Privilege Management for Unix & Linux
User Interface Guide 10.3

Table of Contents

Privilege Management for Unix & Linux GUI Interface Guide

This guide provides detailed information regarding the security policy file programming language for the BeyondTrust Privilege Management for Unix & Linux software. This language is used to create security policy files that are used by Privilege Management for Unix & Linux to:

- Control the tasks a user or group of users may perform
- Control the systems from which a task may be submitted
- Control the systems from which a task may be run
- Determine when a specific task may be run (day and time)
- Determine where a task may be run from
- Determine if secondary security checks, such as passwords or checksums, are required to run a task
- Determine if one or more supplemental security programs are run before a task is started

> ***Note:** This guide assumes that the user has a basic understanding of Unix or Linux system administration and some experience with a scripting or other computer language. It is recommended that you have experience in these areas before you attempt to create or modify security policy files*

> ***Note:** Privilege Management for Unix & Linux Basic refers to the product formerly known as PowerBroker for Sudo. Privilege Management for Unix & Linux refers to the product formerly known as PowerBroker for Unix and Linux.*

> ***Note:** Specific font and line-spacing conventions are used to ensure readability and to highlight important information, such as commands, syntax, and examples.*

Sample Policy Files

When you install Privilege Management for Unix & Linux , you can choose to copy sample Privilege Management for Unix & Linux policy files to the installation host. These sample policy files include detailed explanations of what they do. You can use these files to learn how policy files are typically written for various scenarios. The directory that these sample files are copied to is determined by the GUI library directory option that you specify during installation. By default, this directory is **/usr/local/lib/pbbuilder**. A **readme_samples** text file in that directory includes a brief description of each sample file.

> **IMPORTANT!**
>
> *The Privilege Management for Unix & Linux GUI has been deprecated and will soon no longer be supported. To prepare for this change, we recommend switching to and using BeyondInsight for Unix and Linux.*

Get Started Using the Privilege Management for Unix & Linux Interface

The Privilege Management for Unix & Linux browser interface is a web-based GUI that provides a user-friendly alternative to administering Privilege Management for Unix & Linux from a Unix/Linux command line. The GUI enables you to easily modify the settings file, view event records from the event log, replay I/O logs, and create and modify policy files.

There are two ways to access the GUI:

- Directly, by using the browser interface URL in a web browser. This method is known as stand-alone access.
- By clicking a Privilege Management for Unix & Linux instance on the Privilege Management for Unix & Linux Console menu. The Privilege Management for Unix & Linux browser interface is displayed within the Privilege Management for Unix & Linux Console user interface.

The Privilege Management for Unix & Linux Console is a web application that provides an easy-to-use and centralized console for managing Privilege Management for Unix & Linux and includes advanced tools for reviewing and administering Privilege Management for Unix & Linux logs.

Prerequisites

The GUI is compatible with the following browsers beginning with the indicated versions:

- Opera 8.5+
- Mozilla 1.7+
- Firefox 1.5+
- Netscape 7.1+
- Internet Explorer 6.0+

> ***Note:*** *The browser must have JavaScript, cascading style sheets, and pop-ups enabled. The suggested monitor display settings are 1024 x 768 pixels or higher.*

Before users can use stand-alone access to the GUI, the Privilege Management for Unix & Linux Policy Server host must be configured to allow access to **pbguid**. Update the policy file (either **opt/pbul/policies/pb.conf** or a policy file that is included in **/opt/pbul/policies/pb.conf**) to limit access to the various activities to specific users or groups.

