MYSURVEILLANCE

Administration Manual

Version 1.1

OPEN SOURCE COMPETENCY CENTRE (OSCC) MAMPU

Level 3, APT E302-E304
Enterprise Building, Persiaran APEC
63000 Cyberjaya
Selangor
Tel: (6)03-8319 1200
Fax: (6)03-8319 3206
E-mail: helpdesk@oscc.org.my
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.

Complex and large organizations such as governmental agencies benefit from the flexibility that MySurveillance offers them. In Addition to being compatible with all security systems in the market, there are different configuration variations that are possible with MySurveillance such as filtering system and sensor error detection system with status reporting.

OBJECTIVES

The resources and features available in the MySurveillance would allow the Public Sector agencies to achieve the following objectives:

- To collect and analyze security event logs from various network and system devices.
- To centrally monitor overall network and system security.
- To identify critical security events rapidly and effectively.

FEATURES

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.

ARCHITECTURE

There are four major components 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.

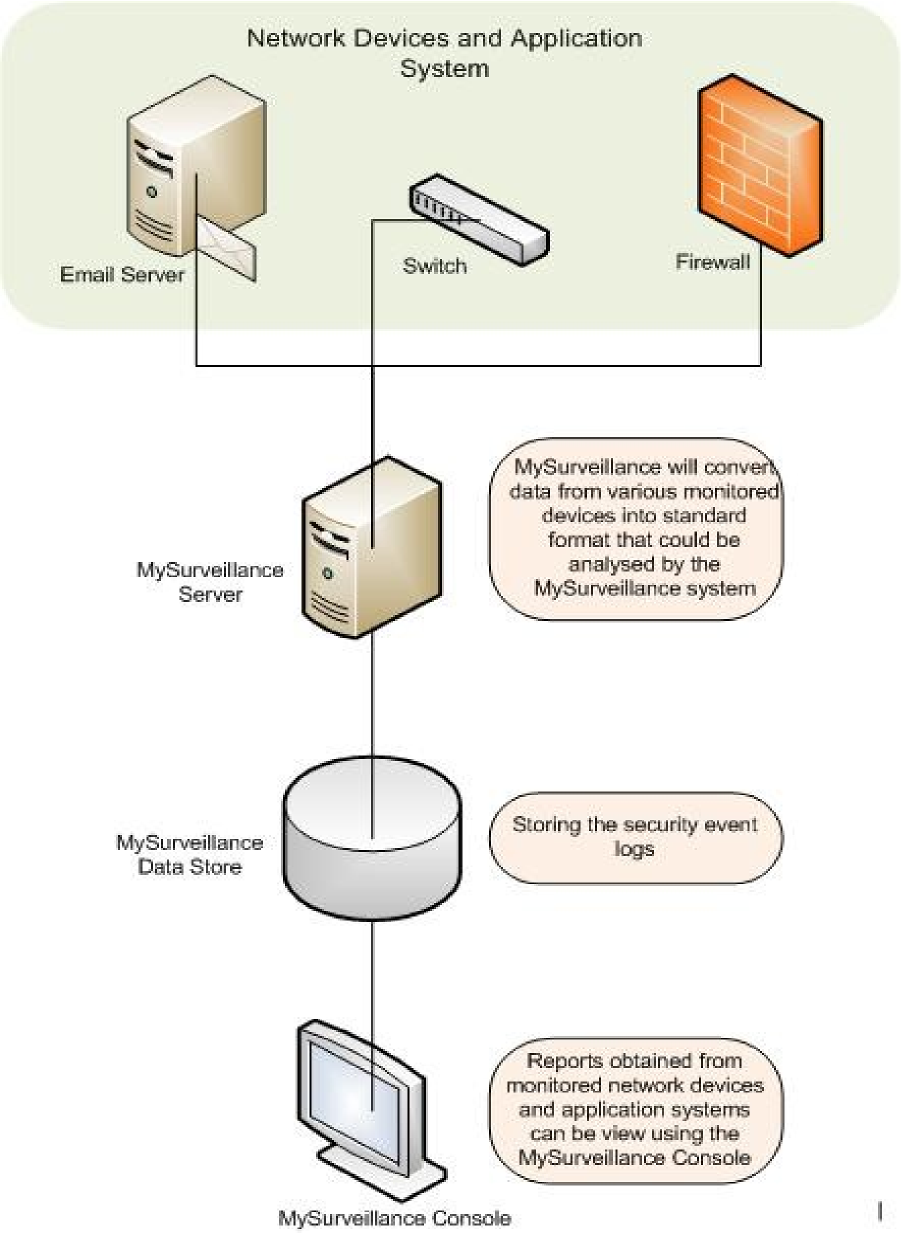

Network Devices and Application System
Email Server
Switch
Firewall
MySurveillance Server
MySurveillance will convert data from various monitored devices into standard format that could be analysed by the MySurveillance system
