details









Normally, clicking on the name of a Definition will show the details for that definition. However, if there are existing instances of that definition, then DMO will instead show a list of the instances, as shown in the example below. To see the real definition details, click on the definition name at the top of the instance list swatch. To return to the instance list, either click on the definition name in the Definition Tree, or click on the magnifier icon which appears in the Instance Browser swatch of an instance details view.



Escalation Preset		Add Column	Page Size 50	Page [1]			
Business Process Instance List							
<input type="checkbox"/>	Name	Date Created	Purpose	Type	Owner	Group	
<input type="checkbox"/>	1 Gehaltsverrechnung	Jun 21 12:14	This is the Payroll Business Process.		admin	default [0]	
<input type="checkbox"/>	2 Penetration Testing	Jan 24, 2004	This is the Penetration testing service, which is offered to external customers.		admin	default [0]	
<input type="checkbox"/>	3 Web Hosting	Feb 7, 2004	This business service relates to the provision of Web hosting.		admin	default [0]	
Add to selection					Replace selection		Page [1]

Editing Definition Attributes

User-defined attributes (not core attributes) may be edited for any definition, subject to user rights. (See the Chapter on Access Control for details on how to enforce access rights, to limit the ability for users to make changes to definitions.) After creating a new definition, it is a good idea (but not essential) to define some attributes for that new definition. Normally, the new definition will inherit all the attributes of its parent definition (but not their values -- only the possibility of assigning a value to the attribute for an instance of the new definition.)

To edit the attributes for a definition, click on the red pencil in the "List of Attributes" tab of the Definition Details view, or edit the core definition, then after saving you will see the following form automatically:

Edit attributes for definition Application	
 	Support Documentation
Revision	10
Description	This attribute is used to attach a document to the instance.
Visible	Yes
Is Password	No
Data Type	file
Inheritable	No
 	Instance Picture
Revision	7
Description	This attribute is used to attach an image of the instance, where available.
Visible	Yes
Is Password	No
Data Type	file
Inheritable	No
 	Escalation Preset
Revision	2
Description	Used to define which escalation preset will be used for incidents
Visible	Yes
Is Password	No
Data Type	escalation_preset
Inheritable	No
 	Configuration File
Name	Configuration File
Revision	2
Description	The configuration file is the primary source of information that
Visible	<input checked="" type="radio"/> Yes <input type="radio"/> No
Is Password	<input type="radio"/> Yes <input checked="" type="radio"/> No
Data Type	Text line
Inheritable	<input type="checkbox"/>

Note that the lock icon  means that the attribute has been defined on one of the definitions which is a parent definition to this one, and should not be edited here. To add a new attribute, use the green plus  icon. After making any required changes, click the "Edit" button to save the new attributes. They will then be immediately available to any instances of that definition (and its child definitions.)

Chapter 5. Instances and their Attributes


About Instances

Instances are Definitions made into specific objects. In other words, an Instance is a concrete example of an abstraction. We make an instance by giving it a unique name, which ensures it can be distinguished from every other instance of the same definition. Instances are always based on specific definitions, however a unique feature of DMO is that we can change the definition associated with an instance. If we do this, any attributes that don't exist for the new definition may be lost. Instances may stand alone, or may be organized into one or more simple trees, which can start with any arbitrary instance as the root. By default, DMO will start display of trees with the first Location instance which it finds, allowing the trees to be organized geographically.

There are several ways in which instances may be viewed:

- Instance Tree -- this is the default, and starts with the first Location instance found. Any other instances should be organized as child instances of this tree.
- Instance List -- this will be shown whenever viewing a definition which has one or more instances associated with it.
- Instance Details -- this is a single page view of a single instance, showing all of its attributes (both core and normal), as well as child instances.
- Instance Selection -- this is a list of one or more instances, which are selected for some group operation, such as creation of a report.