The following policy code shows an example:

```
browseusers = { "chris" };
settingsusers = {"kim"};
logusers = {"kim", "chris"};
iologusers = { "kim" };
policyusers = { "admin" };
policysaveusers = { "admin" };
reportusers = { "admin", "kim", "chris" };
configusers = { "admin" };
reportinfousers = { "admin", "kim" };
reportedituser s = { "admin", "chris" };
reportsaveusers = { "admin", "chris" };
reportexecuteusers = { "admin", "kim" };
```

```
entitlementinfousers = { "admin", "kim" };
entitlementusers = { "admin", "kim", "chris" };
entitlementeditusers = { "admin", "chris" };
entitlementsaveusers = { "admin", "chris" };
entitlementexecuteusers= { "admin", "kim" };

if (pbclientname == "pbguid") {
if ((argv[1] == "settings") && (user in settingsusers))
accept;

if ((argv[1] == "log") && (user in logusers))
accept;

if ((argv[1] == "iolog") && (user in iologusers))
accept;

if ((argv[1] == "browse") && (user in browseusers))
accept;

if ((argv[1] == "policy") && (user in policyusers))
accept;

if ((argv[1] == "save") && (user in policysaveusers))
accept;

if ((argv[1] == "report") && (user in reportusers)) {
if(argc > 2) {
# Restrict access to edit a report set file
if((argv[2] == "edit") && (user ! in reporteditusers))
reject;

# Restrict access to save a report set file
if((argv[2] == "save") && (user ! in reportsaveusers))
reject;

# Restrict access to execute a report set file
if((argv[2] == "exec") && (user ! in reportexecusers))
reject;

# Restrict access to get info from a report set file
if((argv[2] == "info") && (user ! in reportinfousers))
reject;
}
 accept;
}
 if ((argv[1] == "defaults") && (user in configusers))
accept;

if ((argv[1] == "entitlement") && (user in entitlementusers)) {
if (argc > 2) {
# Restrict access to edit a report set file
if((argv[2] == "edit") && (user ! in entitlementeditusers))
reject;

# Restrict access to save a report set file
if((argv[2] == "save") && (user ! in entitlementsaveusers))
reject;

# Restrict access to execute a report set file
if((argv[2] == "exec") && (user ! in entitlementexecusers))
reject;

# Restrict access to info from a report set file
if((argv[2] == "info") && (user ! in entitlementinfousers))
reject;
} accept;
}

reject;
}
```

For more information about the values of **argv[1]** and **argv[2]** for the browser interface program, please see the Privilege Management for Unix & Linux Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.

As an alternative, you can use the following code to enable access to all activities for the **admin** user:

```
if ((pbclientname == "pbguid") && (user == "admin"))
accept;
else
reject;
```

Start the Privilege Management for Unix & Linux Browser Interface

To use the Privilege Management for Unix & Linux browser interface, open Internet Explorer, Mozilla, Firefox, Netscape, or Opera. To start an HTTP session, enter the following in the browser address field:

http://system_name:port_number

For example, if your system is named **orange** and the port assigned for use with HTTP is **24348**, enter:

http://orange:24348

To start an HTTPS session, enter:

https://system_name:port_number

For example, if your system is named **mango** and the port assigned for use with HTTPS is **24349**, enter:

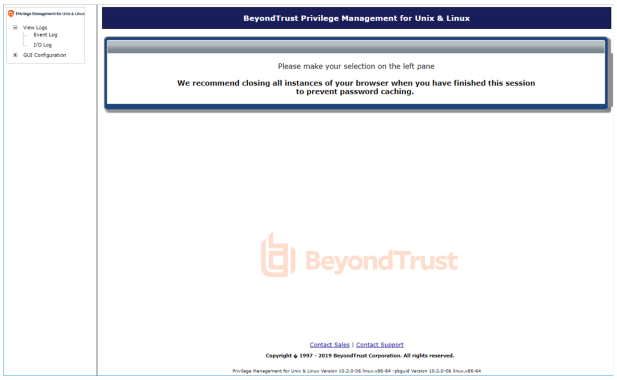
https://mango:24349

system_name	System where Privilege Management for Unix & Linux is installed.
port_number	Port assigned for use with the protocol. By default, the ports are 24348 (HTTP) and 24349 (HTTPS). Ports can be changed during a Privilege Management for Unix & Linux installation. Port numbers are located in the **/etc/services** file or the superdaemon configuration files.

For more information, please see the Privilege Management for Unix & Linux Installation Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.

Main Page

When the Privilege Management for Unix & Linux browser starts, the **Main** page is displayed. This is the point of entry to the features in the Privilege Management for Unix & Linux GUI. To return to this screen, click **Reload** or **Refresh** on your browser.