MySurveillance Data Store
Storing the security event logs
MySurveillance Console
Reports obtained from monitored network devices and application systems can be view using the MySurveillance Console

Figure 4.1 : Architecture Diagram

MySurveillance is compatible with various network and system devices in the market regardless whether it is proprietary or open source. Below are some examples of MySurveillance logs compatibility with various network and system devices.

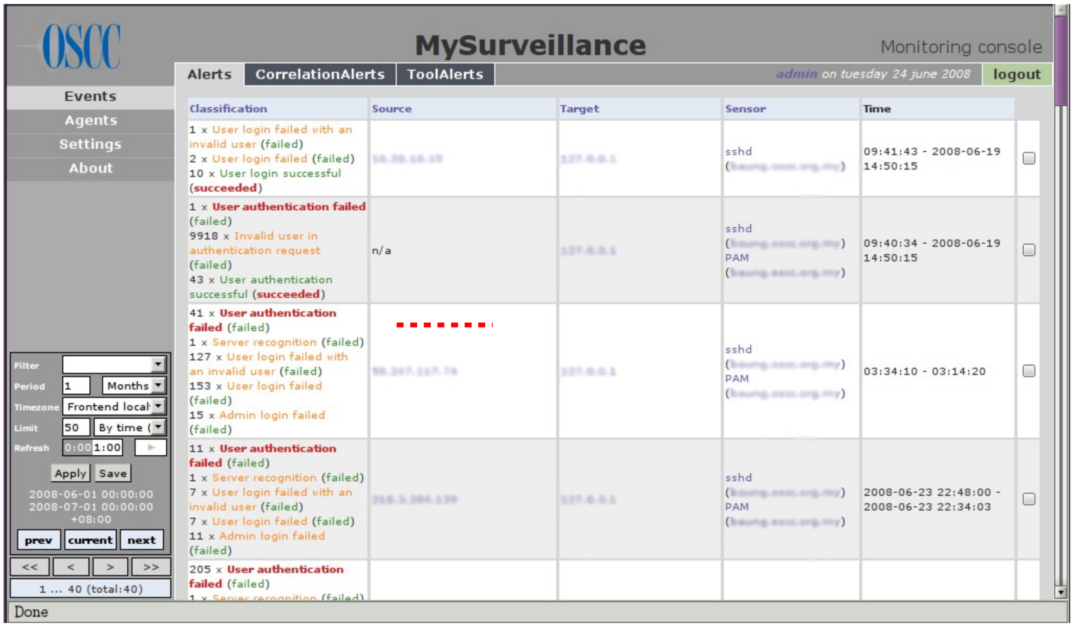
Firewall, Routers & VPN	BIG-IP®, Check Point®, CISCO® ASA, CISCO® IOS, CISCO® Router, CISCO® VPN, D-Link®, Ipchains, IpFw, Juniper Networks® NetScreen, Linksys® WAP11, ModSecurity®, Netfilter, SonicGuard SonicWall®
Switchs	CISCO® CSS
IDS	CISCO® IPS, Portsentry, Shadow, Tripwire®
Monitoring	APC®-EMU, ArpWatch, Dell® OpenManage, Nagios®
AntiVirus/AntiSpam	ClamAV®, P3Scan, SpamAssassin
Database	Microsoft® SQL Server, Oracle®
SMTP/POP Server	Exim, Postfix®, Qpopper®, Sendmail®, Vpopmail
FTP Server	ProFTPD, WU-FTPD
Web Server	Apache®
Vulnerability Scanner	Nessus®
Honeypots	Honeyd, Honeytrap, Kojoney
Authentication	OpenSSH
Applications	Asterisk, Cacti, Libsafe, Shadow Utils, Squid, Sudo
OS (security tools)	GrSecurity, PaX, SELinux
Miscellaneous	Unix® specific logs, Webmin, Windows® Server, Arbor, Linux® bonding, Microsoft® Cluster Service, NetApp® ONTAP®, NTSyslog, OpenHostAPD, Rishi, Suhosin

