MYSURVEILLANCE

Admin Manual

Research & Development Unit
Open Source Competency Centre (OSCC),
MAMPU,
Lot E302-34, Enterprise Building 3,
63000 Cyberjaya, Selangor
Tel: 03-8319 1200
Fax: 03-83193206
http://opensource.mampu.gov.my

TABLE OF CONTENTS

Introduction

MySurveillance is a security monitoring system application that collects and analyzes security reports from all network devices and system applications such as firewalls, databases, web servers and switches. MySurveillance client-server architecture helps organizations/individuals to monitor all security alerts for devices or applications from a central (MySurveillance server).

Each client that need to be monitored will be installed with a MySurveillance sensor which will collect the security event logs and Intrusion Detection Message Exchange Format (IDMEF) will translate the log to a common language using IDMEF before sending it to the MySurveillance server for analysis. Report of all security events will be displayed at the MySurveillance Console.

Features

Some of the features available in MySurveillance are:

- Able to support log files generated by various devices and applications available in the market.
- Real-time analysis of events received from MySurveillance Sensor
- Built-in event log filter enables only critical and error messages to be displayed at central server.
- Data can be collected and corellated from sensors deployed on supported devices.

Hardware and Software

	Manager	Client
Hardware	Pentium IV and above 512MB RAM and above 10GB HD and above	No specification
Software	MySQL Apache libprelude libpreludedb prewikka	
	CentOS5 prelude-manager	Open Source Independent mysurveillance-client prelude-lml

Architecture

There are four components involved in MySurveillance which are ***MySurveillance Sensors/Agents***, ***MySurveillance Server***, ***MySuveillance Data Store*** and ***MySurveillance Console***.

- ***Sensors/Agents*** at the client-server (prelude-lml) are responsible for intrusion detection, and report events in a centralized fashion using a Transport Layer Security (TLS)
- All the report of security events will be collect and analyze at ***MySurveillance Server*** (prelude-manager).
- MySurveillance uses Intrusion Detection Message Exchange Format (IDMEF) as the common language for reporting events. The server can then process these events and deliver them to a ***MySurveillance Data Store***.
- The ***MySurveillance Console*** can then be used to view these events log reading the information from the MySurveillance Data Store.