Privilege Management for Unix & Linux
View Logs
Event Log
I/O Log
GUI Configuration
BeyondTrust Privilege Management for Unix & Linux
BeyondTrust
Contact Sales | Contact Support

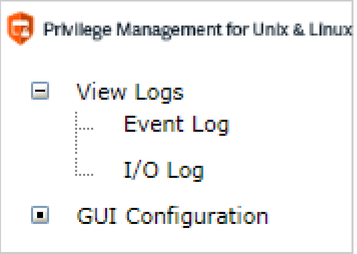
Please make your selection on the left pane

We recommend closing all instances of your browser when you have finished this session to prevent password caching.

Copyright � 1997 - 2019 BeyondTrust Corporation. All rights reserved.

Privilege Management for Unix & Linux Version 10.2.0-06 linux.x86-64 -pbguid Version 10.2.0-06 linux.x86-64

A resizable navigation menu is located on the left side of the Privilege Management for Unix & Linux browser. The menu contains several links that enable easy navigation within the browser. Expand menu items using the **+** icon to view links in the menu hierarchy.



The links present in this menu are as follows:

View Logs	Clicking on this link displays the **Event Log** and **I/O Log** links.
Event Log	Opens the **Event Log Selection** page
I/O Log	Opens the **I/O Log Selection** page
GUI Configuration	Opens the **GUI Configuration** page.

Enter Network Password Dialog

Selecting any of the hyperlinks on the **Navigation** menu for the first time during a session opens the **Enter Network Password** dialog.

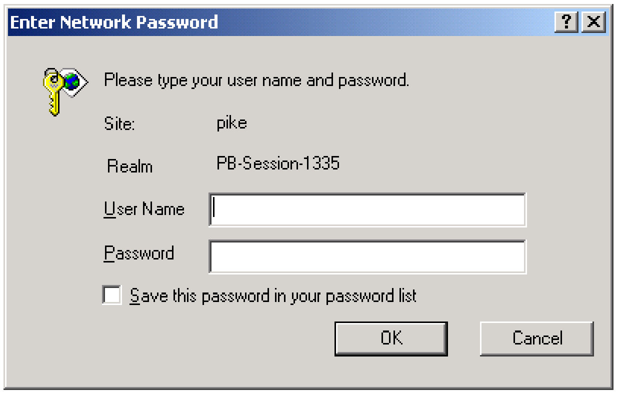
> ***Note:*** *The dialog's appearance varies depending on the browser.*

This dialog is used to obtain user authentication before allowing the user to modify the settings or policy files, view the logs, or use the reporting tools.

The user name and password allows the user to execute only those tasks that are defined by the administrator in the configuration file.

IMPORTANT!

When you finish your session, it is recommended that you close all instances of your browser to prevent password caching. To avoid compromising your system's security, it is also recommended that you do not check the ***Save password*** *box and store your password when using browsers that support this function.*



Enter Network Password

Please type your user name and password.

Site: pike

Realm PB-Session-1335

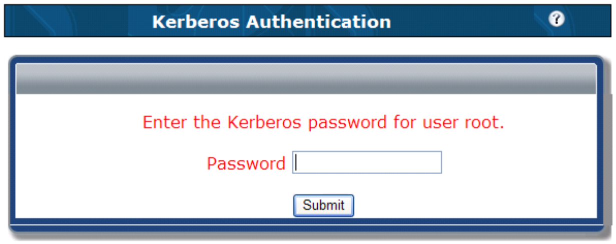
User Name

Password

☐ Save this password in your password list

Kerberos Authentication Dialog

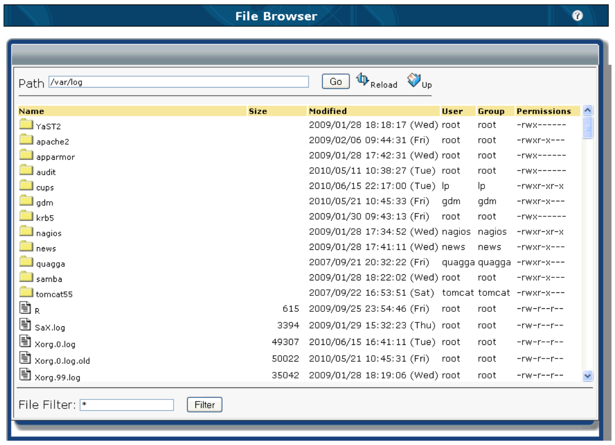
If Privilege Management for Unix & Linux is configured to use Kerberos, you must also enter a password for Kerberos authentication.