Instance Tree

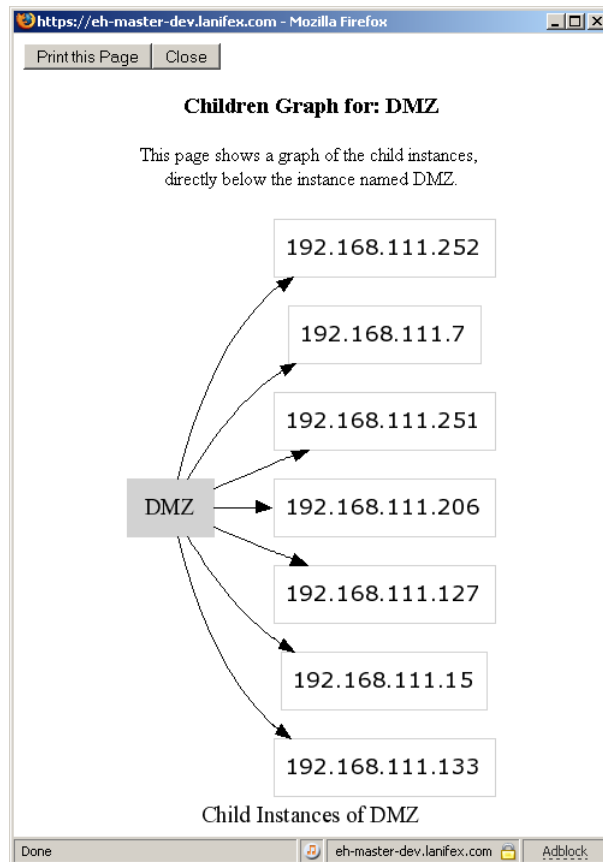
An instance tree is a hierarchical means of viewing instances which have a logical relationship between them. For example, within Event Horizon, we might have a tree consisting of the following elements (note this list will show definition names, but this is a tree made up on instances based on those definitions, it is not a definition tree, and need not follow the structure used by the Definition Tree.) To view the instance tree, click on the tree icon  when viewing the details of an instance.

- Location -- physical place such as an office or building
- Sensor -- a computer used to collect information remotely from a network
- Subnet -- the subnet used to organize hosts within the network
- Host -- a host discovered in the network, such as a router
- Service -- a TCP-based service operating on the host

The following screen shot shows an example of an Instance Tree. Where a tree branch shows a plus sign, click on it to see the instances below in the tree hierarchy. To see the instance itself, click on the magnifier next to the instance name. Clicking on the instance will navigate through the Instance Tree, making the selected instance the root for the view of a new tree. There is no limit to the depth of layers that a tree may use (although the Web browser may be limited by its memory in the number of instances which can be shown on one screen.)



To switch from the tree view back to the detail view for an instance, click on the tree icon [🌳]. Sometimes the topmost instance in the tree will have an up arrow icon [⬆️], which can be used to navigate to its parent instance within the tree view. Also within the tree view, you will find a button labelled "Show Instance Graph", which will show the current instance, plus its immediate child instances in a graphical view, as shown in the screen shot below:



Instance List

A normal view of instances will be the instance list, as shown in the screen shot below. The list is organized into columns, with one row per instance. The columns shown include the name of the instance, its purpose, type, creation date and ownership information. Additional columns may be selected for display using the SELECT control at the top of the swatch (next to the "Add Column" button.) To remove a column from the display (this will NOT delete any data), click on the eraser icon [🧼] in the head of the column. The arrows in each column may be used to control its sorting (alphabetical, or reverse alphabetical.)

Escalation Preset		Add Column	Page Size	50	Page [1]		
Business Process Instance List							
<input type="checkbox"/>	Name	Date Created	Purpose	Type	Owner	Group	
<input type="checkbox"/>	1 Gehaltsverrechnung	Jun 21 12:14	This is the Payroll Business Process.		admin	default [0]	
<input type="checkbox"/>	2 Penetration Testing	Jan 24, 2004	This is the Penetration testing service, which is offered to external customers.		admin	default [0]	
<input type="checkbox"/>	3 Web Hosting	Feb 7, 2004	This business service relates to the provision of Web hosting.		admin	default [0]	
Add to selection					Replace selection		Page [1]

Where there is a large number of instances, the paging mechanism will be activated, which allows control of the number of rows per page, and which provides navigation controls to move forwards or backwards through the pages.

The title of the swatch contains the name of the Definition (as a clickable link leading to the definition) on which these instances are based, along with some controls which are:

- Green sphere -- create a new definition as child of current definition
- Green cube -- create a new instance based on current definition
- Cluster of green cubes -- create several instances based on current definition
- Report icon -- create a report based on the current list of instances




The first column contains check boxes, which are used for adding instances (rows) to the selection. Click on each instance to be selected on a page, then click on either of the buttons "Add to selection" or "Replace selection."

Instance Detail

Click on the name of an instance from the instance list, or the magnifier from the instance tree, and you will get the instance details display, as shown in the screen shot below.