Table 4.1 : Logs Compatibility

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.



Filter:
Period: 1 Months
Timezone: Frontend local
Limit: 50 By time (
Refresh: 0:00 1:00

2008-06-01 00:00:00
2008-07-01 00:00:00
+08:00

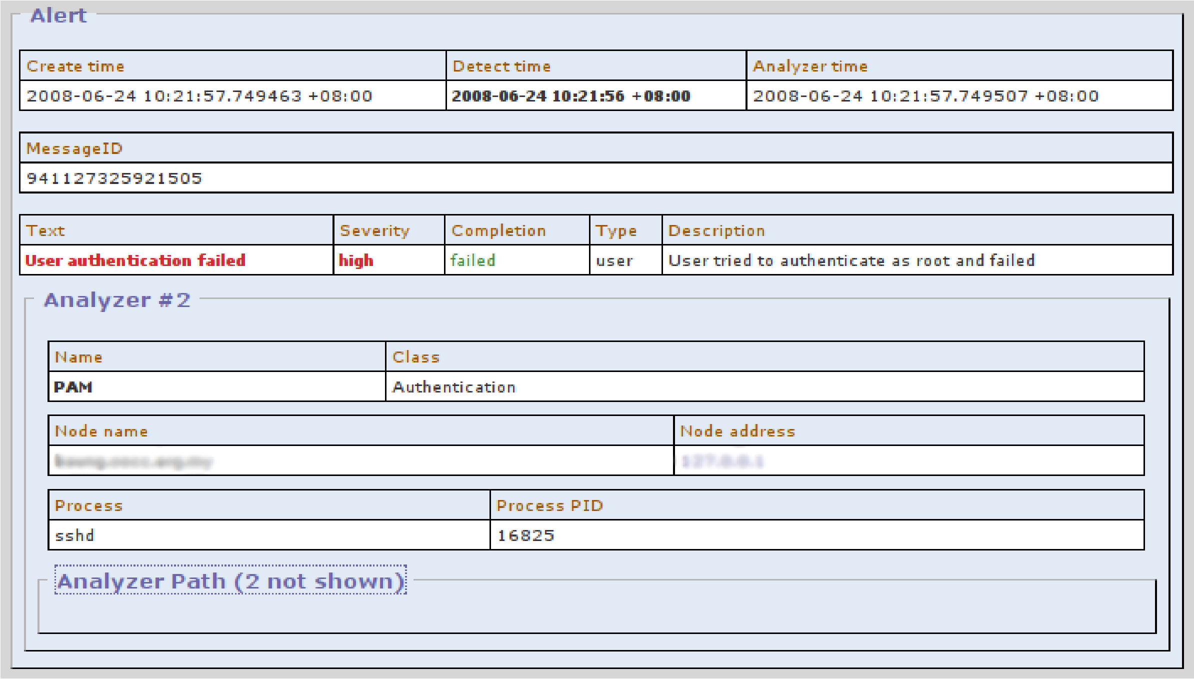
1 ... 40 (total:40)