Enter the Kerberos password for user root.

File Browser Page

The **File Browser** page is used to select files for the **Log Selection** page and **I/O Log Selection** page. For this guide, these pages are known as calling pages.



Path /var/log

Name	Size	Modified	User	Group	Permissions
YaST2		2009/01/28 18:18:17 (Wed)	root	root	-rwx------
apache2		2009/02/06 09:44:31 (Fri)	root	root	-rwxr-x---
apparmor		2009/01/28 17:42:31 (Wed)	root	root	-rwx------
audit		2010/05/11 10:38:27 (Tue)	root	root	-rwx------
cups		2010/06/15 22:17:00 (Tue)	lp	lp	-rwxr-xr-x
gdm		2010/05/21 10:45:33 (Fri)	gdm	gdm	-rwxr-x---
krb5		2009/01/30 09:43:13 (Fri)	root	root	-rwx------
nagios		2009/01/28 17:34:52 (Wed)	nagios	nagios	-rwxr-xr-x
news		2009/01/28 17:41:11 (Wed)	news	news	-rwxr-x---
quagga		2007/09/21 20:32:22 (Fri)	quagga	quagga	-rwxr-x---
samba		2009/01/28 18:22:02 (Wed)	root	root	-rwxr-x---
tomcat55		2007/09/22 16:53:51 (Sat)	tomcat	tomcat	-rwxr-x---
R	615	2009/09/25 23:54:46 (Fri)	root	root	-rw-r--r--
SaX.log	3394	2009/01/29 15:32:23 (Thu)	root	root	-rw-r--r--
Xorg.0.log	49307	2010/06/15 16:41:11 (Tue)	root	root	-rw-r--r--
Xorg.0.log.old	50022	2010/05/21 10:45:31 (Fri)	root	root	-rw-r--r--
Xorg.99.log	35042	2009/01/28 18:19:06 (Wed)	root	root	-rw-r--r--

File Filter: *

Open the File Browser

To open the **File Browser**, click **Browse** in the calling page.

Navigation

The **File Browser** displays directory and file lists in alphabetical order. Only valid file and directory names are listed. The list can be re-sorted by name, size, and so on, by clicking on the appropriate column heading.

There are several ways to navigate through the directories. You can click on the directory icons on the left side of the page or you can type a directory name in the **Path** field and click **Go**. The directory icons can also be used in conjunction with the **Path** field and **Go** button.

Refresh the List

To refresh the contents of the **File Browser**, click **Reload**.

Filter the List

The files that are in the currently selected directory are listed on the left side of the page. These files can be filtered to list items with certain extensions or certain character strings in their file names. To filter a list of files, type a wildcard search character and the character string to search for in the **File Filter** field, and click **Filter**.

Select a File

To select a file, click the file's icon. The **File Browser** closes, and the selected file name is used in the appropriate field in the calling page.

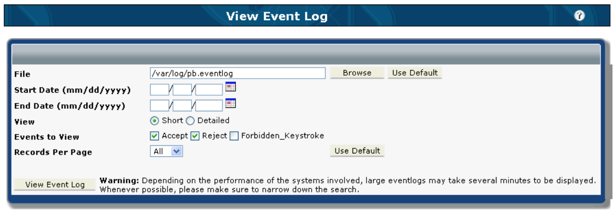
View Logs

You can select and view event and I/O logs. Event logs contain a record of Privilege Management for Unix & Linux events. I/O logs provide a history of a user's keystrokes during a given Privilege Management for Unix & Linux session.

View Privilege Management for Unix & Linux Events

You can view Privilege Management for Unix & Linux events that are saved in event log files. Because events can be saved in more than one event log, the first step in viewing events is to select a log. Individual events can be viewed from the selected event log.