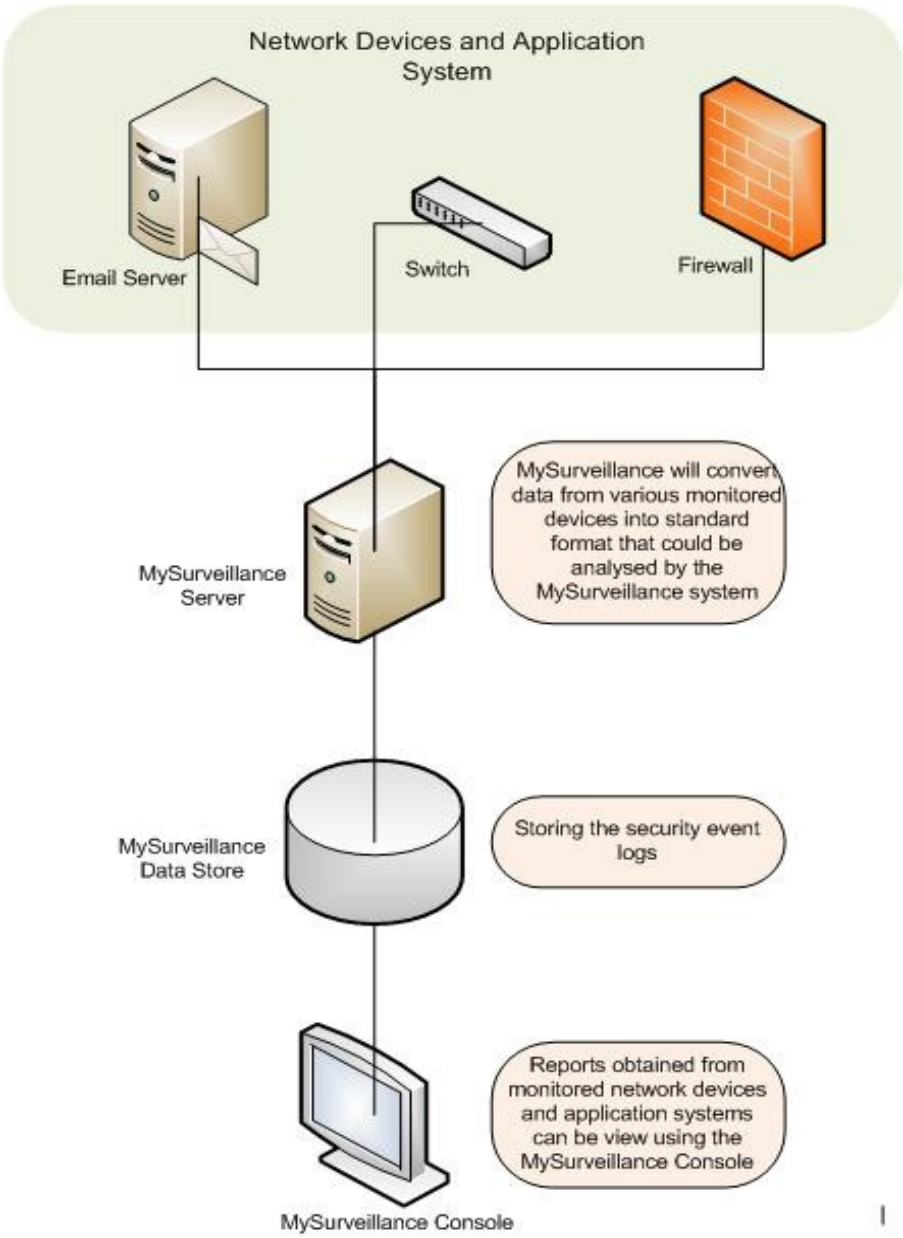


Figure 4.1 : Architecture Diagram

Dependencies

MySurveillance-server

Package	Arch	Version	Repository	Size
Installing:				
mysurveillance-server	i386	1.1-1.oscc	oscc-repo	2.2 k
Installing for dependencies:				
libprelude	i386	0.9.17.2-1	oscc-repo	985 k
libprelude-python	i386	0.9.17.2-1	oscc-repo	520 k
libpreludedb	i386	0.9.14.1-1	oscc-repo	196 k
libpreludedb-mysql	i386	0.9.14.1-1	oscc-repo	28 k
libpreludedb-python	i386	0.9.14.1-1	oscc-repo	90 k
mysurveillance-client	i386	1.0-2.oscc	oscc-repo	1.9 k
oscc-bayesian	noarch	0.0.2-4.oscc	oscc-repo	2.2 M
oscc-tracking	noarch	0.0.2-1.oscc	oscc-repo	29 k
perl-Archive-Tar	noarch	1.30-1.fc6	base	47 k
perl-Compress-Zlib	i386	1.42-1.fc6	base	52 k
perl-Digest-HMAC	noarch	1.01-15	base	12 k
perl-Digest-SHA1	i386	2.11-1.2.1	base	48 k
perl-HTML-Parser	i386	3.56-1	oscc-repo	124 k
perl-IO-Socket-INET6	noarch	2.51-2.fc6	base	13 k
perl-IO-Socket-SSL	noarch	1.07-2.el5.rf	oscc-repo	43 k
perl-IO-Zlib	noarch	1.04-4.2.1	base	15 k
perl-Net-DNS	i386	0.61-1.el5.rf	oscc-repo	276 k
perl-Net-Daemon	noarch	0.43-1	oscc-repo	44 k
perl-Net-IP	noarch	1.25-2.fc6	base	31 k
perl-Net-SSLeay	i386	1.30-4.fc6	base	195 k

perl-Socket6	i386	0.19-3.fc6	base	22 k
perl-libwww-perl	noarch	5.805-1.1.1	base	376 k
prelude-lml	i386	0.9.12.2-5	oscc-repo	187 k
prelude-manager	i386	0.9.12.1-1	oscc-repo	192 k
prewikka	noarch	0.9.14-1	oscc-repo	420 k
python-cheetah	i386	2.0-0.1.rc8.el5.rf	oscc-repo	423 k
spamassassin	i386	3.2.4-1.el5	base	1.0 M