Business Process																									
Gehaltsverrechnung																									
Edit View Create Delete Help																									
<p>Core Attributes</p> <table border="1"> <tr><td>Date Created</td><td>Jun 21 12:14</td></tr> <tr><td>Revision</td><td>1</td></tr> <tr><td>Serial</td><td>-</td></tr> <tr><td>Location</td><td>-</td></tr> <tr><td>Inventory</td><td>-</td></tr> <tr><td>Purpose</td><td>This is the Payroll Business Process.</td></tr> <tr><td>Notes</td><td>-</td></tr> <tr><td>Type</td><td>-</td></tr> <tr><td>Lock inheritance</td><td>No</td></tr> <tr><td>Owner</td><td>EH Admin (admin)</td></tr> <tr><td>Group</td><td>default [0]</td></tr> <tr><td>Parent</td><td>-</td></tr> </table>	Date Created	Jun 21 12:14	Revision	1	Serial	-	Location	-	Inventory	-	Purpose	This is the Payroll Business Process.	Notes	-	Type	-	Lock inheritance	No	Owner	EH Admin (admin)	Group	default [0]	Parent	-	<p>Instance Browser</p> <p>Instance 3 of 3</p> <p>Attributes</p> <p>[no visible attributes]</p> <p>Attribute Parents</p> <p>[no parent attributes]</p> <p>Dependencies</p> <p>Gehaltsverrechnung does not depend on any other instances</p> <p>No other instances depend on Gehaltsverrechnung</p> <p>Intrinsic Links</p> <p>[no intrinsic links]</p>
Date Created	Jun 21 12:14																								
Revision	1																								
Serial	-																								
Location	-																								
Inventory	-																								
Purpose	This is the Payroll Business Process.																								
Notes	-																								
Type	-																								
Lock inheritance	No																								
Owner	EH Admin (admin)																								
Group	default [0]																								
Parent	-																								
<p>Global URL's</p> <p>[no URL's]</p>																									
<p>Instance Children</p> <p>2 Child Instances found. Please click on an instance name, or on the magnifying glass at the right to see details.</p> <table border="1"> <thead> <tr> <th>No.</th> <th>Instance Name</th> <th>Purpose</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Wien Gehaltsverrechnungs Datenbank</td> <td>We use this to calculate payroll. Information is sent to the Bank.</td> </tr> <tr> <td>2</td> <td>Personal Datenbank</td> <td>List of all Personnel</td> </tr> </tbody> </table>		No.	Instance Name	Purpose	1	Wien Gehaltsverrechnungs Datenbank	We use this to calculate payroll. Information is sent to the Bank.	2	Personal Datenbank	List of all Personnel															
No.	Instance Name	Purpose																							
1	Wien Gehaltsverrechnungs Datenbank	We use this to calculate payroll. Information is sent to the Bank.																							
2	Personal Datenbank	List of all Personnel																							
<p>Last 10 Events for this Instance</p> <p>[No events found]</p>																									

The first row shows the name of the definition on which the current instance is based, as a set of "breadcrumbs", which are links to each of the parent definitions. The controls in the top row of the swatch are similar to those described in the previous section, with the addition of the following three:

- Pencil icon  -- edit the current information. If found in the definition part, it means edit the definition. If found in the instance swatch, it means edit the instance, otherwise edit some other part as per context.
- Tree icon  -- show the current instance in a tree view, with all its child instances below it in the tree
- Eraser icon  -- delete the current definition. Always be very careful before selecting this -- although it requires confirmation anyway.

The second row of this swatch shows the unique name of the instance (plus the eraser icon which will delete the instance.) Below this is a menu, which provides alternatives to clicking on the various icons, regarding the instance currently shown. This menu is dynamic, with a second level. Hover over the menu item to see the second level choices displayed -- clicking on the second level choice will activate it.

The swatches shown in the instance details view are described below:

- *Core attributes* -- these are the attributes which are available for every different type of definition. By default, the "Date Created" attribute is set by the system, and the "Revision" attribute is incremented each time this instance is changed. These core attributes (including the name) may be changed using the pencil icon in the upper left corner of this swatch, or the "Edit // Instance" item from the menu.
- *Instance Browser* -- this is used to navigate between the instances that belong to the same definition. It offers forward and back arrows (for single steps), or the double arrows to move to the end or beginning of the list. Entering a number (this is not the same as the DMO id#) can also be used. The magnifier in this swatch may be used to return to the Instance List view.
- *Attributes* -- these are the non-core attributes, which are available only for the currently selected definition, and its child definitions. Some objects might have no

attributes defined, in which case no information might be shown here. Attributes which contain file attachments with images (of type JPEG, GIF or PNG) will be rendered in-line. A pencil is available to edit these attributes, while the magnifier is used to see a list of the attributes along with descriptions of them.