Select an Event Log and Records Page



View Event Log

File	/var/log/pb.eventlog [Browse] [Use Default]
Start Date (mm/dd/yyyy)	/ /
End Date (mm/dd/yyyy)	/ /
View	● Short ○ Detailed
Events to View	☑ Accept ☑ Reject □ Forbidden_Keystroke
Records Per Page	All [Use Default]

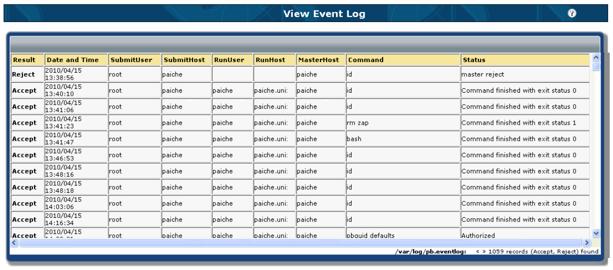
[View Event Log] **Warning:** Depending on the performance of the systems involved, large eventlogs may take several minutes to be displayed. Whenever possible, please make sure to narrow down the search.

1. In the left navigation menu, select **View Logs > Event Log**. If prompted, log in with your Unix/Linux user name and password. The **Event Log Selection** page will open.
2. In the **File** field, enter an absolute path (directory and file name) for the event log. You can click **Browse** to select the event log from the **File Browser**, or you can click **Use Default** to select the default event log.
3. *(Optional)* Specify a date range in the **Start Date** and **End Date** fields. Leave the **Start Date** blank to view logs from the beginning of the log file, and leave the **End Date** blank to include the most recent events.
4. Use the **View** options to select how you want to view the events. Select **Short** to view a table of events, or select **Detailed** to view the details for each event.
5. *(Optional)* Choose the event types to view by selecting or clearing the **Accept**, **Reject** or **Forbidden Keystroke** check boxes.
6. *(Optional)* Use the **Records Per Page** dropdown to limit the number of event records to display on a single page.
7. Click **View Event Log**.

If you select the **Short** option, Privilege Management for Unix & Linux displays the event log in the **Event Log** page. If you selected the **Detailed** option, Privilege Management for Unix & Linux displays the event log in the **Event Log Detail** page.

Use the Event Log Page

The **Event Log** page displays the event log records selected in the **Event Log Selection** page. This page provides information similar to the output from Privilege Management for Unix & Linux's **pblog** program.



View Event Log

Result	Date and Time	SubmitUser	SubmitHost	RunUser	RunHost	MasterHost	Command	Status
Reject	2010/04/15 13:38:56	root	paiche			paiche	id	master reject
Accept	2010/04/15 13:40:10	root	paiche	paiche	paiche.uni:	paiche	id	Command finished with exit status 0
Accept	2010/04/15 13:41:06	root	paiche	paiche	paiche.uni:	paiche	id	Command finished with exit status 0
Accept	2010/04/15 13:41:23	root	paiche	paiche	paiche.uni:	paiche	rm zap	Command finished with exit status 1
Accept	2010/04/15 13:41:47	root	paiche	paiche	paiche.uni:	paiche	bash	Command finished with exit status 0
Accept	2010/04/15 13:46:53	root	paiche	paiche	paiche.uni:	paiche	id	Command finished with exit status 0
Accept	2010/04/15 13:48:16	root	paiche	paiche	paiche.uni:	paiche	id	Command finished with exit status 0
Accept	2010/04/15 13:48:18	root	paiche	paiche	paiche.uni:	paiche	id	Command finished with exit status 0
Accept	2010/04/15 14:03:06	root	paiche	paiche	paiche.uni:	paiche	id	Command finished with exit status 0
Accept	2010/04/15 14:16:34	root	paiche	paiche	paiche.uni:	paiche	id	Command finished with exit status 0
Accept	2010/04/15	root	paiche	paiche	paiche.uni:	paiche	pbguid defaults	Authorized

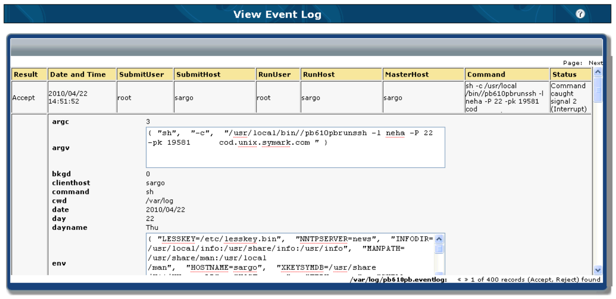
/var/log/pb.eventlog: « » 1059 records (Accept, Reject) found

You can do any of the following on this page:

- Use the links in the top right of the report to go to a specific page that displays 50 records.
- The bottom right corner of the report window displays the event log name and the total number of events that are displayed.
- Use the **Expand** icon to view the report across the entire browser window. Use the **Shrink** icon to restore the normal report view.
- Click a column heading to sort the table by that column.
- Click on the value in the **Result** column for an event to view details about that event in the **Event Log Detail** page.

