User Guide - eScan for Linux Desktop

I. Required eScan for Linux RPMS / Debian packages

RPM Package Name	File name
mwadmin	mwadmin-x.x-x.<linux distro><release>.i386.rpm
mwav	mwav-x.x-x.<linux distro><release>.i386.rpm
escan	escan-x.x-x.<linux distro><linux release>.i386.rpm

Debian Package Name	File name
mwadmin	mwadmin-x.x-x.<linux distro><release>.i386.deb
mwav	mwav-x.x-x.<linux distro><release>.i386.deb
escan	escan-x.x-x.<linux distro><linux release>.i386.deb

II. Installation

NOTE: The packages should be installed as per the order given below

Command Line Installation:

For RPM Packages:

```
# rpm -ivh  mwadmin-x.x-x.<linux distro><release>.i386.rpm

# rpm -ivh  mwav-x.x-x.<linux distro><release>.i386.rpm

# rpm -ivh   escan-x.x-x.<linux distro><linux release>.i386.rpm
```

For Debian packages:

```
# dpkg -i  mwadmin-x.x-x.<linux distro><release>.i386.deb

# dpkg -i  mwav-x.x-x.<linux distro><release>.i386.deb

# dpkg -i  escan-x.x-x.<linux distro><linux release>.i386.deb
```

III. Managing eScan for linux using the Web Administrator

(NOTE: Browser supported is Firefox).

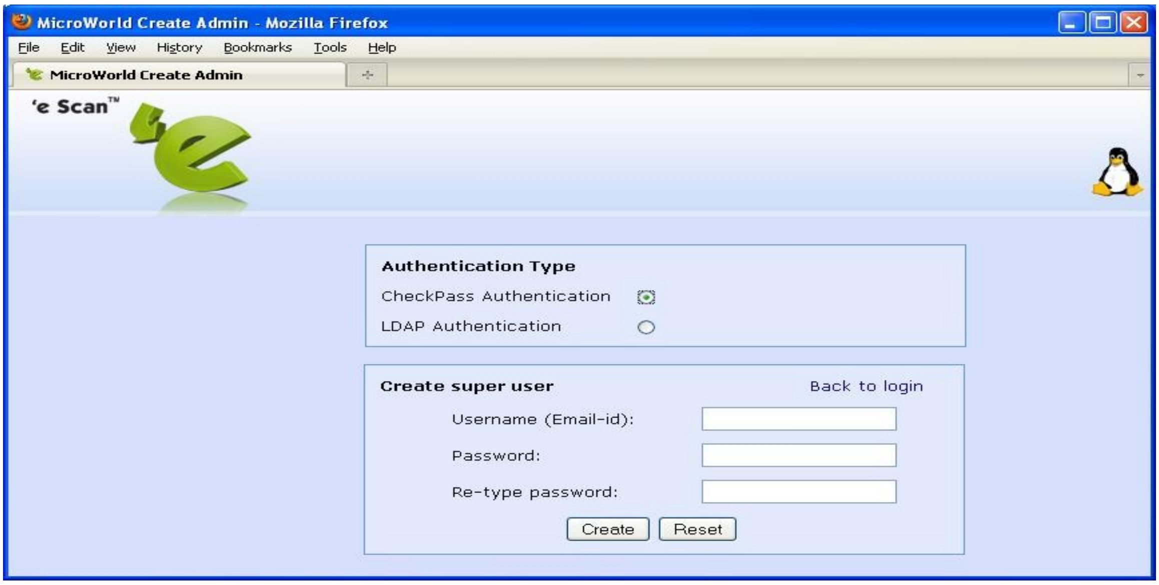
a) To login to the Web Administration using the Hypertext Transfer Protocol Secure (HTTPS)

https://<eScan_Server_IP_address>:10443

b) On first time login, there are two ways of Authentication types.

- CheckPass Authentication – Selecting this option shall enable to create a Super User in database. Once created, login to the Web-administration by clicking on Back to Login option. **(Refer Fig.1).**

  Username should be in the EMAIL-ID format i.e. username@domain.com


MicroWorld Create Admin - Mozilla Firefox
File Edit View History Bookmarks Tools Help
MicroWorld Create Admin
'e Scan™

Authentication Type

CheckPass Authentication ●

LDAP Authentication ○

Create super user Back to login

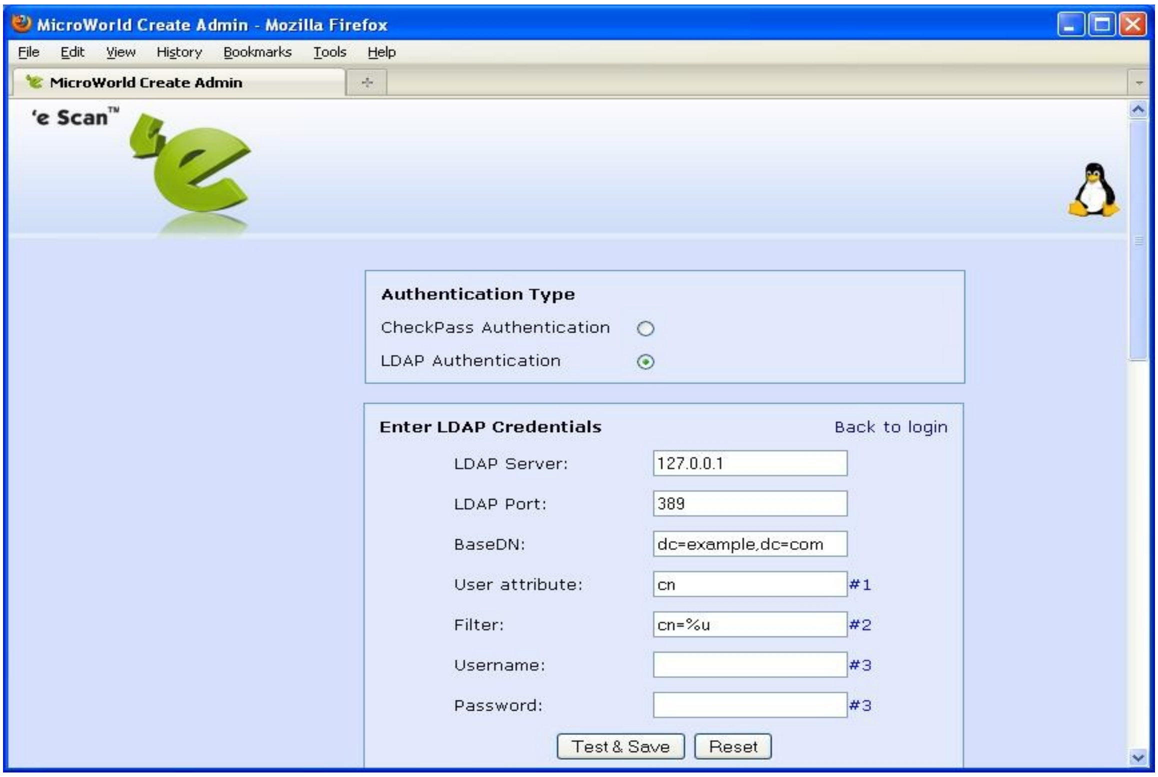
Username (Email-id):

Password:

Re-type password:

Fig.1

- LDAP Authentication : Selecting this option shall configure the Web-Administration of the eScan using the LDAP server in the network to authenticate the login. For more information check **Preferences in this document.**
  Once configured click on Test & Save button **(Refer Fig.2)**. If the Authentication by the LDAP server is successful, the credentials will be saved. Then click on Back to Login option to login to the WebScan Administration using the LDAP User


MicroWorld Create Admin - Mozilla Firefox
File Edit View History Bookmarks Tools Help
MicroWorld Create Admin
'e Scan™
Back to login
Test & Save
Reset

Authentication Type

CheckPass Authentication ○

LDAP Authentication ●

Enter LDAP Credentials

LDAP Server: 127.0.0.1

LDAP Port: 389

BaseDN: dc=example,dc=com

User attribute: cn #1

Filter: cn=%u #2

Username: #3

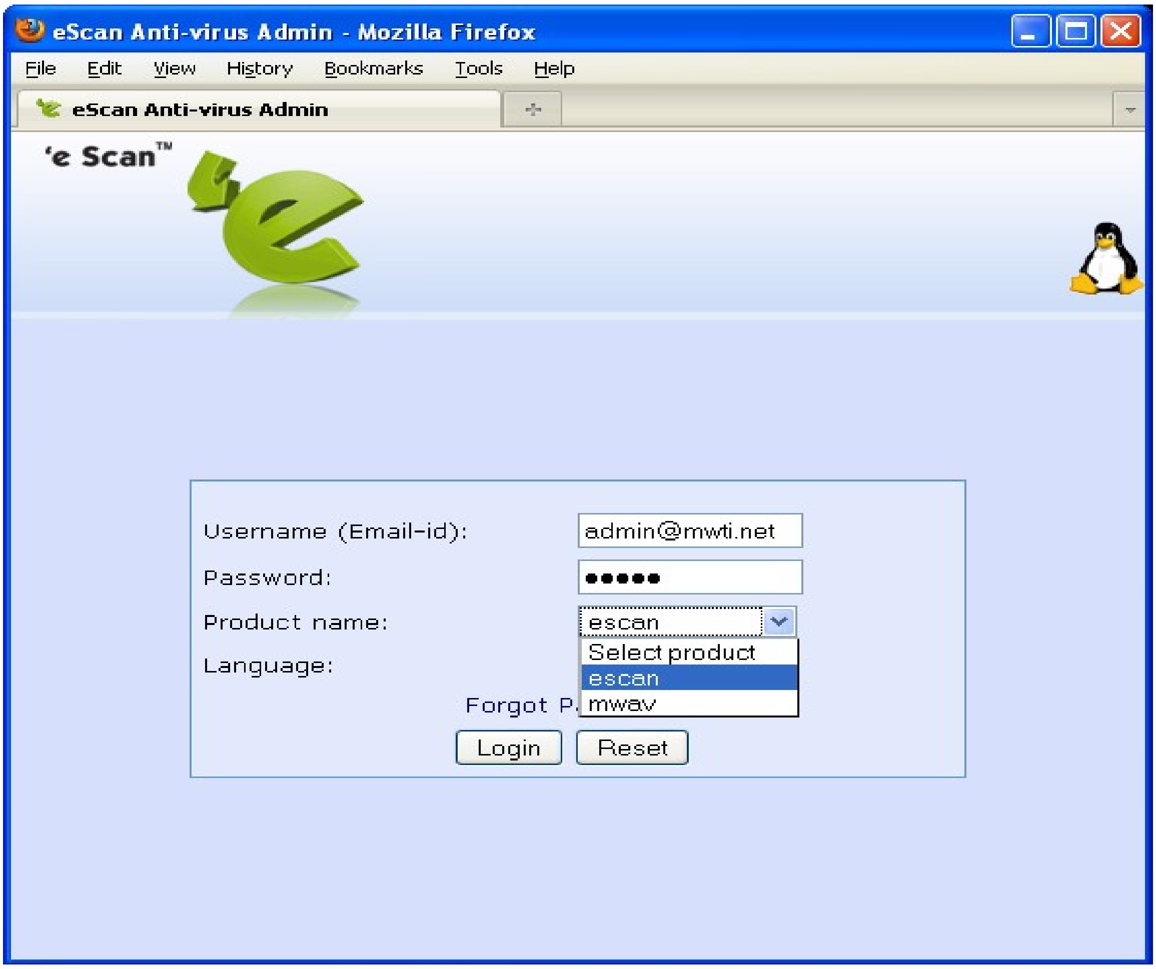
Password: #3

Fig.2

- **MANAGING eScan AV FROM THE WEB ADMINISTRATOR:**

1) To access the eScan AV settings, select **eScan** in the list of Product-Name drop down box.