MySurveillance-client

Package	Arch	Version	Repository	Size
Installing:				
mysurveillance-client	i386	1.0-2.oscc	oscc-repo	1.9 k
Installing for dependencies:				
libprelude	i386	0.9.17.2-1	oscc-repo	985 k
oscc-tracking	noarch	0.0.2-1.oscc	oscc-repo	29 k
prelude-lml	i386	0.9.12.2-5	oscc-repo	187 k

Prerequisites

Prelude-manager

Prelude Manager is the main program of MySurveillance system. It is a multithreaded server which handles connections from the MySurveillance sensors. It is able to register local or remote sensors, enable the operator to configure them remotely, receive and store alerts in a database or any format supported by reporting plugins, thus providing centralized logging and analysis. It also provides relaying capabilities for failover and replication. Support for filtering plugins allows you to hook in different places in the Manager to define custom criteria for alert relaying and logging.

Prelude-lml

The Prelude Log Monitoring Lackey (LML) is the host-based sensor program component. It can act as a centralized log collector for local or remote systems. It can run as a network server listening on a syslog port or analyze log files. It supports logfiles in the Berkeley Software Distribution (BSD) syslog format and is able to analyze any logfile by using the Perl Compatible Regular Expressions (PCRE) library. It can send an alert to the Prelude Manager when a suspicious log entry is detected.

Libprelude Library

Libprelude is the library that provides the framework used to access the Prelude system. It handles secure communications with the MySurveillance sensor, and provides an Application Programming Interface (API) to create Intrusion Detection Message Exchange Format (IDMEF) based events. It also provides important features like fail-over (by saving to a local file for later retransmission later and usage of a fallback route), in case one of the MySurveillance servers goes down. Moreover, it gives you the ability to create sensors that read events received by one or more MySurveillance servers.

Libpreludedb Library

The PreludeDB Library provides an abstraction layer based upon the type and the format of the database used to store Intrusion Detection Message Exchange Format (IDMEF) alerts. It allows developers to use the MySurveillance Data Store easily and efficiently without worrying about Structured Query Language (SQL), and to access the MySurveillance Data Store independently of the type/format of the database.

Prewikka

Prewikka is a web-based management console for MySurveillance. Some of the features available in Prewikka are contextual filtering, aggregation and permission management.

Apache HTTP Server (for MySurveillance Console)

The Apache HTTP Server is the most popular Open Source and widely used web server in the world. The Apache HTTP server is known to be a stable and extensible server.

Centos Linux Operating System

CentOS is an Enterprise-class Linux Distribution derived from sources freely provided to the public by Red Hat . CentOS conforms fully with the upstream vendors redistribution policy and aims to be 100% binary compatible to Red Hat Enterprise Linux.

MySQL (for MySurveillance Data Store)

MySQL is a very popular and widely used Open Source database that is known for its robustness and ease of use. Some features available are multiple storage, query caching, Secure Sockets Layer (SSL) support and many more.

Installation Steps

There are two steps of installation involved with installation of the admin-server with an IP of 192.168.0.1 and a client-server with an IP of 192.168.0.2 to the system.

Section 1: Installing the mysurveillance server

1) To sync date and time at the server to an NTP server, run the command:

```
ntpdate pool.ntp.org
service ntpd start
chkconfig ntpd on
```

2) Install/Enable the OSCC repos:

```
rpm -Uvh http://repos.oscc.org.my/repos2/centos/5/oscc/i386/CentOS/oscc-repos2-0.0.1-1.noarch.rpm
```

3) Install mysurveillance-server

```
yum install mysurveillance-server
```

4) Change configurations in the */etc/prelude-manager/prelude-manager.conf* file

```
listen = SERVER_IP
       (eg: 192.168.0.1)
```

5) Add prelude-manager to the system by run this command

```
prelude-admin add "prelude-manager" --uid 0 --gid 0
```

6) Start prelude-manager service by run this command

```
service prelude-manager start
```

7) After the installation is complete, open web browser.

```
http://SERVER_IP/mysurveillance
      (eg: http://localhost/mysurveillance)
   or (eg: http://192.168.0.1/mysurveillance)
```

**Use this default login and password, but we recommend that you change the password as soon as possible for security purposes .

login: **admin**

password: **admin**

Section 2: Adding client to the system

Installation steps for the client:

1) To sync date and time at the client-server to ntp time, run command:

```
ntpdate pool.ntp.org
service ntpd start
chkconfig ntpd on
```

2) Install/Enable OSCC repos

```
rpm -Uvh http://repos.oscc.org.my/repos2/centos/5/oscc/i386/CentOS/oscc-repos2-0.0.1-1.noarch.rpm
```

3) Install mysurveillance-client

```
yum install mysurveillance-client
```

4) Change the following in the config files:

4.1) /etc/prelude/default/client.conf

```
server-addr = IP_ADMIN_SERVER
  (eg: 192.168.0.1)
```

4.2) /etc/prelude/default/global.conf

```
analyzer-name = NAME
        (eg: test)
  node-name = MACHINE_NAME
        (eg: oscc1)
  node-location = COMPANY_NAME
              (eg: OSCC)
  node-category = REFER_NODE_TYPE
              (eg: unknown)

  [Node-Address]
  address = IP_ADDRESS
        (eg: 192.168.0.2)
```

4.3) /etc/prelude-lml/prelude-lml.conf

comment out all command in the config file **EXCEPT**:

```
[format=syslog]
time-format = "%b %d %H:%M:%S"
      prefix-regex = "^(?P<timestamp>.{15}) (?P<hostname>\S+) (?:(?
      P<process>\S+?)(?:\[(?P<pid>[0-9]+) \])?: )?"
file = /var/log/messages
file = /var/log/secure
file = /var/log/httpd/access_log
```

5) Add client to the system by run this command

```
prelude-admin register prelude-lml "idmef:w admin:r" IP_ADMIN-SERVER --
uid 0 --gid 0
```

```
(eg: prelude-admin register prelude-lml "idmef:w admin:r"
192.168.0.1 --uid 0 --gid 0)
```

**It will ask you to enter one-shot password provided from admin-server (please refer to the admin server configuration #6 before you proceed to the next step).

7) Start prelude-lml service by run this command

```
service prelude-lml start
```

Installation step at the server

6) Register client to the server by run this command

```
prelude-admin registration-server prelude-manager
```

**Use the password given for configuration #5 at the client-server.

Administration

Main Page

All of security events from network devices and application systems that MySurveillance monitors will be displayed at the MySurveillance Console, as shown in Figure 1.