Use the Event Log Detail Page

The **Event Log Detail** page is opened from the **Privilege Management Event Log Selection** page by selecting the **Detailed** option and clicking **View Event Log**. It can also be opened from the **Event Log** page by clicking the value in the **Result** column for an event.



View Event Log

Page: Next

Result	Date and Time	SubmitUser	SubmitHost	RunUser	RunHost	MasterHost	Command	Status
Accept	2010/04/22 14:51:52	root	sargo	root	sargo	sargo	sh -c /usr/local /bin//pb610pbrunssh -l neha -P 22 -pk 19581 cod	Command caught signal 2 (Interrupt)

argc	3
argv	{ "sh", "-c", "/usr/local/bin//pb610pbrunssh -l neha -P 22 -pk 19581 cod.unix.symark.com " }
bkgd	0
clienthost	sargo
command	sh
cwd	/var/log
date	2010/04/22
day	22
dayname	Thu
env	{ "LESSKEY=/etc/lesskey.bin", "NNTPSERVER=news", "INFODIR=/usr/local/info:/usr/share/info:/usr/info", "MANPATH=/usr/share/man:/usr/local/man", "HOSTNAME=sargo", "XKEYSYMDB=/usr/share

/var/log/pb610pb.eventlog: « » 1 of 400 records (Accept, Reject) found

- The **Event Log Detail** page displays detailed information for a specific log entry. This page shows the same information for a listing as the **Event Log** page, plus all of the additional variables that were set for the command. The information is similar to that displayed by running **pblog –l** from the command line.
- The bottom right corner of the report window displays the event log name and which event out of the total events from the last query is being displayed.
- Use the **Expand**icon to view the report across the entire browser window. Use the **Shrink** icon to restore the normal report view.
- In the top right corner of the report page, you can use the **Prev** and **Next** links to navigate to the previous record or the next record. Each system-defined variable has a hyperlink that opens online help that describes the variable.

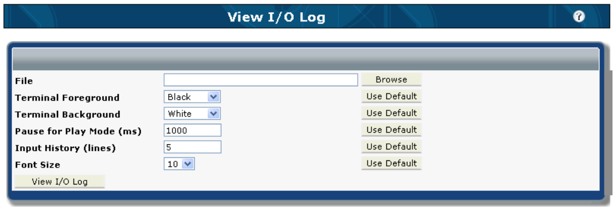
View Privilege Management for Unix & Linux I/O Logs

You can view Privilege Management for Unix & Linux I/O logs.

For more information about I/O logging, please see the Privilege Management for Unix & Linux Administration Guide and the Privilege Management for Unix & Linux Language Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.

***Note:** The I/O Viewer supports vt100, xterm, and dtterm terminals. The viewer attempts to display I/O logs from any terminal type, but there is no guarantee that unsupported terminals will be rendered accurately. Special graphic characters such as line drawing characters are not supported.*

Select an I/O Log



View I/O Log

File		Browse
Terminal Foreground	Black	Use Default
Terminal Background	White	Use Default
Pause for Play Mode (ms)	1000	Use Default
Input History (lines)	5	Use Default
Font Size	10	Use Default

1. In the left navigation menu, select **View Logs > I/O Log**. If prompted, log in with your Unix/Linux user name and password.
2. In the **File** field, enter the absolute path (directory and file name) for an I/O log. You can click **Browse** to select the I/O log from the file browser.
3. *(Optional)* From the **Terminal Foreground** and **Terminal Background**, select the terminal foreground and background colors. Click **Use Default** to select the default colors.
4. *(Optional)* Set the amount of time, in milliseconds, to pause after displaying each line during playback. Click **Use Default** to reset this value to the default.
5. *(Optional)* Set the number of lines of input to display. To display all input lines, enter **0**. Click **Use Default** to reset this value to the default.