2) Login to the Web Administrator using the Super User email id and password.



eScan Anti-virus Admin - Mozilla Firefox
File Edit View History Bookmarks Tools Help
eScan Anti-virus Admin
'e Scan™
Select product
escan
mwav
Forgot P
Login
Reset

Username (Email-id): admin@mwti.net

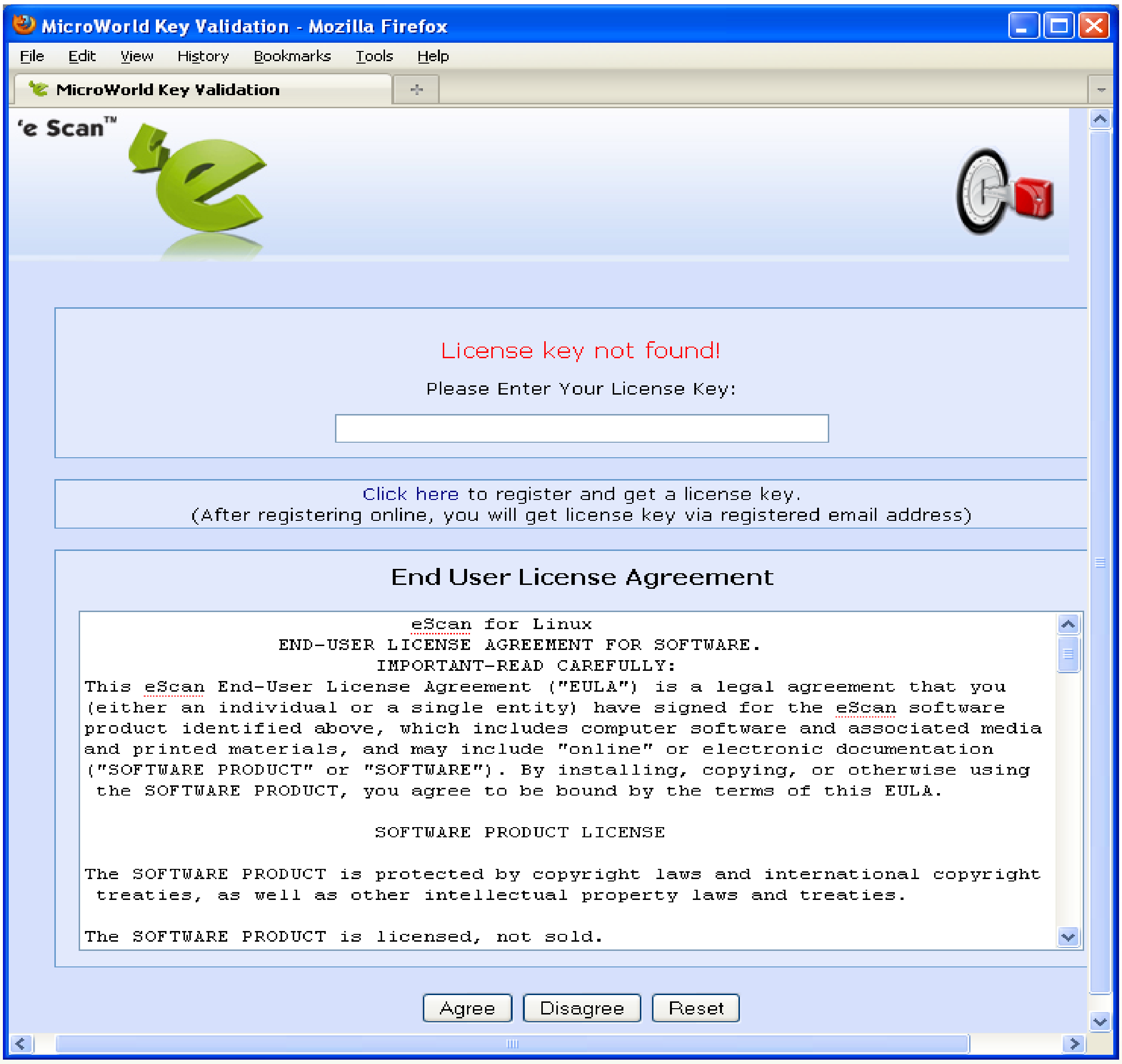
Password: ●●●●●

Product name: escan

Language:

Fig.3

3) This will open the field to enter the License Key with the EULA page. Apply the eScan License key provided to you. For evaluation, select the “Click here to register and get a license key”. This will be taken to the official web-site whereing you have to fill up the required details and submit. A license key will then be emailed to the registered email id. Apply the same in the field for License Key.


MicroWorld Key Validation - Mozilla Firefox
File Edit View History Bookmarks Tools Help
MicroWorld Key Validation
'e Scan™

License key not found!

Please Enter Your License Key:

Click here to register and get a license key.
(After registering online, you will get license key via registered email address)

End User License Agreement

```
                         eScan for Linux
                END-USER LICENSE AGREEMENT FOR SOFTWARE.
                        IMPORTANT-READ CAREFULLY:
This eScan End-User License Agreement ("EULA") is a legal agreement that you
(either an individual or a single entity) have signed for the eScan software
product identified above, which includes computer software and associated media
and printed materials, and may include "online" or electronic documentation
("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using
 the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA.

                        SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright
 treaties, as well as other intellectual property laws and treaties.

The SOFTWARE PRODUCT is licensed, not sold.
```

Fig.4

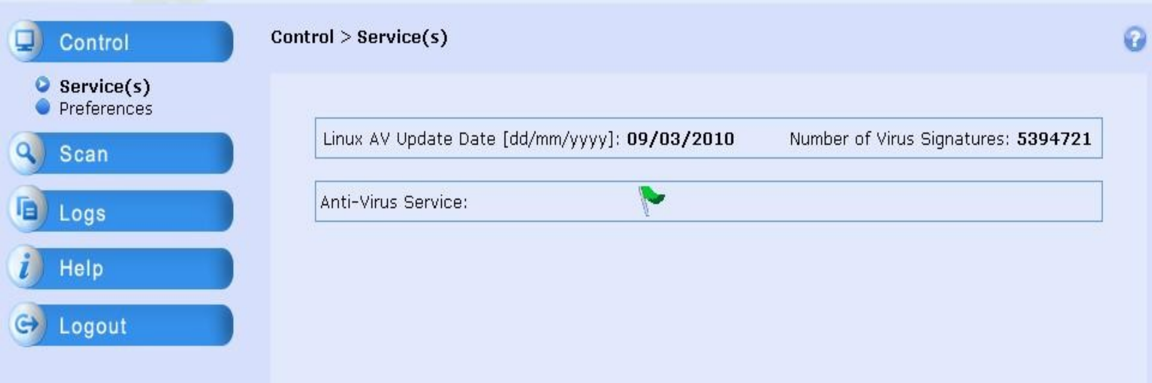
4) The Welcome Screen displayed after applying the eScan License Key.

5) Features and Options in eScan AV:

a) Control > Services

Displays the MicroWorld Anti-virus database update status, AV Service status.

- Services running is indicated with a Green Flag.
- Services stopped is indicated with a Red Flag.



Control > Service(s)

Linux AV Update Date [dd/mm/yyyy]: **09/03/2010** Number of Virus Signatures: **5394721**

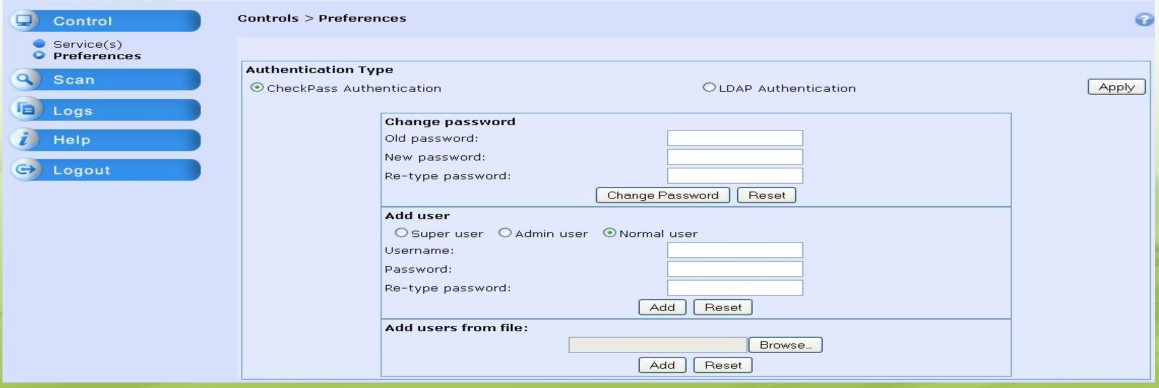
Anti-Virus Service: 🟩

Fig.5

b) Control > Preferences : In this section, Web-Console login credentials can be set either using the CheckPass or LDAP Authentication type.

CheckPass Authentication: Selecting this authentication, will create user database to enable login. Admin password can be changed, new users can be added.
The type of users that can be created are Super user and Admin user. Normal user types are not available for eScan for Linux Desktop.

- Super users can access both the eScan AV module and the MWAV module from the Webscan Administrator.
- Admin users can access the particular module in which they are created. For eg. A normal user created in the eScan module can access only the eScan Module and not the MWAV module in the Web Administrator.



Controls > Preferences

Authentication Type

● CheckPass Authentication ○ LDAP Authentication

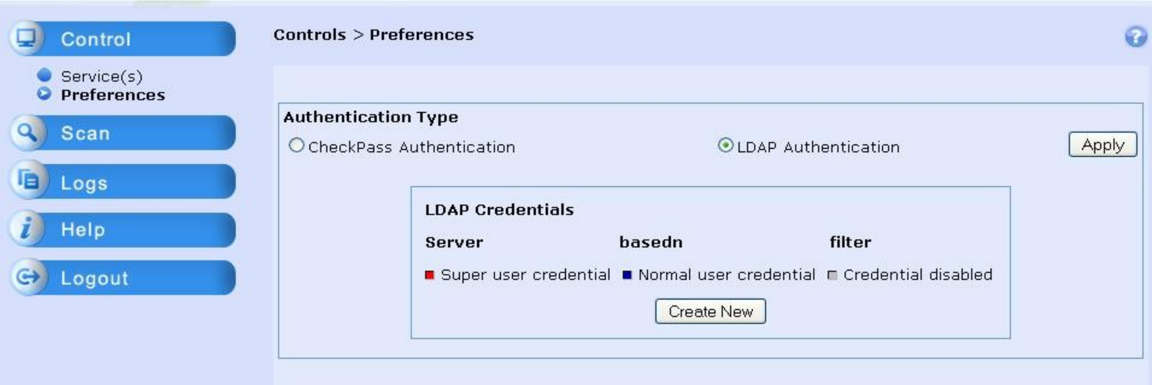
Change password
Old password:
New password:
Re-type password:

Add user
○ Super user ○ Admin user ● Normal user
Username:
Password:
Re-type password:

Add users from file:

Fig.6

LDAP Authentication: Selecting this authentication shall configure the Web-Administration of the eScan using the LDAP server in the network to authenticate the login.