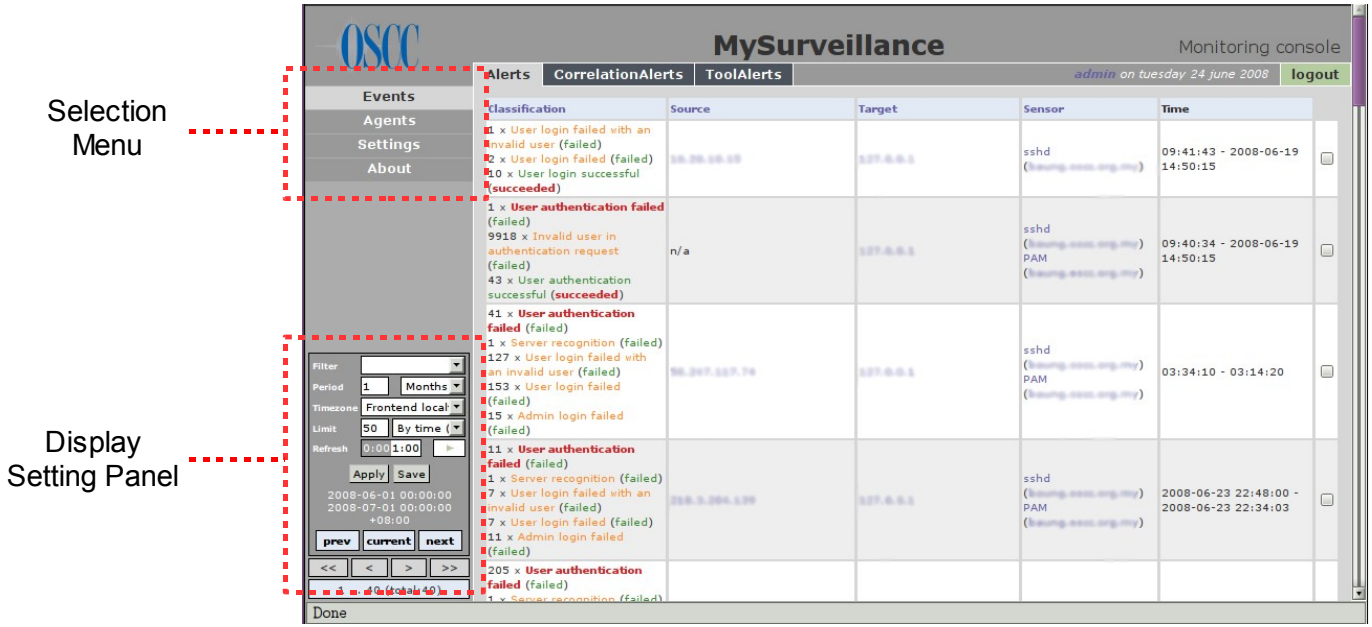


Figure 1 : MySurveillance Main Page

There are 4 menu selections can be chosen when you login into MySurveillance Console which are ***Events***, ***Agents***, ***Settings*** and ***About***. Some features that are available in the Display Setting panel are adjustable period for displaying reports, limitation to how many reports to be displayed in each page and refresh interval.

There are 3 pages to be display under Events which are ***Alert***, ***CorrelationAlert*** and ***ToolsAlert***. A double-click at the respective security event at the Classification column will open a different screen with detail information for the security event as shown in Figure 2.

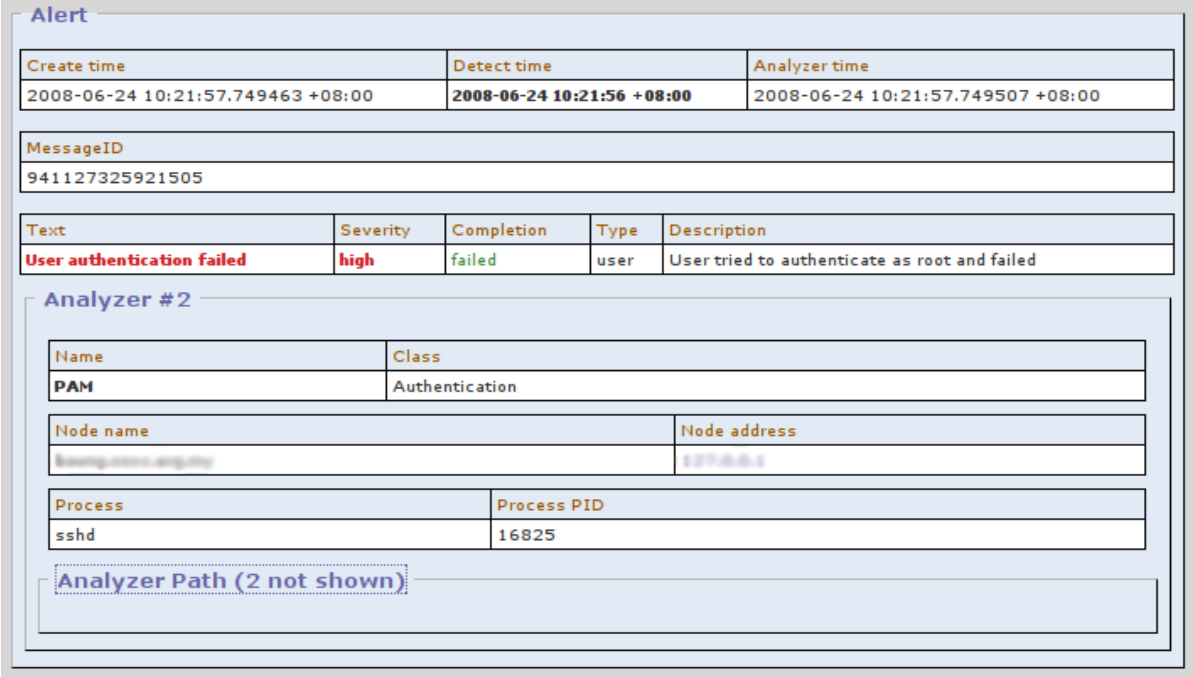


Figure 2 : Security Event Details

Agents page

Network devices or application systems that have been registered under MySurveillance system will be displayed at the Agent page. Sensors or agents will be grouped depending on the devices location. There are 2 colour codes used to refer to the availability of the sensors or agents at a particular time. Green refers to the availability of the sensors and red refers to the missing sensors.