- *Attribute Parents* -- this is a unique DMO feature, which allows any instance "A" to be an attribute of another instance "B" -- in which case we say that "B" is the "Attribute Parent" of "A". Effectively, this allows definition of complex interlocking multiple hierarchies of instances, based on an arbitrary number of attributes. Note that we don't edit the parent -- instead, visit the other instance, and define another instance as one of its child attributes.
- *Dependencies* -- any instance may have other instances that depend upon it, and in turn may depend upon another instance. These dependencies may be modelled using this swatch. Use the red pencil to edit them.
- *Intrinsic Links* -- this is an internal reserved feature of DMO, which is part of the proprietary product.
- *Global URLs* -- this is a list of shared URLs which may be associated with one or more instances. Typically, these will lead to more information about this instance, or a set of instances. These URLs are often used for documentation. (Note that URLs may also be stored as attributes for a single instance, but they are not available to be shared between instances, as are Global URLs.)
- *Instance Children* -- this is a list of all direct child instances of the currently selected instance. Also included in the list is the "Purpose" Core Attribute.
- *Last 10 Events* -- when used within Event Horizon, this shows a list of the last 10 events associated with this instance, sorted in reverse time order, with most recent first.
- *Forum* -- a simple tool for adding notes onto the current instance without editing an attribute.

Instance Selection

Some operations allow the selection of an arbitrary number of different, unrelated instances, into a single group that we call a Selection. One of the primary purposes of the Selection is to prepare information for a Report. The "Instance Selection" swatch (found to the left of the display, under the definition tree) gives three options:

- Add Instance to Selection -- the currently selected instance will be added to the selection
- Clear Selection -- remove all instances from the selection
- View Selection -- switch to view the current items in the Instance Selection

Instance may also be added to the selection (either additional or replacing the current selection) from within the Instance List. The following screen shot shows an Instance Selection:

Create Report

[select definition]
Move Selection

[select group]
Change Group

[select owner group]
[select member]
Change owner

[select definition]
[select instance]
Change parent

Selected Instance List

	Instance Name	Definition
1	Primary Internal Subnet	Subnet
2	Bucharest, Romania	Location
3	Vienna, Austria	Location

Change attribute
Escalation Preset
TO

PG Test chain 8 mins
Change

Change core attributes
Revision

☐ Value to:

☐ Pattern:

TO

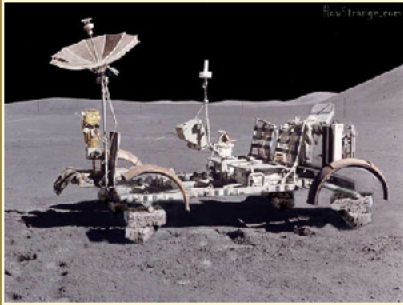
Change

Once a selection has been made, many things can be done against it, including:

- Move Selection -- move all the instances to a different Definition (some attribute values may be lost as a result, if the target definition doesn't contain the same attributes as the selected definition's instances). Note that one of the targets is Deletion, which allows all items in the selection to be permanently deleted.
- Create Report -- allows data from the Selection to be used in a report, in one of PDF, CSV, HTML or XML formats
- Change Owner -- changes the user who owns the instances in the selection
- Change Group -- changes the group who owns the instances in the selection
- Change Parent -- allows selection of an instance (from a selected definition) which will be substituted as the parent instance for all the currently selected instances in the Selection
- Change Attribute -- allows selected attributes to be changed, including attachments
- Change Core Attribute -- allows selected core attributes to be changed, either by directly replacement or by a search and replace

Instance Attributes

User-defined attributes may be established for any definition. (See Chapter 4, Section 7 on how to edit definition attributes.) Once an attribute has been associated with a definition (either directly, or inherited from a parent definition), it may then be added to an instance and assigned a value. To edit the attributes for an instance, click on the red pencil in the Attributes swatch, or use the menu item "Edit//Attributes" from the Instance Details view. The following screen will appear:

Edit Instance Attributes	
<div> <div>Support Documentation</div> <div>This attribute is used to attach a document to the instance.</div> <div> <div>Language</div> <div>English</div> <div>Version</div> <div></div> </div> <div> <div>File</div> <div>Last uploaded file: None</div> <div>Browse...</div> </div> </div>	
<div> <div>Escalation Preset</div> <div>Used to define which escalation preset will be used for incidents</div> <div> <div>Escalation Preset</div> <div>PG Test chain 8 mins</div> </div> </div>	
<div> <div>Confidentiality</div> <div>This attribute is used to assess the confidentiality.</div> <div> <div>Instance Link</div> <div>Public [Edit]</div> </div> </div>	
<div> <div>Instance Picture</div> <div>This attribute is used to attach an image of the instance, where available.</div> <div> <div>Language</div> <div>English</div> <div>Version</div> <div></div> </div> <div> <div>File</div> <div>Last uploaded file: 707268moon_buggy_wallpaper.jpg</div> <div>Browse...</div> </div> <div>  </div> </div>	
<div> <div>HTML page of Location</div> <div>This is a Large Text attribute that will be used to contain HTML for a Location.</div> <div> <div>Language</div> <div>English</div> <div>Version</div> <div></div> </div> <div> <div>This is an HTML description of the Location.</div> </div> </div>	
<div> <div>yesnomaybe</div> <div>testing boolean</div> <div> <div>Boolean</div> <div>True</div> </div> </div>	
<div> <div>Save</div> <div>Reset Form</div> </div>	