Controls > Preferences

Authentication Type

○ CheckPass Authentication ● LDAP Authentication [Apply]

LDAP Credentials

Server	basedn	filter

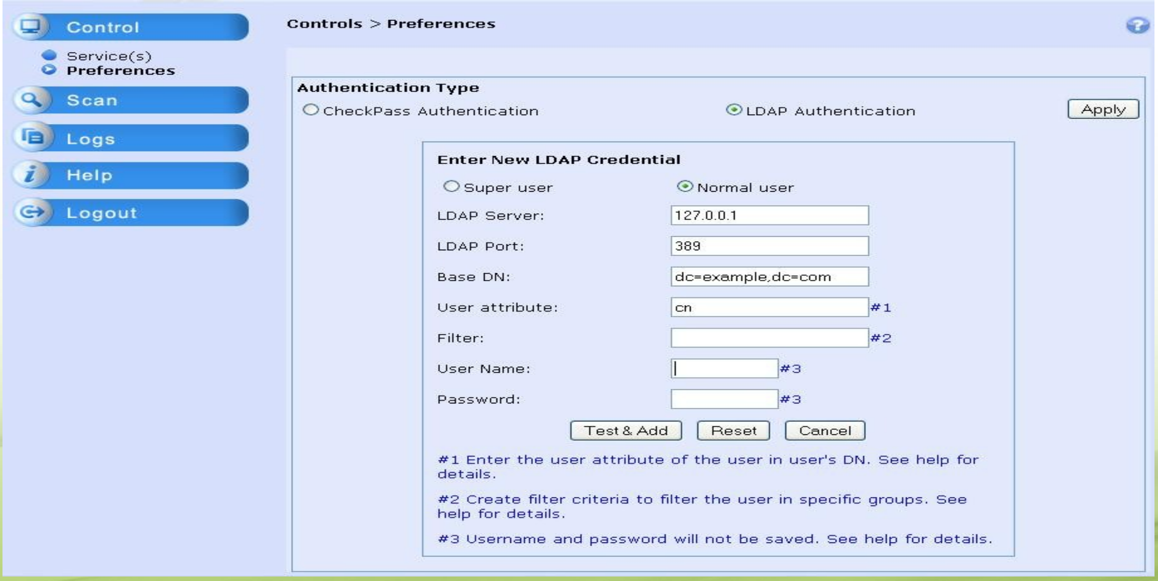
🟥 Super user credential 🟦 Normal user credential ▨ Credential disabled

[Create New]

Fig.7

To enable the Web-Admin login using the LDAP Authentication,

1. Click on the Create New button,
2. Enter the new LDAP credentials (refer fig.8) in the fields provided,
3. Select Super user option and enter the LDAP server ip address and the LDAP port,
4. Enter the base disitinguished name (Base DN),
5. Enter User attribute to search in the user DN in which the user name will be searched.
6. Filter field is optional. It is useful, if only users of specific groups should be allowed to login to eScan Web-Admin.
7. Enter the user and password to test and validate the LDAP authentication.
8. Click on Test & Add button.
9. If the Ldap settings are successfully authenticated, the credentials will be added (refer fig.9). Then click on the Apply button to enable the LDAP Authentication.



Controls > Preferences

Authentication Type

○ CheckPass Authentication ● LDAP Authentication [Apply]

Enter New LDAP Credential

○ Super user ● Normal user

LDAP Server:	127.0.0.1
LDAP Port:	389
Base DN:	dc=example,dc=com
User attribute:	cn #1
Filter:	#2
User Name:	#3
Password:	#3

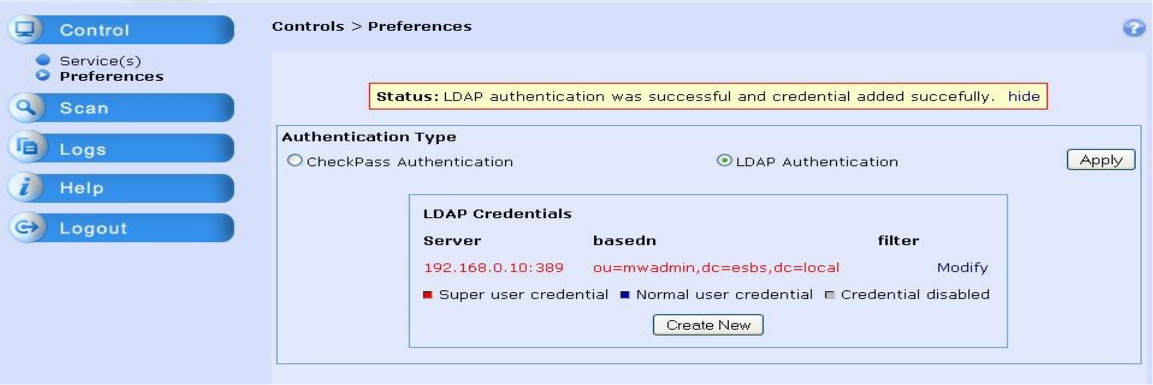
[Test & Add] [Reset] [Cancel]

#1 Enter the user attribute of the user in user's DN. See help for details.

#2 Create filter criteria to filter the user in specific groups. See help for details.

#3 Username and password will not be saved. See help for details.

Fig.8



Controls > Preferences

Status: LDAP authentication was successful and credential added succefully. hide

Authentication Type

○ CheckPass Authentication ● LDAP Authentication [Apply]

LDAP Credentials

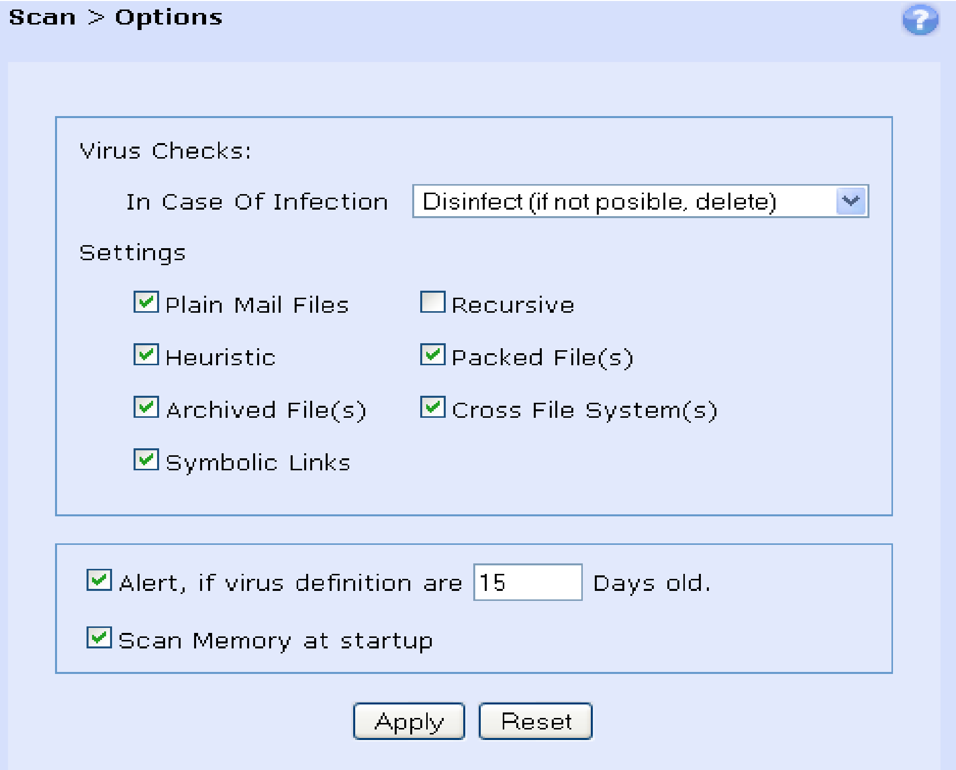
Server	basedn	filter
192.168.0.10:389	ou=mwadmin,dc=esbs,dc=local	Modify

🟥 Super user credential ■ Normal user credential □ Credential disabled

[Create New]

Fig.9

c) Scan > Options: In this section, the default action scan options can be set for **On Demand Virus Scanning** i.e. Manual Virus scanning of the system. Also, here it allows you to set the option to alert for outdated AV database.



Scan > Options

Virus Checks:

In Case Of Infection: Disinfect (if not posible, delete)

Settings

☑ Plain Mail Files ☐ Recursive

☑ Heuristic ☑ Packed File(s)

☑ Archived File(s) ☑ Cross File System(s)

☑ Symbolic Links

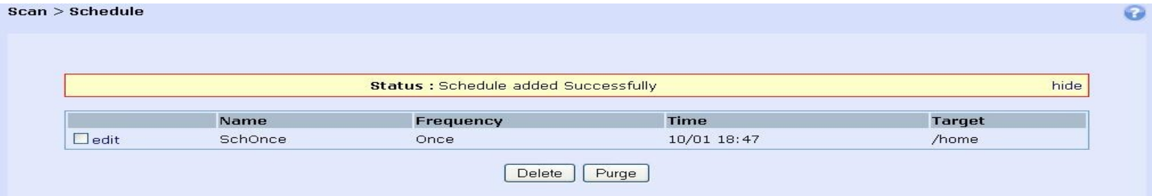
☑ Alert, if virus definition are 15 Days old.

☑ Scan Memory at startup

Fig.10

d) Scan > Schedule : In this section, a schedule can be set for auto-scan of the system at a specified date and time. This ensures a periodic scanning is carried out.

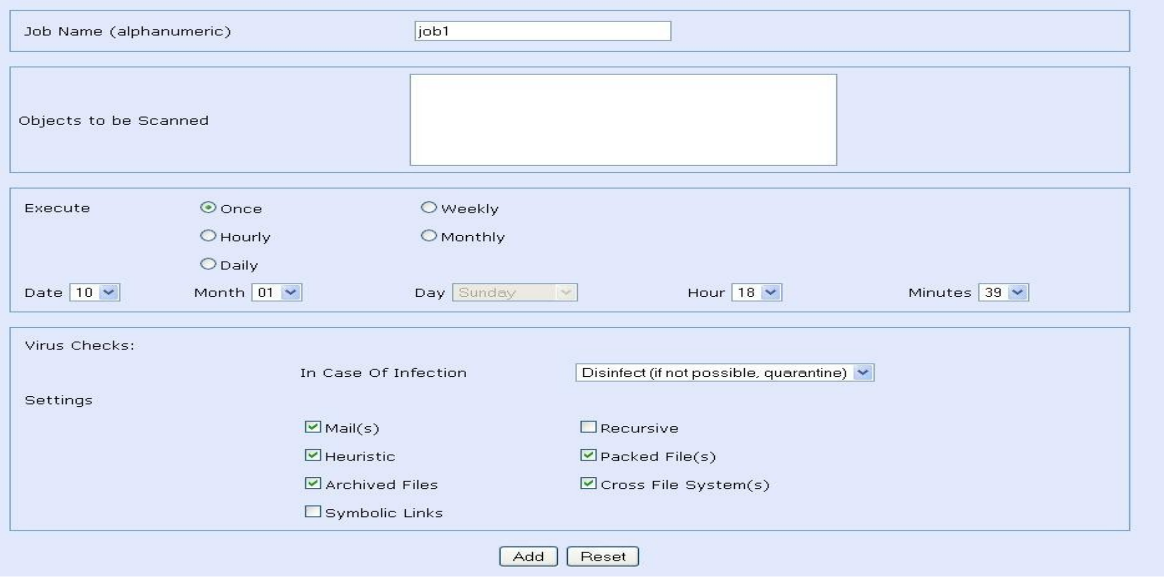
A list of schedules, already created is displayed in the top list box. Schedule name, time when it should start, when it is next due. User can delete the existing schedule by selecting the schedule and choosing Delete.