Classification	Source	Target	Sensor	Time	
1 x User login failed with an invalid user (failed) 2 x User login failed (failed) 10 x User login successful (succeeded)	[redacted]	[redacted]	sshd ([redacted])	09:41:43 - 2008-06-19 14:50:15	□
1 x User authentication failed (failed) 9918 x Invalid user in authentication request (failed) 43 x User authentication successful (succeeded)	n/a	[redacted]	sshd ([redacted]) PAM ([redacted])	09:40:34 - 2008-06-19 14:50:15	□
41 x User authentication failed (failed) 1 x Server recognition (failed) 127 x User login failed with an invalid user (failed) 153 x User login failed (failed) 15 x Admin login failed (failed)	[redacted]	[redacted]	sshd ([redacted]) PAM ([redacted])	03:34:10 - 03:14:20	□
11 x User authentication failed (failed) 1 x Server recognition (failed) 7 x User login failed with an invalid user (failed) 7 x User login failed (failed) 11 x Admin login failed (failed)	[redacted]	[redacted]	sshd ([redacted]) PAM ([redacted])	2008-06-23 22:48:00 - 2008-06-23 22:34:03	□
205 x User authentication failed (failed) 1 x Server recognition (failed)					

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.



Alert

Create time	Detect time	Analyzer time
2008-06-24 10:21:57.749463 +08:00	**2008-06-24 10:21:56 +08:00**	2008-06-24 10:21:57.749507 +08:00

MessageID
941127325921505

Text	Severity	Completion	Type	Description
User authentication failed	**high**	failed	user	User tried to authenticate as root and failed

Analyzer #2

Name	Class
PAM	Authentication

Node name	Node address
[redacted]	[redacted]

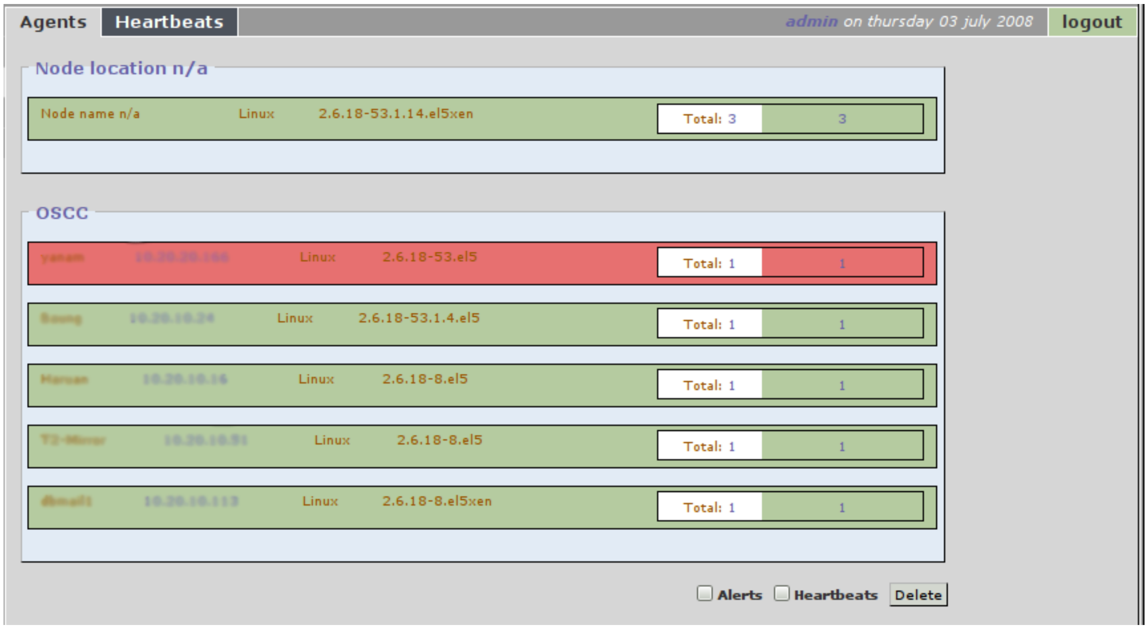
Process	Process PID
sshd	16825

Analyzer Path (2 not shown)

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.