Each attribute (which is visible) may now be changed, according to its type. For example, files may be attached (including images, which are shown inline), text may be added to text boxes (in multiple languages), items may be chosen from a SELECT list (such as the Escalation Presets), boolean values selected, and other instances attached as attributes. Once the changes are made, click on the "Save" button, and each attribute will be stored for that instance.


Note that if the "Inheritable" attribute is set for an attribute, then when it is assigned a value, all of the child instances below the current instance will receive a copy of that attribute and its value. This is particularly useful for objects which should inherit information such as a security classification. Note also that this can be blocked by using the core attribute "Lock Inheritance" set to no, in which case all instances of that definition type will ignore such inherited attribute values.

Pluggable Actions

This section will describe the pluggable actions associated with instance attributes, including the mechanism for defining new plug-ins.

Chapter 6. Creating Reports

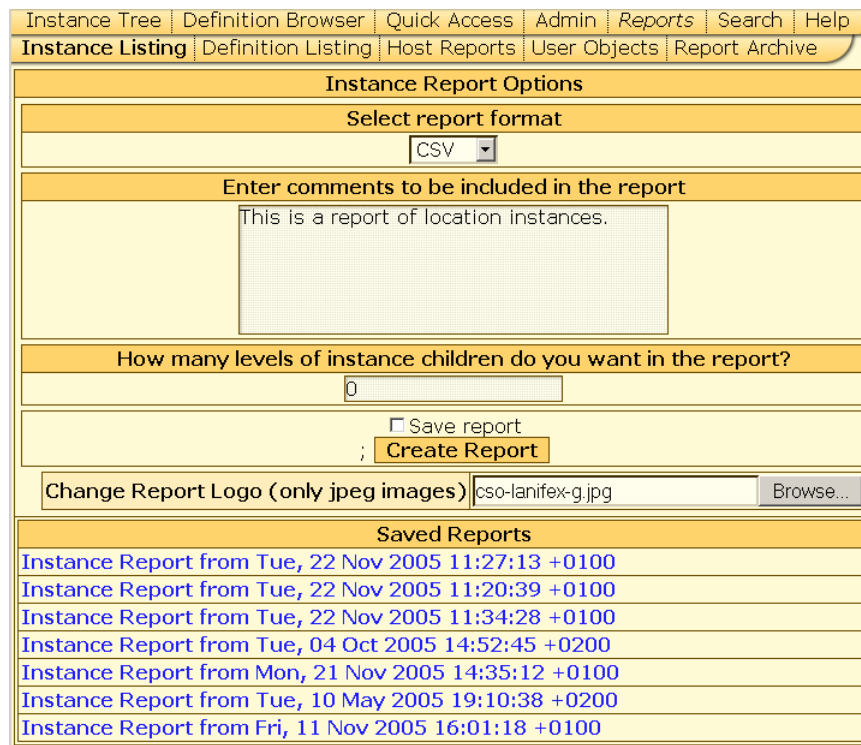
Selecting Report Objects

There are three methods used to prepare a report. First, use the Instance Selection mechanism described above to select all of the instances which will be included in a report. This has no limit to the number of instances which may be selected. Alternatively, reports may be based on the results of a search (see the next Chapter.) A third (and fastest) method for producing a report is to use the Report icon  which appears in the instance list, which will prepare a report based on all the currently shown instances.

Choosing Report Type

After selecting which instances will be used for a report, the following form will be displayed. This form offers four different types of reports:

- PDF -- a multi-page Portable Document Format file, which will be saved via the browser
- XML -- output formatted according to Extensible Markup Language rules
- CSV -- comma separated values, suitable for import into a database or spreadsheet
- HTML -- output designed to be viewed in a Web browser



The screenshot shows a web interface for creating reports. At the top is a navigation bar with links: Instance Tree, Definition Browser, Quick Access, Admin, Reports, Search, and Help. Below this is a sub-navigation bar with links: Instance Listing, Definition Listing, Host Reports, User Objects, and Report Archive. The main form is titled "Instance Report Options" and contains several sections:

- Select report format:** A dropdown menu with "CSV" selected.
- Enter comments to be included in the report:** A text area containing the text "This is a report of location instances."
- How many levels of instance children do you want in the report?:** A text input field with the value "0".
- Buttons:** A checkbox for "Save report" and a "Create Report" button.
- Change Report Logo (only jpeg images):** A text input field with the value "cso-lanifex-g.jpg" and a "Browse..." button.
- Saved Reports:** A list of previously saved reports with their timestamps.