Status : Schedule added Successfully

	Name	Frequency	Time	Target
□ edit	SchOnce	Once	10/01 18:47	/home

Fig.11



Job Name (alphanumeric): job1

Objects to be Scanned:

Execute: ● Once ○ Weekly ○ Hourly ○ Monthly ○ Daily

Date 10 Month 01 Day Sunday Hour 18 Minutes 39

Virus Checks:

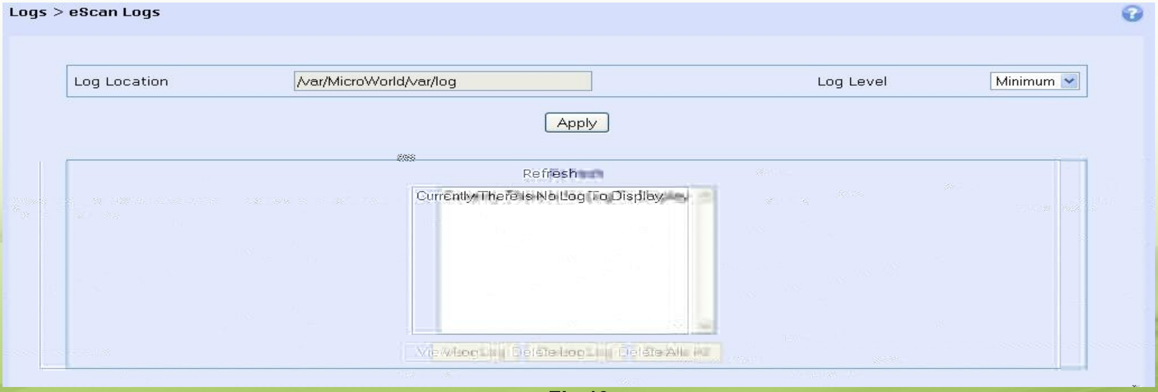
In Case Of Infection: Disinfect (if not possible, quarantine)

Settings

☑ Mail(s) □ Recursive
☑ Heuristic ☑ Packed File(s)
☑ Archived Files ☑ Cross File System(s)
□ Symbolic Links

Fig.12

e) Logs > eScan Logs: In this section, you can set the log related settings and to view a previous log of eScan activity as well as to clear previous log(s).



Log Location: /var/MicroWorld/var/log

Log Level: Minimum

Currently There Is No Log To Display

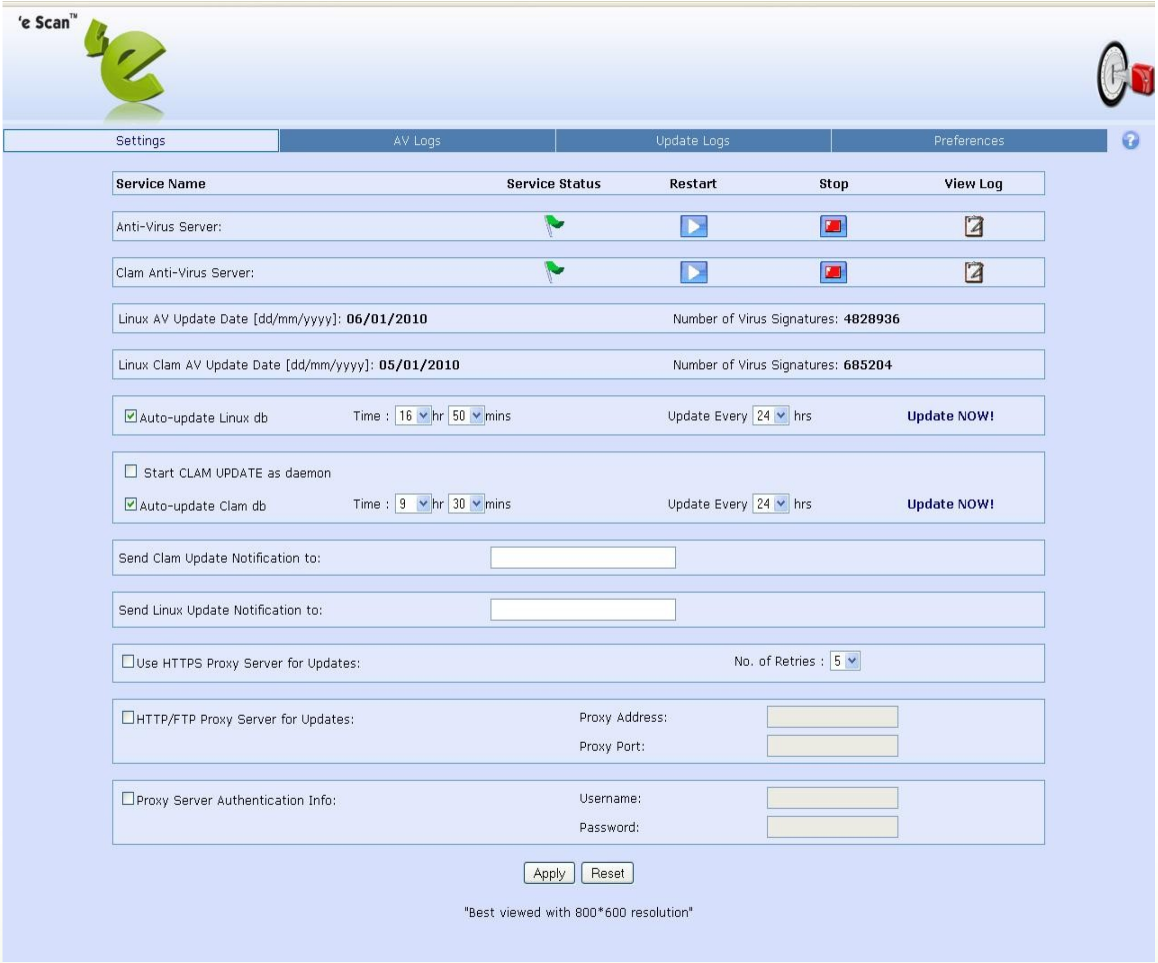
Fig.13

- **MANAGING MWAV FROM THE Web ADMINISTRATOR:**

1) To access the eScan AV settings, select **MWAV** in the list of Product-Name drop down box.

2) Login to the Web Administrator using the Super User email id and password

3) This screen specifies Server Status, and Settings to schedule the download of updates for MWAV for Linux and Clam AV for Linux.



Service Name	Service Status	Restart	Stop	View Log
Anti-Virus Server:	⚑	▶	■	📝
Clam Anti-Virus Server:	⚑	▶	■	📝

Linux AV Update Date [dd/mm/yyyy]: **06/01/2010** Number of Virus Signatures: **4828936**

Linux Clam AV Update Date [dd/mm/yyyy]: **05/01/2010** Number of Virus Signatures: **685204**

☑ Auto-update Linux db Time : 16 hr 50 mins Update Every 24 hrs **Update NOW!**

☐ Start CLAM UPDATE as daemon

☑ Auto-update Clam db Time : 9 hr 30 mins Update Every 24 hrs **Update NOW!**

Send Clam Update Notification to:

Send Linux Update Notification to:

☐ Use HTTPS Proxy Server for Updates: No. of Retries : 5

☐ HTTP/FTP Proxy Server for Updates: Proxy Address: Proxy Port:

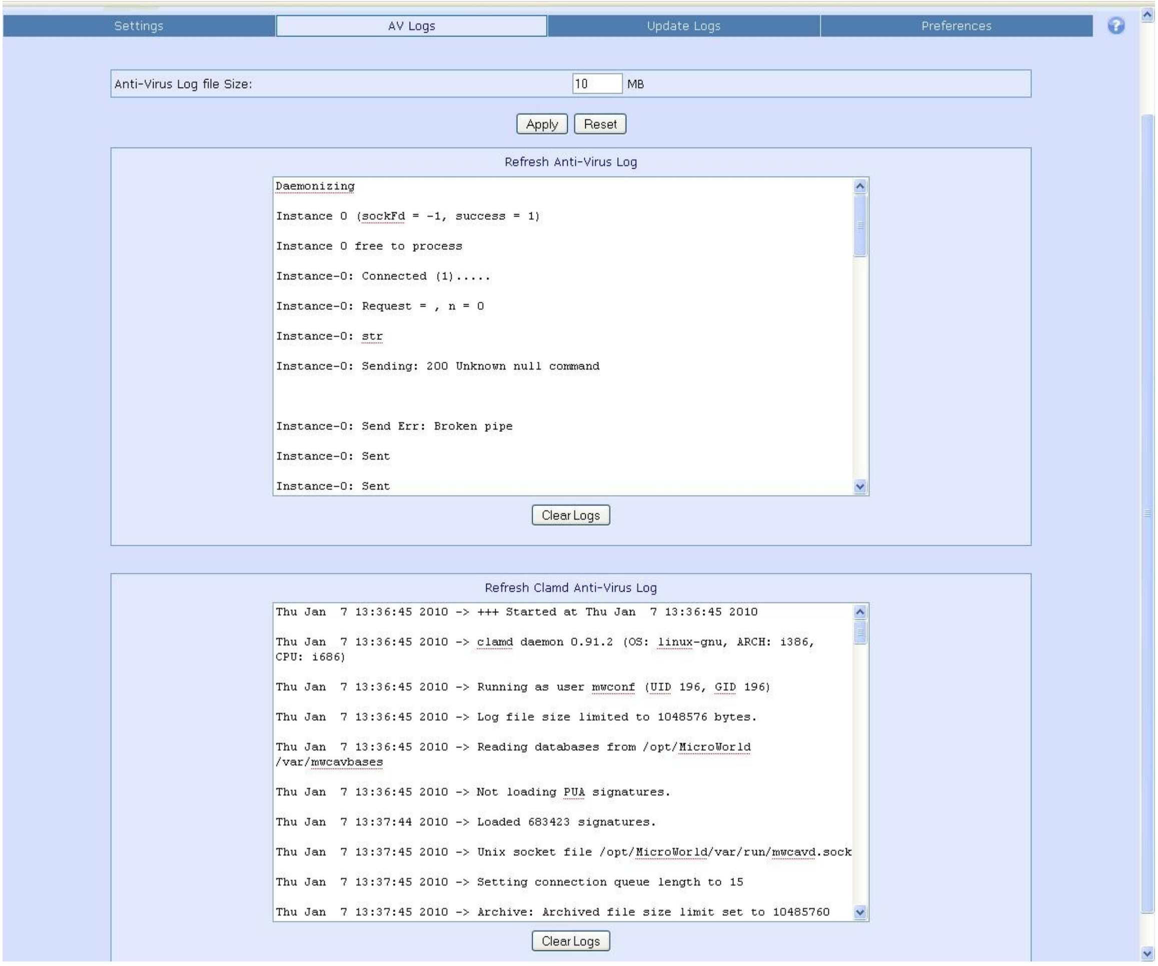
☐ Proxy Server Authentication Info: Username: Password:

"Best viewed with 800*600 resolution"