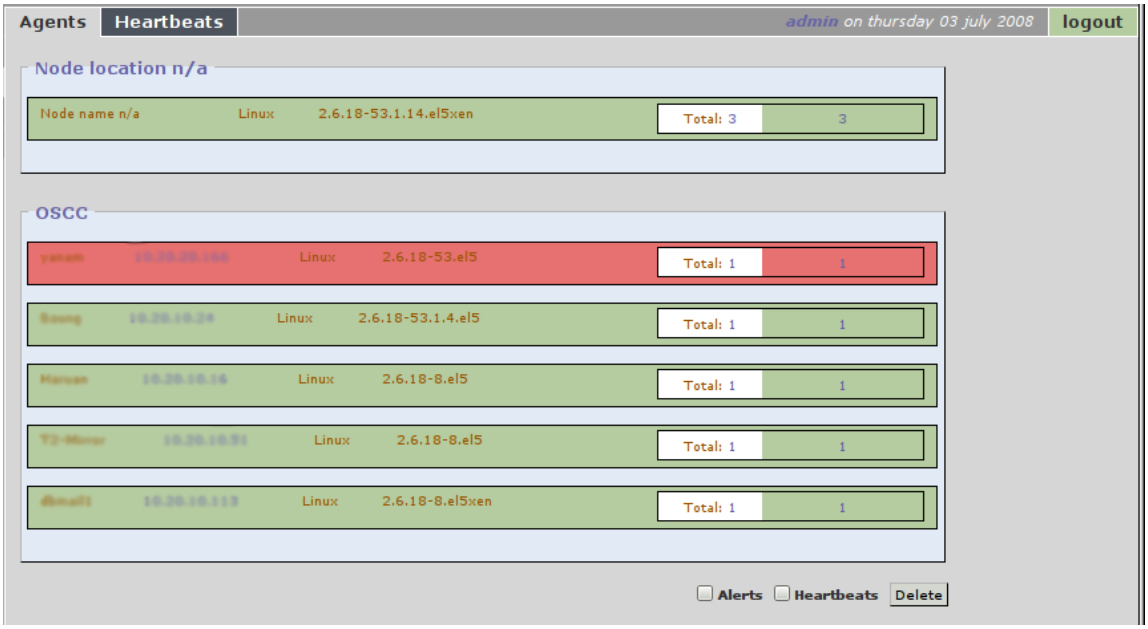
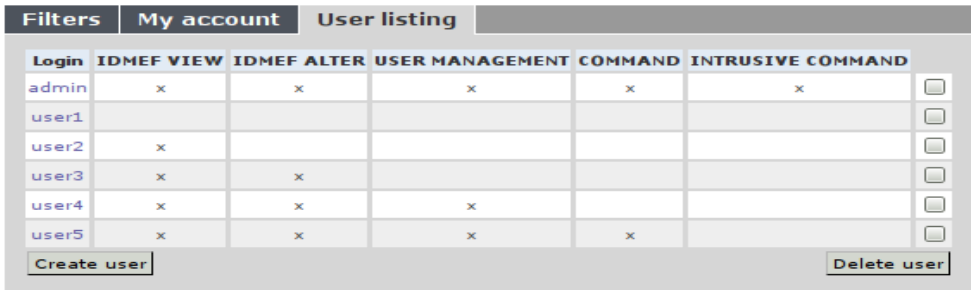