Saved Reports
Instance Report from Tue, 22 Nov 2005 11:27:13 +0100
Instance Report from Tue, 22 Nov 2005 11:20:39 +0100
Instance Report from Tue, 22 Nov 2005 11:34:28 +0100
Instance Report from Tue, 04 Oct 2005 14:52:45 +0200
Instance Report from Mon, 21 Nov 2005 14:35:12 +0100
Instance Report from Tue, 10 May 2005 19:10:38 +0200
Instance Report from Fri, 11 Nov 2005 16:01:18 +0100

The above screenshot shows selection of report options. First, the type of output should be selected. Next, a box is available into which you can enter some text which will be prepended to the report. Underneath is a field where you can enter the number of levels of instance children which will be included in the report. This is designed to enable reports on instances and their child instances (the default is 0, which means no child instances will be included.)

Next, there is a checkbox, which if selected will save a copy of the report onto disk, for later access. Below this is a file selector which allows you to choose the logo or image to be used in the PDF version of the report. Finally, there is a list of the reports which have been previously saved, and which may be viewed by clicking on them.

Report Menu Items

The DMO menu at the top has five options, which provide the following capabilities:

1. *Instance Listing*

This will show a form similar to that above (excluding child instance level selection). If no instances have been selected, this report will default to showing ALL instances, which may generate a large amount of output.

2. *Definition Listing*

This menu item shows a similar form for definitions, with the default behaviour being to create a report on all definitions within the system. Note that there is a core attribute "Definition Reporting", which will exclude definitions from the report if it is not checked for them.

3. *Host Report*

This menu item will produce the screen shot below (or similar.) It will generate a tree containing all the definitions under the //Network Object//Node//Host part of the definition tree, along with all of their instances, with check boxes. Check each of the instances you wish to appear in the report, choose between the options available, then click on the Submit button.

Instance Tree	Definition Browser	Quick Access	Admin	Reports	Search	Help
Instance Listing	Definition Listing	Host Reports	User Objects	Report Archive		

Please select instances to generate Host Report

Host

- UNIX Server
- UNIX Workstation
- Windows Server
- Desktop Computers
- Printer
 - ☐ 192.168.0.11
- Tape Robot
- Time Server
- Laptop
 - ☐ 192.168.0.95
 - ☐ 192.168.0.35
 - ☐ CYBERTOWN-PP
 - ☐ 192.168.0.72
 - ☐ OVERDOSE
 - ☐ GOLE
 - ☐ Andrei test
- Mainframe
- Dial-in Server
- Novell Server
- Wireless AP
- Load Balancer

Options	
Include into report: <input type="checkbox"/> Core Attributes <input type="checkbox"/> Attributes <input type="checkbox"/> Dependencies <input type="checkbox"/> Children <input type="checkbox"/> Events <input type="checkbox"/> Nessus/AIDA Report	Output: <input checked="" type="radio"/> HTML (Display in Browser) <input type="radio"/> PDF (External reader) <input type="radio"/> Subscribers
<input type="button" value="Submit"/>	

4. User Objects

The User Objects report allows creation of a report containing all instances which are owned by a selected user.

Instance Tree	Definition Browser	Quick Access	Admin	Reports	Search	Help
Instance Listing	Definition Listing	Host Reports	User Objects	Report Archive		

DMO User Objects

Select a User, and this will display a list of the DMO instances owned by that user.

Please select a user from this list:

Gillingwater, Paul (paul)

5. Report Archive

This menu option shows the archive of reports, and provides a mechanism to filter reports, based on their type and the date they were generated. Selected reports (using check boxes) may be sent via email to selected addresses.