Fig.14

4) AV Logs

This section will display the logs of the AV services



Anti-Virus Log file Size: 10 MB

Refresh Anti-Virus Log

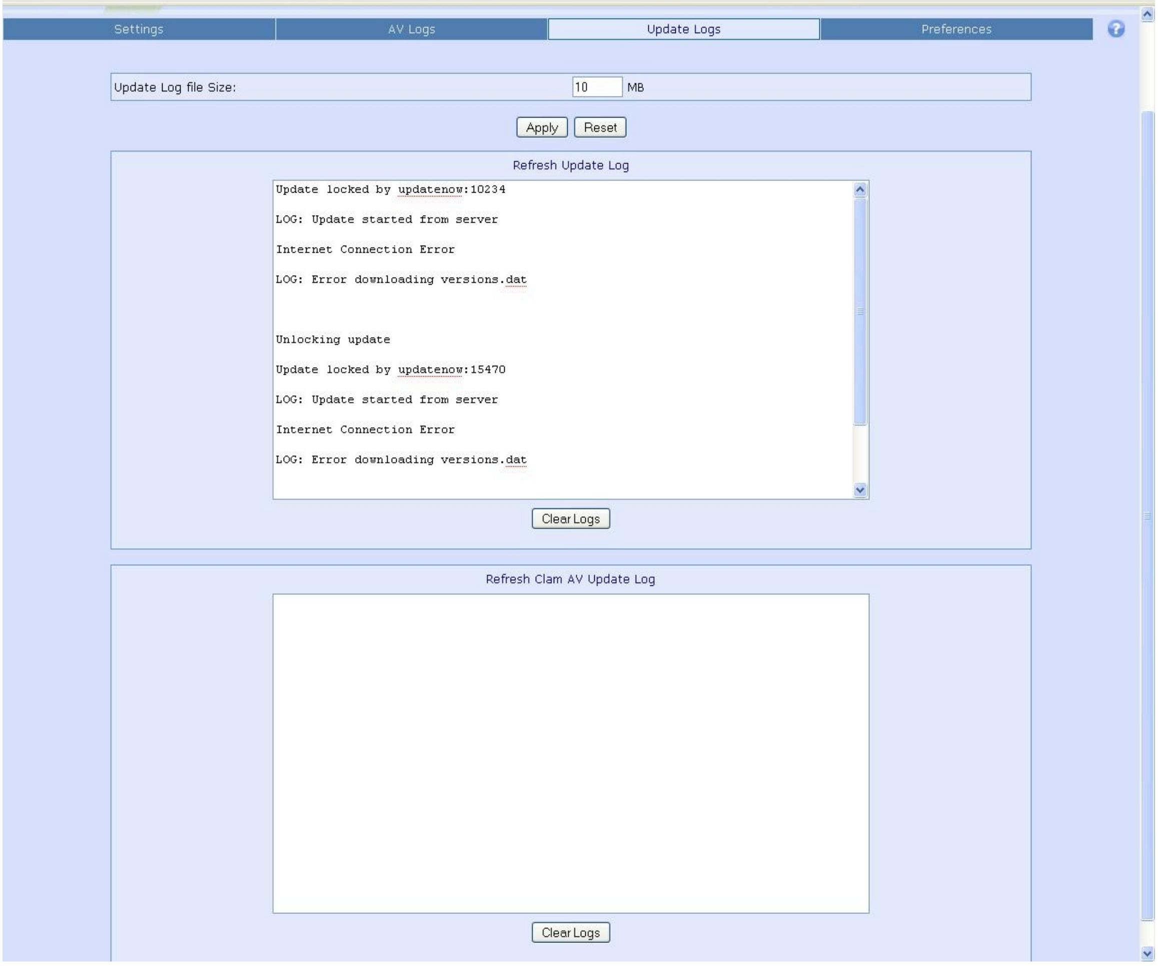
```
Daemonizing

Instance 0 (sockFd = -1, success = 1)

Instance 0 free to process

Instance-0: Connected (1).....

Instance-0: Request = , n = 0

Instance-0: str

Instance-0: Sending: 200 Unknown null command


Instance-0: Send Err: Broken pipe

Instance-0: Sent

Instance-0: Sent
```

Refresh Clamd Anti-Virus Log

```
Thu Jan  7 13:36:45 2010 -> +++ Started at Thu Jan  7 13:36:45 2010

Thu Jan  7 13:36:45 2010 -> clamd daemon 0.91.2 (OS: linux-gnu, ARCH: i386,
CPU: i686)

Thu Jan  7 13:36:45 2010 -> Running as user mwconf (UID 196, GID 196)

Thu Jan  7 13:36:45 2010 -> Log file size limited to 1048576 bytes.

Thu Jan  7 13:36:45 2010 -> Reading databases from /opt/MicroWorld
/var/mwcavbases

Thu Jan  7 13:36:45 2010 -> Not loading PUA signatures.

Thu Jan  7 13:37:44 2010 -> Loaded 683423 signatures.

Thu Jan  7 13:37:45 2010 -> Unix socket file /opt/MicroWorld/var/run/mwcavd.sock

Thu Jan  7 13:37:45 2010 -> Setting connection queue length to 15

Thu Jan  7 13:37:45 2010 -> Archive: Archived file size limit set to 10485760
```

Fig.15

5) Update Logs: This section will display the logs of the AV update database.



Update Log file Size: 10 MB

Refresh Update Log

```
Update locked by updatenow:10234

LOG: Update started from server

Internet Connection Error

LOG: Error downloading versions.dat


Unlocking update

Update locked by updatenow:15470

LOG: Update started from server

Internet Connection Error

LOG: Error downloading versions.dat
```

Refresh Clam AV Update Log

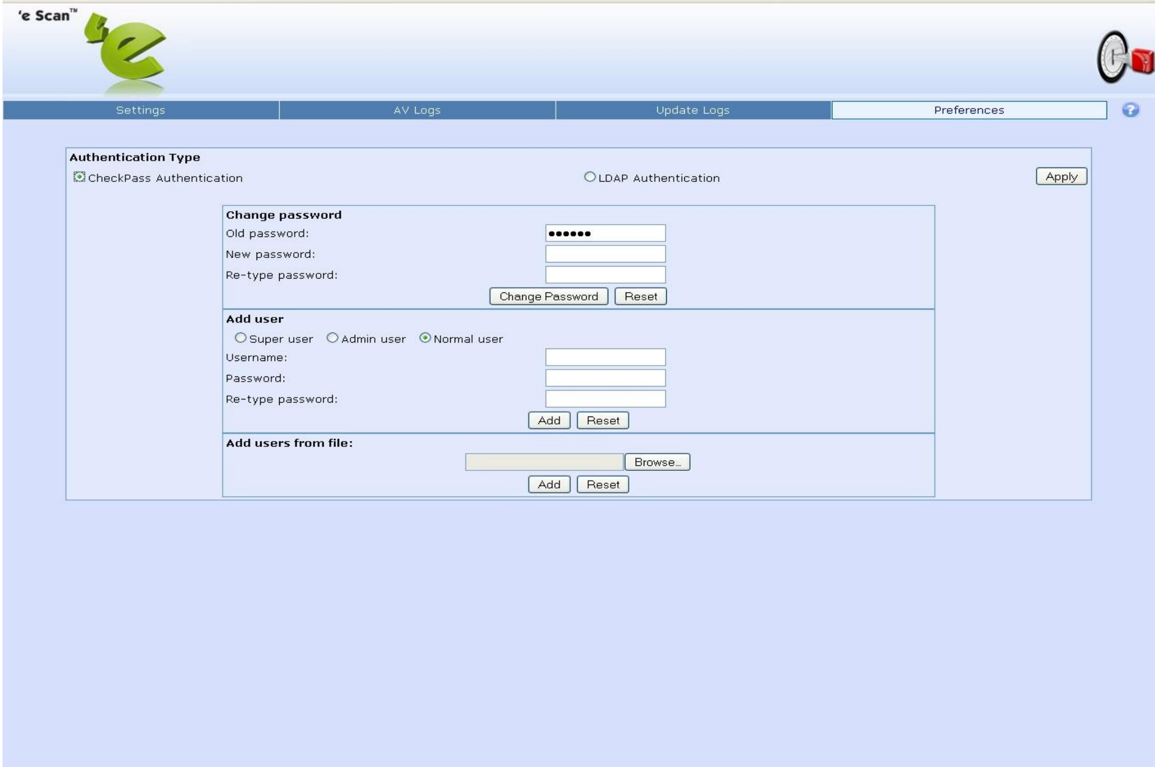
Fig.16

6) Preferences

In this section, Web-Console login credentials can be set either using the CheckPass or LDAP Authentication type ***(This is same as the Preferences in the eScan Module)***.

CheckPass Authentication: Selecting this authentication, will create user database to enable login. Admin password can be changed, new users can be added.
The type of users that can be created are Super user and Admin user. Normal user types are not available for eScan for Linux Desktop.

- Super users can access both the eScan AV module and the MWAV module from the Webscan Administrator.
- Admin users can access the particular module in which they are created. For eg. A normal user created in the eScan module can access only the eScan Module and not the MWAV module in the Web Administrator.



Authentication Type

● CheckPass Authentication ○ LDAP Authentication

Change password

Old password: ••••••

New password:

Re-type password:

Add user

○ Super user ○ Admin user ● Normal user

Username:

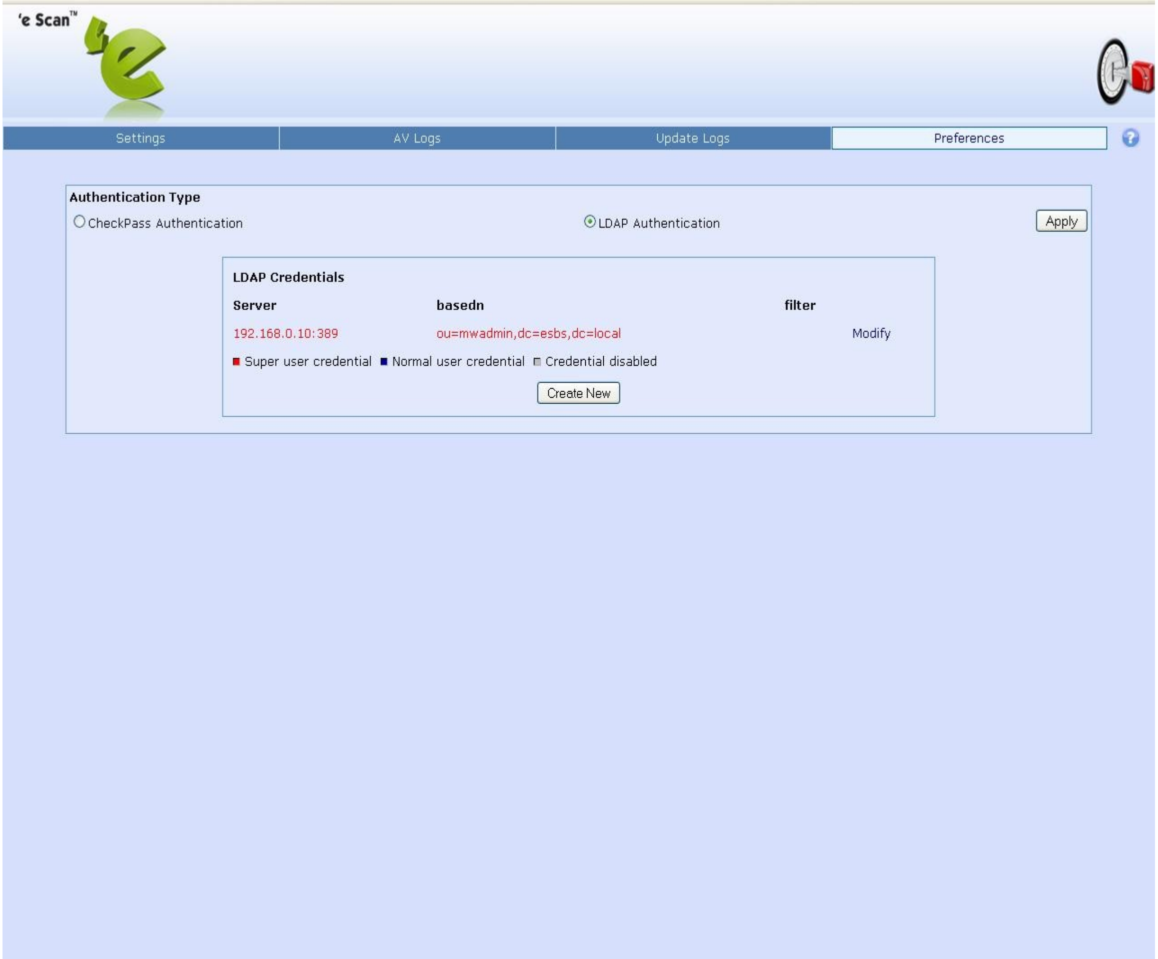
Password:

Re-type password:

Add users from file:

Fig.17

LDAP Authentication: Selecting this authentication shall configure the Web-Administration of the eScan using the LDAP server in the network to authenticate the login.