Node location n/a

Node name n/a		Linux	2.6.18-53.1.14.el5xen	Total: 3 | 3

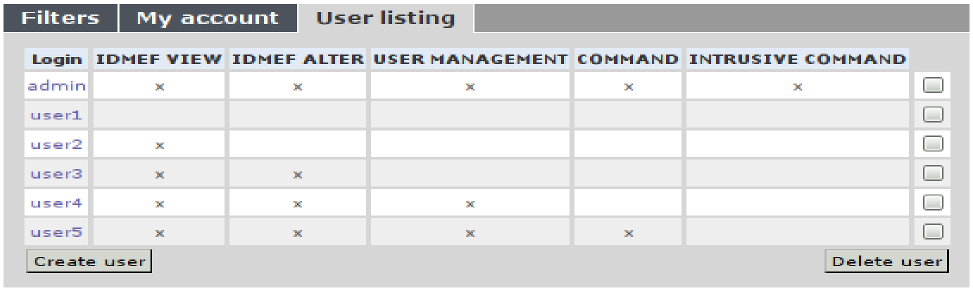
OSCC

[redacted]	[redacted]	Linux	2.6.18-53.el5	Total: 1 | 1
[redacted]	[redacted]	Linux	2.6.18-53.1.4.el5	Total: 1 | 1
[redacted]	[redacted]	Linux	2.6.18-8.el5	Total: 1 | 1
[redacted]	[redacted]	Linux	2.6.18-8.el5	Total: 1 | 1
[redacted]	[redacted]	Linux	2.6.18-8.el5xen	Total: 1 | 1

Figure 3 : Agents page

Change password

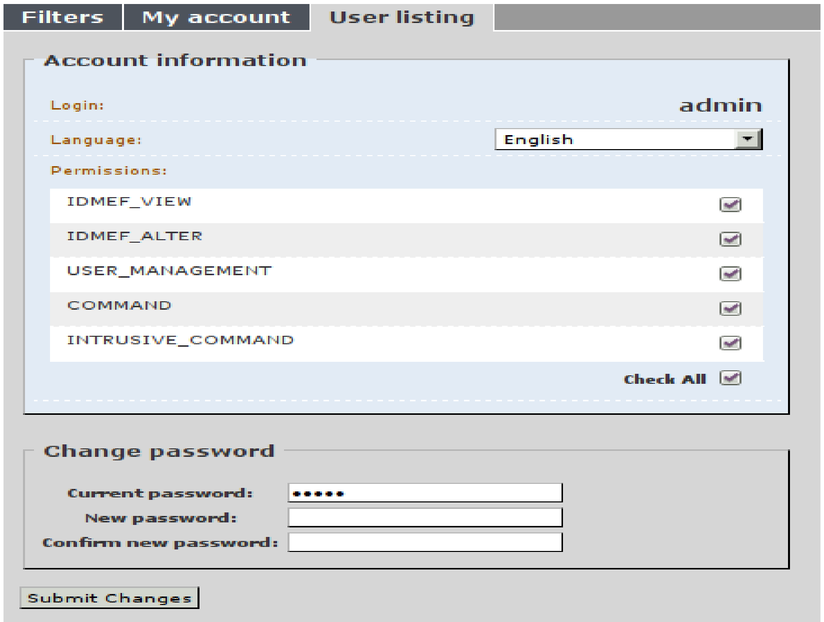
1. To change password, first click Settings on the left panel.
2. Next, click User listing as shown below. It will show a list of user accounts with its permissions.