Instance Tree	Definition Browser	Quick Access	Admin	Reports	Search	Help
Instance Listing	Definition Listing	Host Reports	User Objects	Report Archive		

Saved Reports			
Search Filters			
Creation Date (MM/DD/YYYY)		Report Type	
From	<input type="text"/>	<input checked="" type="checkbox"/>	Definition Listings
Until	<input type="text"/>	<input checked="" type="checkbox"/>	Instance Listings
Description Contains		<input checked="" type="checkbox"/>	Definition Instances
<input type="text"/>		<input checked="" type="checkbox"/>	Selection Listings
Reports per page		<input checked="" type="checkbox"/>	Query Search Results
<input type="text" value="20"/>		<input checked="" type="checkbox"/>	Advanced Search Results
<input type="button" value="Apply Filters"/>			

[1]			
<input type="checkbox"/>	Report Type	Creation Date	Deletion Date
<input type="checkbox"/> ?	Definition Listing	Jul 5	Aug 4
<input type="checkbox"/> ?	Definition Listing	Jun 9	Jul 9
<input type="checkbox"/> ?	Definition Listing	Jun 9	Jul 9
With selected (only first selected)		Mail To	<input type="text"/>

Chapter 7. Searching and Selection

Searching within DMO

There are three main ways available for searching for information within the DMO using the Web interface. Two of them are available in the "Search" menu (Query Search and Advanced Search), and the third method (Quick Search) is available when viewing Instances or Definitions. Query and Advanced searches may be saved for later re-use. The Quick search is fast, but limits what can be searched.

Quick Search

The Quick Search function is available from at the left of the display when viewing instances or definitions, and their lists.

The screenshot shows the 'Quick Search' section of a web application. It features a search bar with a 'Go' button. Below the search bar are four radio buttons for selecting the search scope: 'Definitions' (selected), 'Instances', '[By owner]', and '[By attribute]'. There are also dropdown menus for '[By owner]' and '[By attribute]'. Below these are sections for 'Query Search' (with a '[select query]' dropdown) and 'Advanced Search' (with a '[select search]' dropdown). At the bottom is an 'Instance Selection' section with links for 'Add Instance to Selection', 'Clear Selection', and 'View Selection'. To the right of the search section is a 'Location' panel showing a world map and the text 'Vienna, Austria'. Below the map is a list of locations: 'Location : Vienna, Austria', 'Branch Office : Lanifex Office', 'Branch Office : Bartexim Office', and 'Subnet : Subnet Test Eddie'.

The Quick Search has an entry box, where a search string may be entered, and four radio buttons below, which provide the following choices:

- Definitions -- search among the names of definitions, and show the definitions which match
- Instances -- search among the names of instances, and show the instances which match
- By Owner -- search either the names of the owner of instances or of definitions
- By Attribute -- search among the attributes of instances, and show the instances which match

Note that the Quick Search is implemented using SQL syntax, which means that a "%" character can be used as a substitution for matching many characters. For example, to find all instances which have an IP Address in the subnet 192.168.111.0/24, select the "By Attribute" radio button, choose "IP Address" from the select list, and enter the following text into the search box:

192.168.111.%

The result of the search will be a list of the matching instances, with check boxes next to them. To add the results of the search to the selection (e.g., to perform other

actions), click the check boxes of the instances of interest and click the "Add to Selection" button. The following screen shot shows the results of such a search.

Instance Tree		Definition Browser		Quick Access		Admin		Reports		Search		Help	
Definition Tree				Search Results For Query: [192.168.111.%]									
CSO Lanifex System[0+1573]				Instances									
<input checked="" type="checkbox"/> Application [0+28]				<input type="checkbox"/> midgard-dev.lanifex.com									
<input checked="" type="checkbox"/> Asset [1+3]				<input type="checkbox"/> 192.168.111.175									
Business Process[3+0]				<input type="checkbox"/> monkey2-dmz.lanifex.com									
<input checked="" type="checkbox"/> COBIT Processes[0+2]				<input type="checkbox"/> monkey1-dmz.lanifex.com									
Dependency [1+0]				<input type="checkbox"/> eh-master-dev.lanifex.com									
<input checked="" type="checkbox"/> Infrast... Object[0+10]				<input type="checkbox"/> acs-dev.lanifex.com									
<input checked="" type="checkbox"/> ITIL Process [0+0]				<input type="checkbox"/> 192.168.111.9									
<input checked="" type="checkbox"/> Location [2+4]				<input type="checkbox"/> 192.168.111.203									
<input checked="" type="checkbox"/> Network Object[0+1487]				<input type="checkbox"/> 192.168.111.7									
<input checked="" type="checkbox"/> Policy Object [1+20]				<input type="checkbox"/> 192.168.111.10									
<input checked="" type="checkbox"/> Processes [0+8]				<input type="checkbox"/> 192.168.0.6									
<input checked="" type="checkbox"/> Responsibility [0+1]				<input type="checkbox"/> 192.168.111.251									
Risk [1+0]				<input type="checkbox"/> 192.168.111.252									
Securit...ication[1+0]				<input type="checkbox"/> 192.168.111.206									
Unassigned [0+0]				<input type="checkbox"/> 192.168.111.127									
Quick Search				<input type="checkbox"/> 192.168.111.127-test									
192.168.111.% <input type="button" value="Go"/>				<input type="checkbox"/> 192.168.111.15									
<input type="radio"/> Definitions				<input type="checkbox"/> 192.168.111.133									
<input type="radio"/> Instances				<input type="button" value="Add to selection"/> <input type="button" value="Replace selection"/>									
<input type="radio"/> [By owner]				<input type="button" value="View Selection"/>									
<input checked="" type="radio"/> IP Address													
Query Search													
[select query]													
Advanced Search													
[select search]													
Instance Selection													
Add Instance to Selection													