Authentication Type

○ CheckPass Authentication ● LDAP Authentication Apply

LDAP Credentials

Server	basedn	filter	
192.168.0.10:389	ou=mwadmin,dc=esbs,dc=local		Modify

🟥 Super user credential ■ Normal user credential ▫ Credential disabled

Create New

Fig.18

To enable the Web-Admin login using the LDAP Authentication,

1. Click on the Create New button,
2. Enter the new LDAP credentials (refer fig.8) in the fields provided,
3. Select Super user option and enter the LDAP server ip address and the LDAP port,
4. Enter the base disitinguished name (Base DN),
5. Enter User attribute to search in the user DN in which the user name will be searched.
6. Filter field is optional. It is useful, if only users of specific groups should be allowed to login to eScan Web-Admin.
7. Enter the user and password to test and validate the LDAP authentication.
8. Click on Test & Add button.
   If the Ldap settings are successfully authenticated, the credentials will be added (refer fig.9). Then click on the Apply button to enable the LDAP Authentication.

IV. On-Demand Scanner (eScan GUI)

To access the On-Demand Scanner from the Desktop, click on the eScan “e” icon on the Desktop.

Normal User:

Fig.19 will be displayed when in Normal User login.

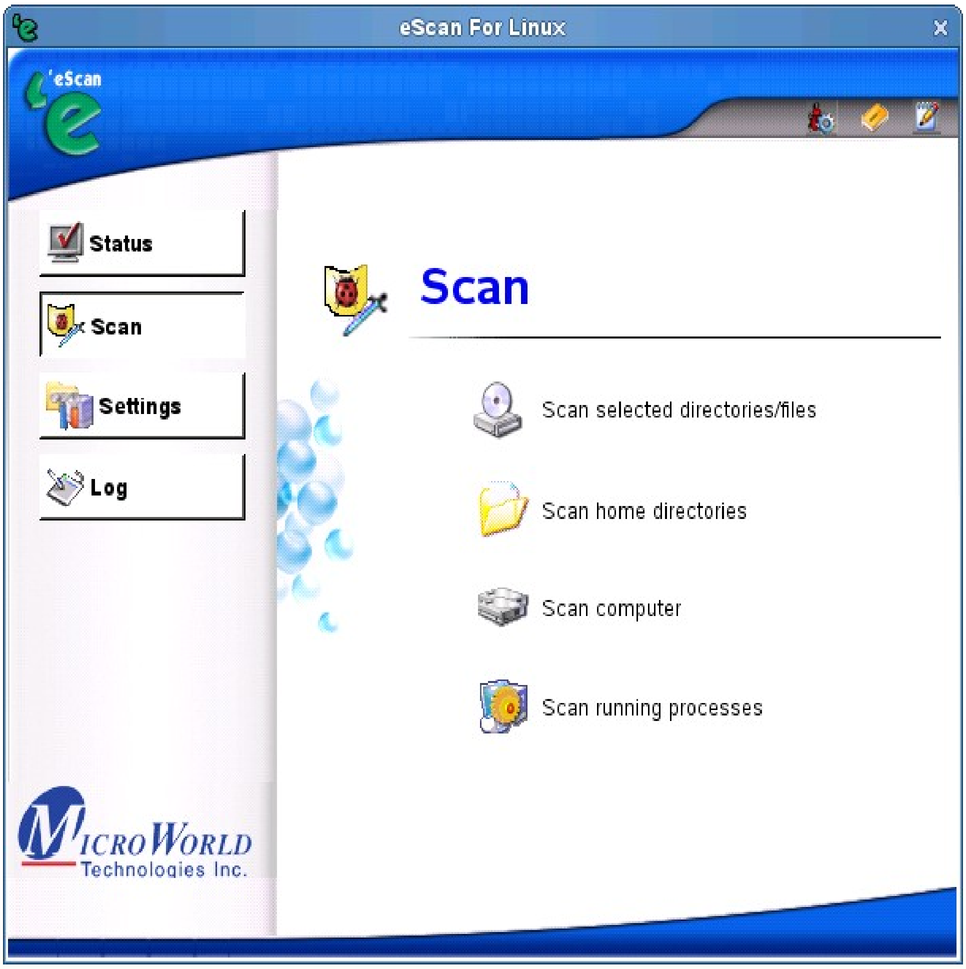
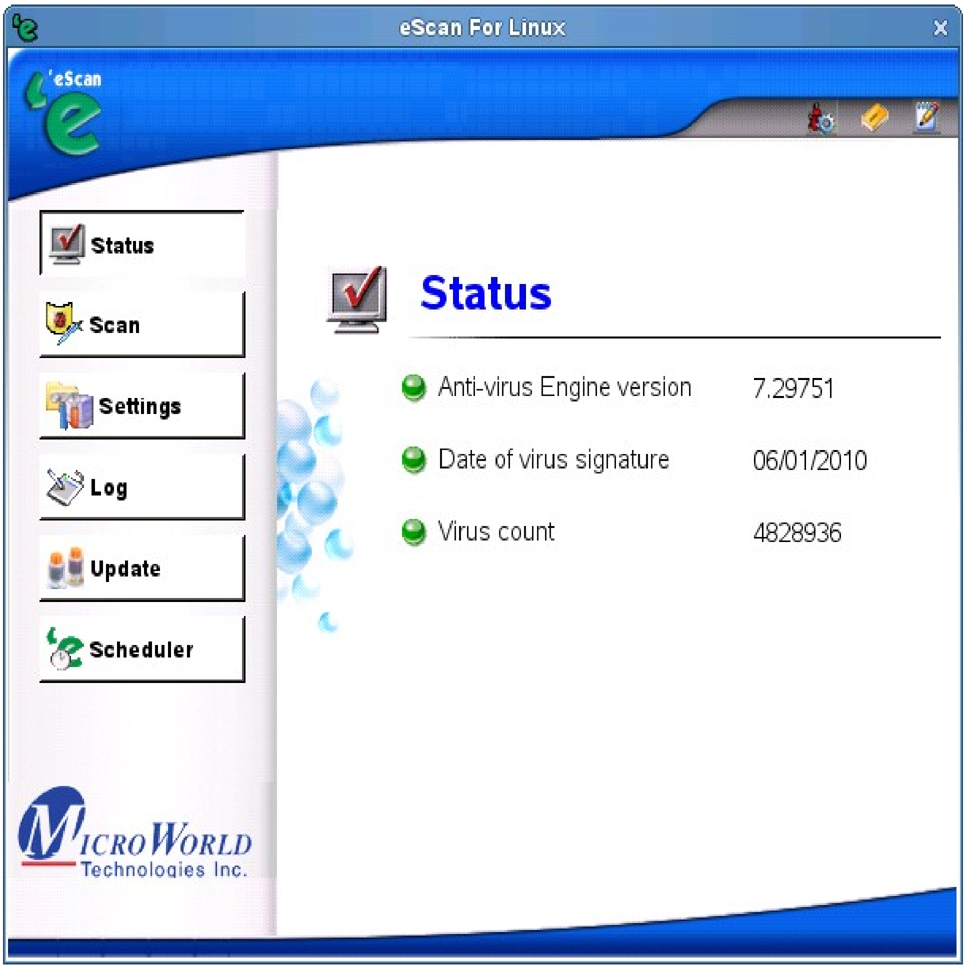


Fig.19

Root User: Fig. 20 will be displayed when in Root User login with additional option of Update and Scheduler.



Status

Anti-virus Engine version 7.29751

Date of virus signature 06/01/2010

Virus count 4828936

Fig. 20

Clicking on this button will display the Status of :

- Anti-virus Engine version – Displays the version number eScan AV engine.
- Date of virus signature – Displays the date of the downloaded virus signature updates.
- Virus count – Displays the total count of the Viruses detected by eScan.

Clicking on this button will display the various options to execute the On-Demand Scanning

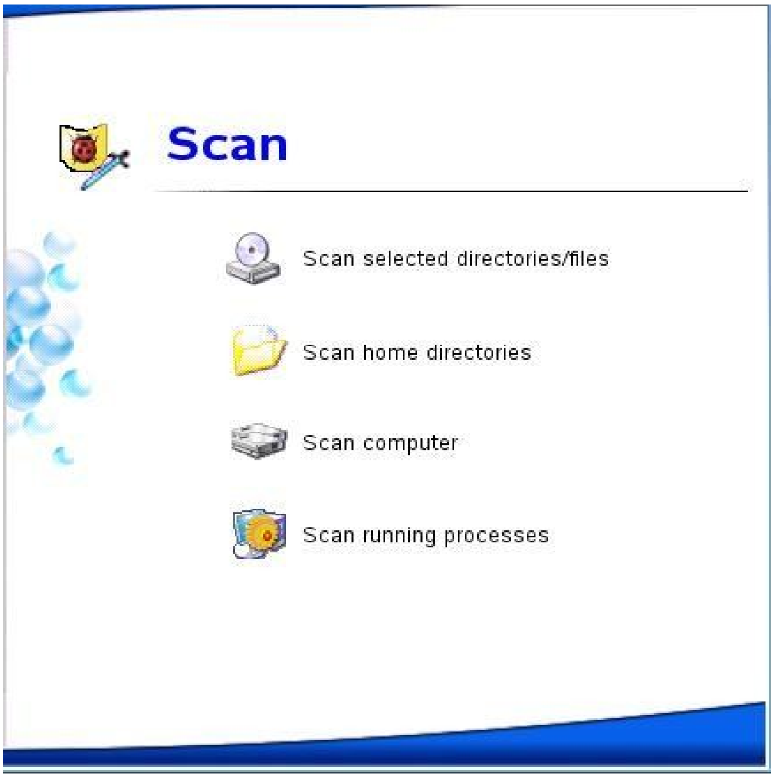
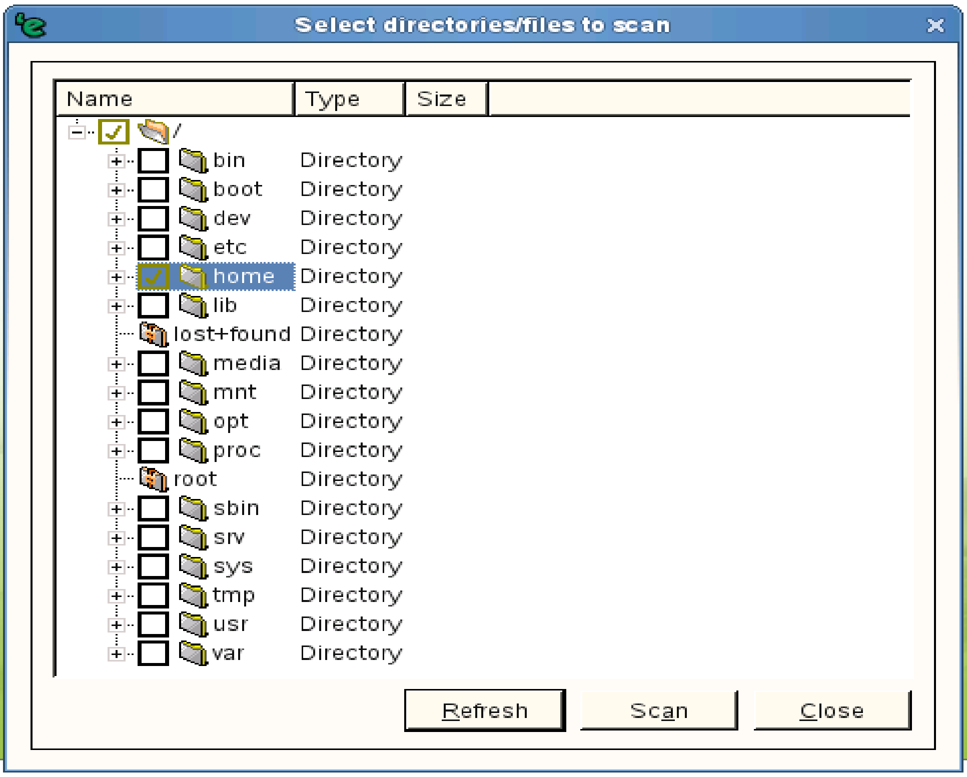