Login	IDMEF VIEW	IDMEF ALTER	USER MANAGEMENT	COMMAND	INTRUSIVE COMMAND	
admin	x	x	x	x	x	□
user1						□
user2	x					□
user3	x	x				□
user4	x	x	x			□
user5	x	x	x	x		□

3. Click on the required username in the Login column.

4. It will open up Account information for the user you had choose.



Account information

Login: admin

Language: English

Permissions:

IDMEF_VIEW	☑
IDMEF_ALTER	☑
USER_MANAGEMENT	☑
COMMAND	☑
INTRUSIVE_COMMAND	☑
Check All	☑

Change password

Current password: ●●●●●

New password:

Confirm new password:

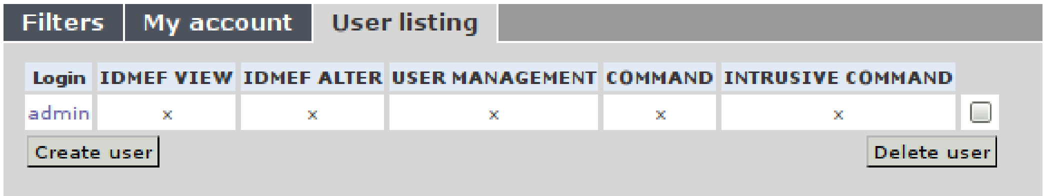
5. In the Change password section, fill in your Current password, New password and Confirm new password.

6. Click on Submit Changes to update you new password.

Add User

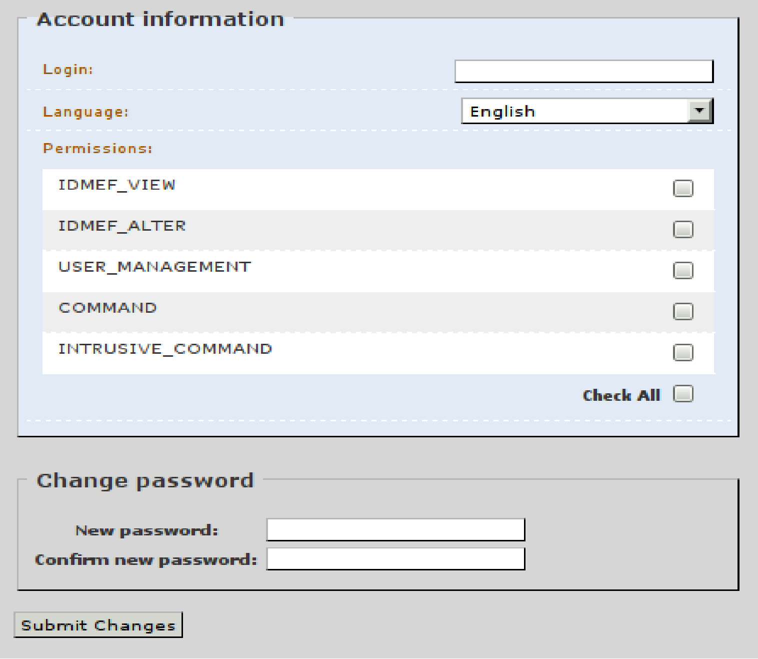
1. To add user, first click Settings on the left panel.

2. Next, click User listing as shown below. Click on button Create user.



Login	IDMEF VIEW	IDMEF ALTER	USER MANAGEMENT	COMMAND	INTRUSIVE COMMAND	
admin	x	x	x	x	x	□

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



Account information

Login:

Language: English

Permissions:

IDMEF_VIEW □
IDMEF_ALTER □
USER_MANAGEMENT □
COMMAND □
INTRUSIVE_COMMAND □

Check All □

Change password

New password:
Confirm new password:

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.

e.g: *#/etc/init.d/[service_name] start/stop/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 -lh* command.

Password change

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

Service update

Check for services update for the main components in MySurveillance such as libprelude, libpreludedb, prewikka and prelude_lml.