To select all of the results of the Quick Search, click on the first checkbox in the list, which should activate all checkboxes below it.

Configuring Quick Search Attributes

The attributes shown by default in the Quick Search menu are configurable. There is a magnifier  icon in the Quick Search swatch. Click on it to open the Quick Search Attribute Selector, as shown below.

Instance Tree Definition Browser Quick Access Admin Reports Search Help							
Definition Tree <ul style="list-style-type: none"> CSO Lanifex System[0+1573] <ul style="list-style-type: none"> Application [0+28] <ul style="list-style-type: none"> Asset [1+3] <ul style="list-style-type: none"> Business Process[3+0] COBIT Processes[0+2] <ul style="list-style-type: none"> Dependency [1+0] Infrast... Object[0+10] ITIL Process [0+0] Location [2+4] Network Object[0+1487] Policy Object [1+20] Processes [0+8] Responsibility [0+1] <ul style="list-style-type: none"> Risk [1+0] Securit...ication[1+0] Unassigned [0+0] 	Quick Search By Attribute Selector <div> <input type="text" value="IP Address"/> </div> <div> Create/Edit <table> <tr> <td>Name</td> <td><input type="text" value="IP Address"/></td> </tr> <tr> <td>Attribute</td> <td><input type="text" value="IP Address"/></td> </tr> <tr> <td>Type</td> <td><input type="text" value="System"/></td> </tr> </table> <div>Save</div> </div>	Name	<input type="text" value="IP Address"/>	Attribute	<input type="text" value="IP Address"/>	Type	<input type="text" value="System"/>
Name	<input type="text" value="IP Address"/>						
Attribute	<input type="text" value="IP Address"/>						
Type	<input type="text" value="System"/>						
Quick Search <div> <input type="text"/> <input type="button" value="Go"/> </div> <div> <input checked="" type="radio"/> Definitions <input type="radio"/> Instances <input type="radio"/> [By owner] <input type="radio"/> IP Address </div>							
Query Search <div> <input type="text" value="[select query]"/> </div>							
Advanced Search <div> <input type="text" value="[select search]"/> </div>							
Instance Selection <div> <input type="button" value="Add Instance to Selection"/> <input type="button" value="Clear Selection"/> <input type="button" value="View Selection"/> </div>							

The attributes are selected from a list of all simple text instance attributes, plus some core attributes. Choose the attribute you wish to search on, and assign it a name (usually the same name as the attribute itself.) Select "System" if it is to be made available to all users in the system, or "User" if the saved search attribute is specific to the current user only. Use the eraser icon to delete the current attribute from the list of attributes available for a Quick Search. This form can also be used to edit existing saved attributes.

Query Search

The Query Search

Advanced Search

Chapter 8. DMO Administration

A guide to the administration functions of the DMO.

Chapter 9. Access Controls

How to set up Access Controls within the DMO.

Chapter 10. Inheritance

This is a complex topic that requires its own chapter.

Chapter 11. Modeling Dependencies

This chapter describes how to model dependencies between DMO instances, and how to perform a failure simulation.

Chapter 12. DMO within Event Horizon

How the DMO is used specifically within Event Horizon

Chapter 13. DMO within Policy Compliance Manager

How the DMO is used specifically within the PCM

Chapter 14. DMO within Crisis Manager

How the DMO is used within the Lanifex Crisis Manager

Chapter 15. LFXlib

This is the foundation library of the DMO, which requires its own documentation.

Chapter 16. Customization and Development

How developers can customize the DMO, and write their own plug-ins and programs using the DMO. It also provides a road-map for future development of DMO, plus guidelines for Open Source contributors who wish to work in the DMO project.

Chapter 17. DMO and Security Audits

Lanifex uses the DMO in its security audits, as a central repository of information that has been discovered.

Chapter 18. DMO Operations

This is a guide to how to use DMO in an operational environment. It includes information on which information should be backed up, how DMO can be used with a database cluster, how to troubleshoot DMO problems and security considerations. It also talks about the security of DMO itself.