Fig.21

- Scan selected directories/files – Click on this button to scan a specific directories/files. Select the directories / files and the click on the Scan button, which will begin the scanning of the selected directories / files. (Ref. Fig.22)



Name	Type	Size
☑ /		
□ bin	Directory	
□ boot	Directory	
□ dev	Directory	
□ etc	Directory	
☑ home	Directory	
□ lib	Directory	
lost+found	Directory	
□ media	Directory	
□ mnt	Directory	
□ opt	Directory	
□ proc	Directory	
root	Directory	
□ sbin	Directory	
□ srv	Directory	
□ sys	Directory	
□ tmp	Directory	
□ usr	Directory	
□ var	Directory	

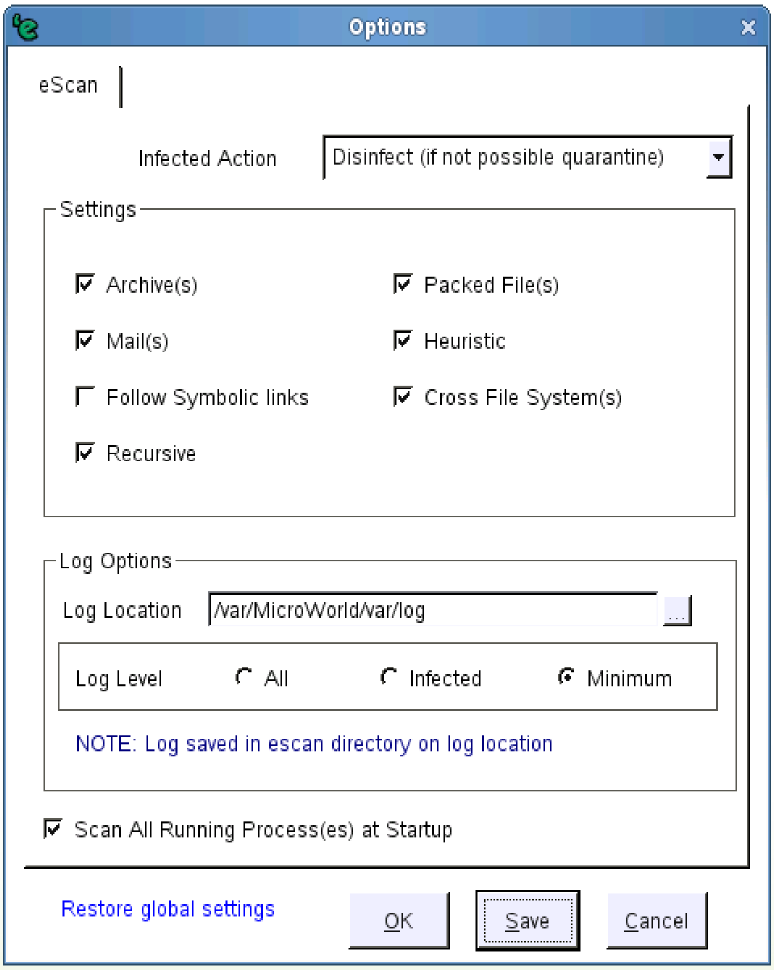
Fig.22

- Scan home directories – Click on this button to scan the Home directories and files of the logged in user.

- Scan Computer- Click on this button to scan the entire computer.
- Scan running processes – Click on this button to scan the processes running in the memory.

Clicking on this button, the eScan tab will display the settings for the On-Demand Scanning (ODS). Settings configured in this section will be the default action by the On-Demand Scanner whenever it is being executed.:

eScan Tab: In case of normal user login, only the eScan tab will be visible.



Infected Action: Disinfect (if not possible quarantine)

Settings

☑ Archive(s) ☑ Packed File(s)

☑ Mail(s) ☑ Heuristic

☐ Follow Symbolic links ☑ Cross File System(s)

☑ Recursive

Log Options

Log Location /var/MicroWorld/var/log

Log Level ○ All ○ Infected ● Minimum

NOTE: Log saved in escan directory on log location

☑ Scan All Running Process(es) at Startup

Fig. 23

- Infected Action – The selected action, from the drop-down list, will be taken during the eScan On-Demand scanning.

i. Log Only – This will only log the information of the infected object.

ii. Disinfect (if not possible Log) – This will try to disinfect and if disinfection is not possible it will only log the information of the infected object.

iii. Disinfect (if not possible Delete) - This will try to disinfect and if disinfection is not possible it will delete the infected object.

iv. Disinfect (if not possible quarantine) – This will try to disinfect and if disinfection is not possible it will quarantine the infected object.

v. Disinfect (if not possible Rename) - This will try to disinfect and if disinfection is not possible it will rename the infected object.

vi. Disinfect (if not possible prompt action) - This will try to disinfect and if disinfection is not possible it will prompt the user for an action to be taken on the infected object.

vii. Delete Infected – This will directly delete the infected object.

viii. Quarantine – This will directly quarantine the infected object.

ix. Rename – This will directly rename the infected object.

x. Prompt for an action (no disinfect) – This will prompt the user for an action to be taken on the infected object.

- Settings – The selected objects will be scanned by default during On-Demand Scanning.

i. Archive(s) – This option will specify the On-Demand Scanner to scan the archived files like zip, tar etc.

ii. Mail(s) – This option will specify the On-Demand Scanner to scan mail files.

iii. Follow Symbolic Links - Symbolic links allows to access one file from another through links. This option specifies the On-Demand scanner whether to resolve the symbolic link before actually scanning the object or to skip any such links.

iv. Recursive - This option spcifies the On-Demand scanner to scan the sub-driectories while scanning the directory object.

v. Packed File(s) - This option specifies whether to scan compressed executables.

vi. Heuristic - Selecting this option allows eScan to check for unusual sequence(s), pattern(s) or content.

vii. Cross File System(s) - In Linux, different file systems can be mounted at different location. Crossing the file systems means checking files on different partitions and/or network mounted file systems. This option specifies to On-Demand scanner whether to cross file system in scan path.

- Log Options

i. Log Location – This option specifies the location of the eScan log.

ii. Log Level – This option specifies the type of logs to be created.

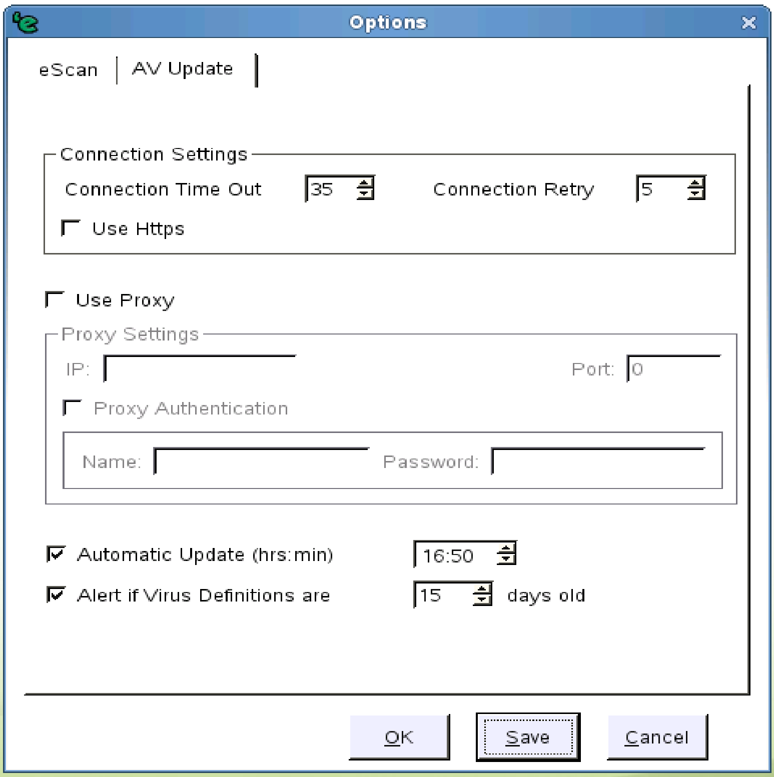
(a) All – This option will specify a detailed eScan log.

(b) Infected – This option will specify only details of the infected objects in the eScan log.

(c) Minimum – This option will specify only a minimum detail of the objects scanned in the eScan log.

- Scan All Running Process(es) at Startup – This option specifies the On-Demand scanner to scan all processes that are running are checked for any memory resident and other viruses.
- Restore global settings – This option is available only for Normal user. Clicking on this option will restore the settings made by the ROOT user.

AV Update Tab: In case of root user login, the eScan tab as well as AV Update tab will be visible. This section contains the internet settings for downloading of virus signature updates.


Options

eScan | AV Update

Connection Settings

Connection Time Out 35

Connection Retry 5

□ Use Https

□ Use Proxy

Proxy Settings

IP:

Port: 0

□ Proxy Authentication

Name:

Password:

☑ Automatic Update (hrs:min) 16:50

☑ Alert if Virus Definitions are 15 days old

Fig. 24

- Connection Settings – This specifies in case of :

   i. Connection Time Out – It will disconnect after a specified time in seconds, if it is unable to connect to the internet.
   ii. Connection Retry – It will try to reconnect the specified number of times in case of internet connection timed out.

- Proxy Settings – Select Use Proxy, to configure the Proxy settings for connecting to the internet to download the AV updates.
   i. IP – Enter the IP address of the Internet proxy server.