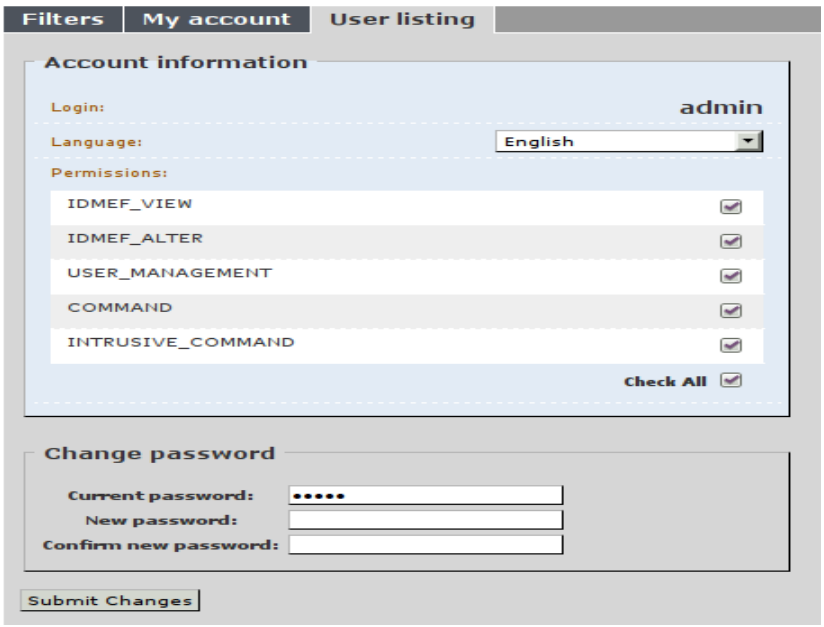
Figure 3 : Agents page

Change password

1. To change password, first click Settings on the left panel.
2. Next, click User listing as shown below. It will show a list of user accounts with its permissions.



3. Click on the required username in the Login column.
4. It will open up Account information for the user you had choose.

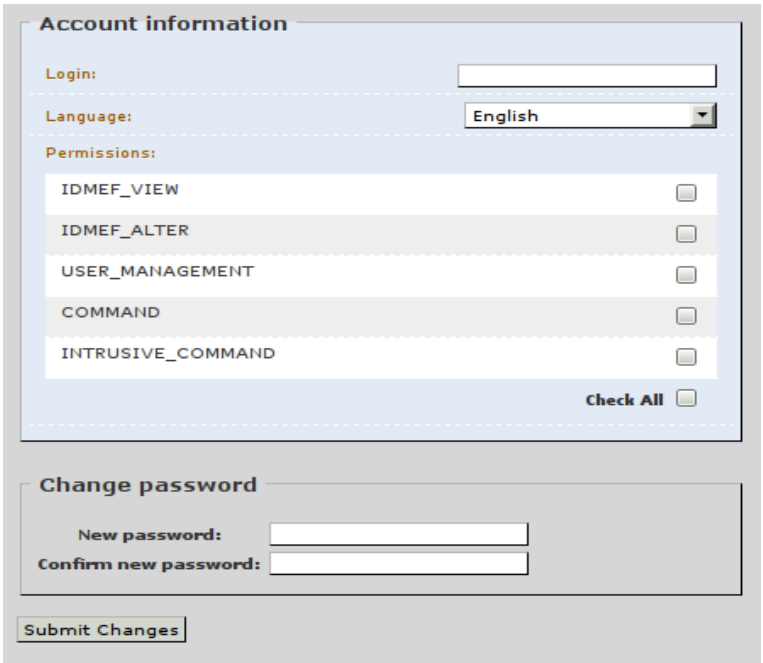


5. In the Change password section, fill in your Current password, New password and Confirm new password.
6. Click on Submit Changes to update you new password.

Add User

1. To add user, first click Settings on the left panel.
2. Next, click User listing as shown below. Click on button Create user.

3. Fill up the details for new user in the space provided. Specified permissions for the user at the Permissions box.



4. Click Submit Changes to update new user.

Maintenance

The following should be checked on a regular basis:

Network connections

The administrator should verify the server is reachable from the public network to avoid service interruption. Network monitoring is beyond the scope of these manual.

Log files

With the log files, it is possible to identify and monitor hardware and software problems on the servers. The log files should be checked at least once a week. All log files in /var/log/ directory.

Services

Used to start, stop or cancel a service on a local or remote computer. It is also a tool to set up recovery actions to take place if a service should fail. Should be checked in case of service failure.

```
#/etc/init.d/[service_name] start/stop/status
```

e.g:

```
#/etc/init.d/prelude-manager start
#/etc/init.d/ prelude-manager stop
#/etc/init.d/ prelude-manager status
```

Package update/patch

Check that the latest package update/patches has been installed on the servers. It should be checked and done at least once a month.

Disk Space

to verify that there is always enough space on the most mission critical servers. It should be done at least once a week. Use *df -h* command.

Password change

Password should be changed periodically, at least every three months.