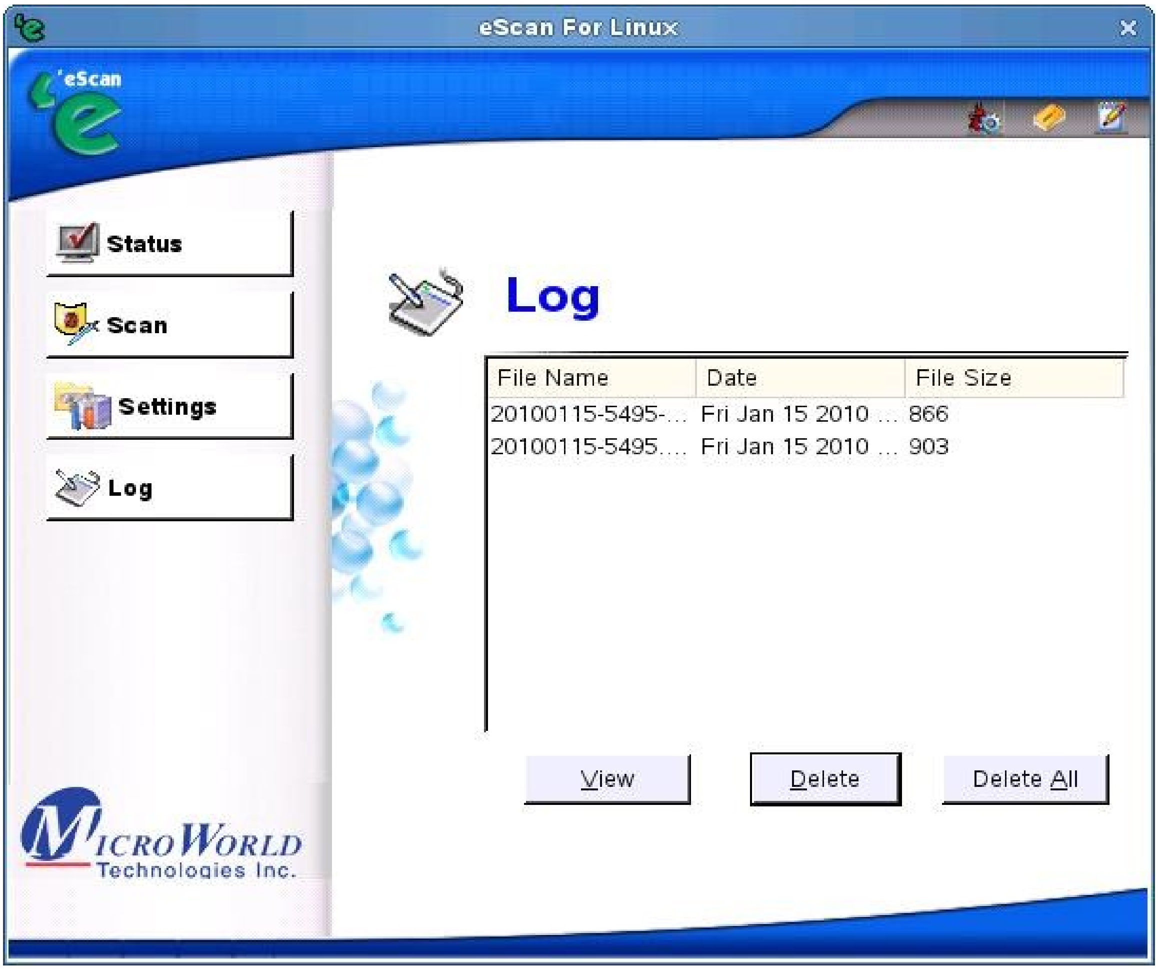
   ii. Port – Enter the Port of the internet proxy server.

   iii. Proxy Authentication: Enter the credentials in case the Proxy requires authentication.
      - Name – Enter the user name for the proxy server.
      - Password – Enter the password.

- Automatic Update – Select this option for eScan to download the AV updates automatically at specified time.

- Alert if Virus Definitions are ___ days old – This will Alert the user when AV updates are more than the specified number of days.

Clicking on this button will display all the On-Demand Scanner logs.



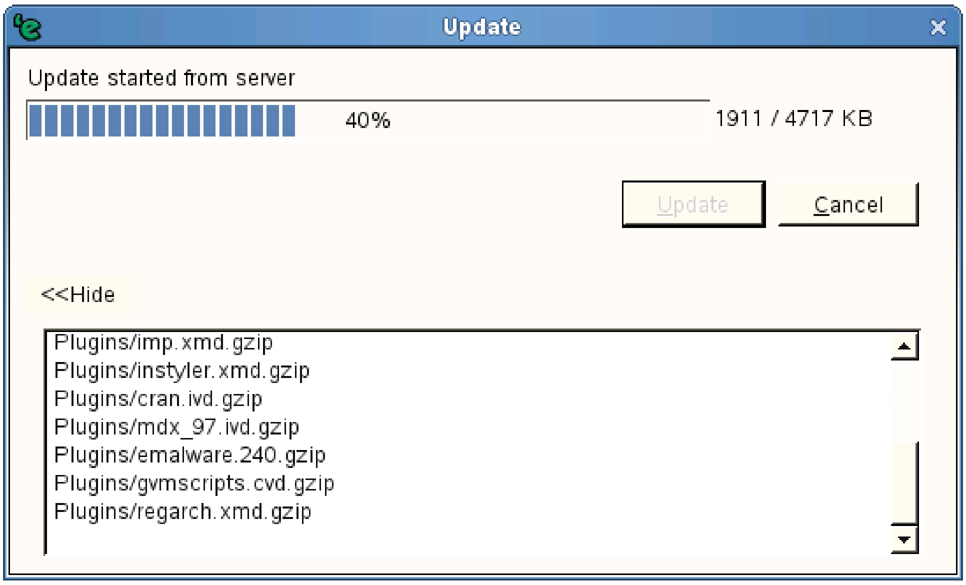
Log

File Name	Date	File Size
20100115-5495-...	Fri Jan 15 2010 ...	866
20100115-5495....	Fri Jan 15 2010 ...	903

Fig. 25

Update

Clicking on this button will begin the downloading of latest eScan AV updates. **(NOTE:- This button is available for root user login only).**

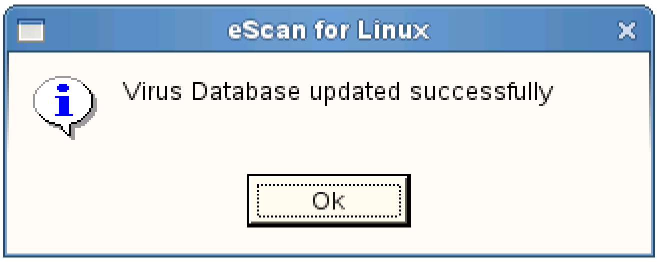


Update started from server

40% 1911 / 4717 KB

```
Plugins/imp.xmd.gzip
Plugins/instyler.xmd.gzip
Plugins/cran.ivd.gzip
Plugins/mdx_97.ivd.gzip
Plugins/emalware.240.gzip
Plugins/gvmscripts.cvd.gzip
Plugins/regarch.xmd.gzip
```

Fig.2

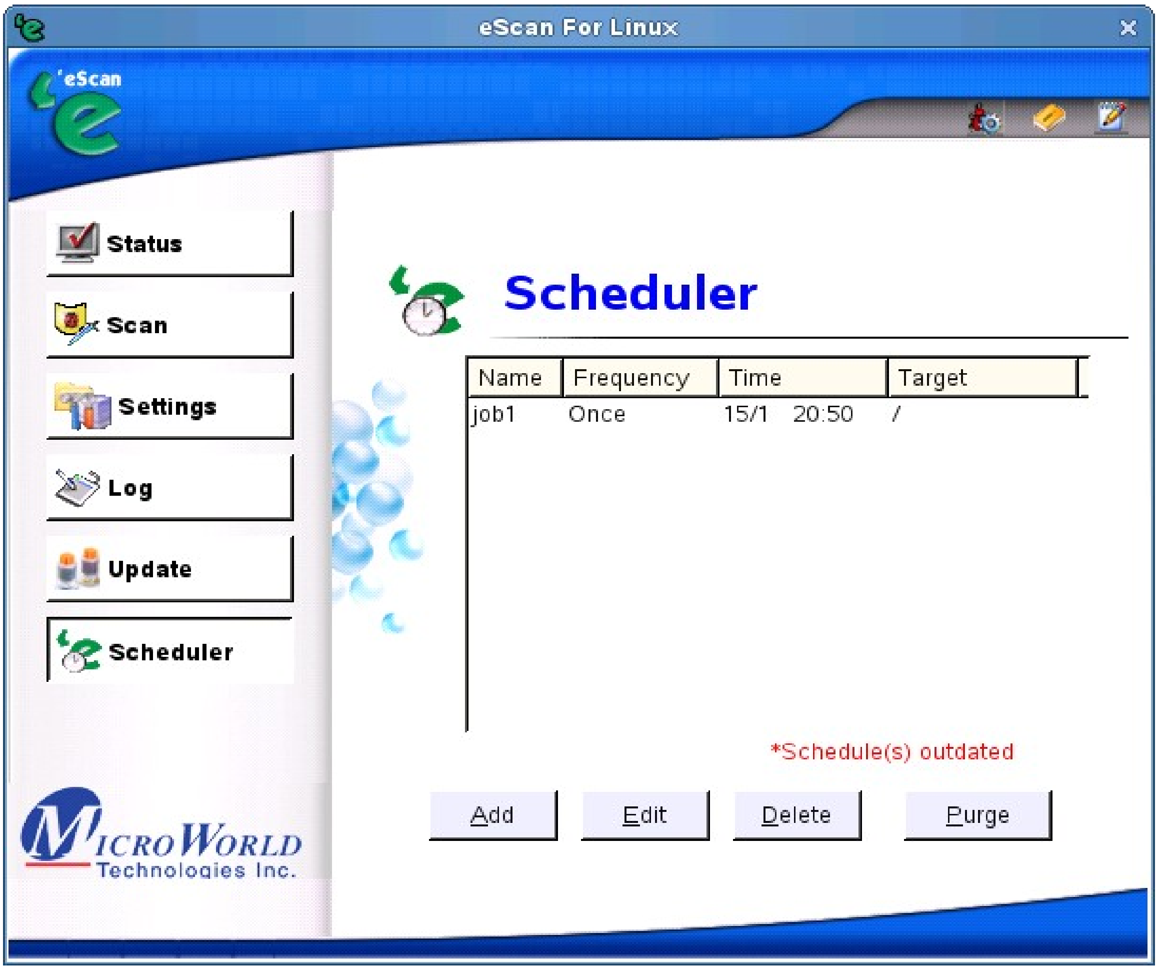


Virus Database updated successfully

Fig. 27

Once the download completes, “Virus Database updated successfully” alert message is displayed.

Clicking on this button, will display the list of On-Demand scanning scheduled to be executed at a specified time.



Scheduler

Name	Frequency	Time	Target
job1	Once	15/1 20:50	/

*Schedule(s) outdated

Fig.28

BUTTONS

1) **Add –** Click on this button to add a new job for scanning.

2) **Edit -** Click on this button to modify an existing job.

3) **Delete –** Click on this button to delete an existing job.

4) **Purge –** Click on this button to delete outdated jobs i.e. jobs already have been completed.

IV. Command-Line to run eScan from Terminal for scanning of viruses and other malwares

For Command-line help to run eScan for scanning of viruses and other malwares, refer to the manual page
# man escan