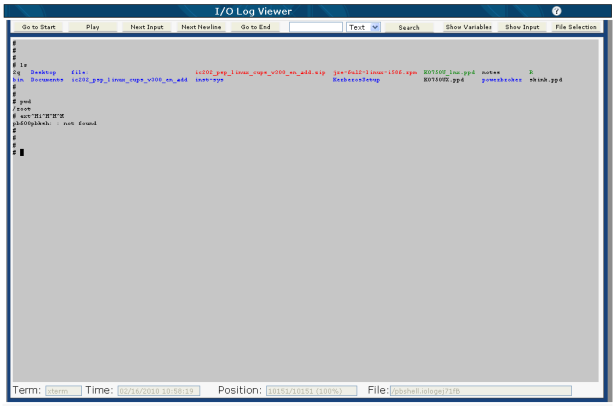
6. *(Optional)* Select the font size for the display. Click **Use Default** to reset this value to the default.
7. Click **View I/O Log**. Privilege Management displays the I/O log in the **I/O Log Viewer** page.

Use the I/O Log Viewer Page

This page opens after you select an I/O log file in the **I/O Log Selection** page and click **View I/O Log**. The **I/O Log Viewer** page enables you to play back an I/O log and see a simulation of the keystrokes that were made by a user during a session.

Limitations

- The terminal emulation (color, font, etc.) might not match what the user saw during the session.
- The essential keystrokes and responses are displayed but not all of the original formatting.
- I/O logging records keystrokes, output streams, and error streams but not mouse clicks or other GUI actions.
- No attempt is made to reproduce the timing of the original input. The simulation is taking place in a browser and the timing observed is constrained by the location of the server processing the browser requests and network traffic.
- The operating system may become overwhelmed if **New Input** or **Next Newline** are clicked multiple times too rapidly. Clicking these buttons rapidly can cause you to be prompted for a user name and password, but you are unable to log in.



```
#
#
#
# ls
2q   Desktop    file:                                 ic202_psp_linux_cups_v300_en_add.zip  jre-6u12-linux-i586.rpm  K0750U_lnx.ppd  notes       R
bin  Documents  ic202_psp_linux_cups_v300_en_add  inst-sys                              KerberosSetup            K0750UX.ppd     powerbroker  skink.ppd
#
#
# pwd
/root
# ext^Hi^H^H^H
pb600pbksh: : not found
#
#
#
# ▮
```

Term: xterm Time: 02/16/2010 10:58:19 Position: 10151/10151 (100%) File: /pbshell.iologej71fB

The **I/O Log Viewer** consists of three areas:

- The top is a toolbar used for controlling the I/O log playback, moving within the log, and navigating to other parts of the application.
- The center section of the screen displays the I/O log playback. This playback is a simulation of what the original user would have seen on the Unix/Linux terminal.
- The bottom of the page shows information about when the current I/O event was logged and its location in the I/O log.

To play back a I/O log, click **Play**. Click **Pause** to stop the playback. Use the following controls to go through the log and access additional features:

Go to Start	Moves to the beginning of the log.
Play/Pause	Starts and stops the I/O log playback loop.
Next Input	Advances the playback to the next keystroke.
Next Newline	Advances the playback to the next newline in the I/O log.
Go to End	Moves to the end of the log. Enter a place (position), text string, or time to search for in the I/O log. Place is a position from the start of the file. It is any positive number limited to the size of the I/O log. Text to search for can be individual characters and whole or partial strings. Wildcard search characters cannot be used.
Search field	Time is set as **[MM/DD/[CC]YY] HH:MM[:SS]** (for example, **13:40** or **11/28/2001 13:40:48**).

	Note: *The I/O log file uses discrete positions and time intervals. You cannot go to an exact position or time. You must go to the next highest position or time increment.* This field is used with the **Search** list and **Search** button. Select the entry to search for: • Place (location) • Text string • Time.
Search list	This list is used with the **Search** field and **Search** button.
Search button	Looks for the exact search text, next greatest time, or next largest place in the input stream, depending on which option was selected. This button is used with the **Search** field and **Search** list.
Show Variables	Shows the variables that were stored in the I/O log when it was created.
Show Input	Shows the input that a user typed. The information is displayed in a separate window.
File Selection	Returns to the **I/O Log Selection** page.

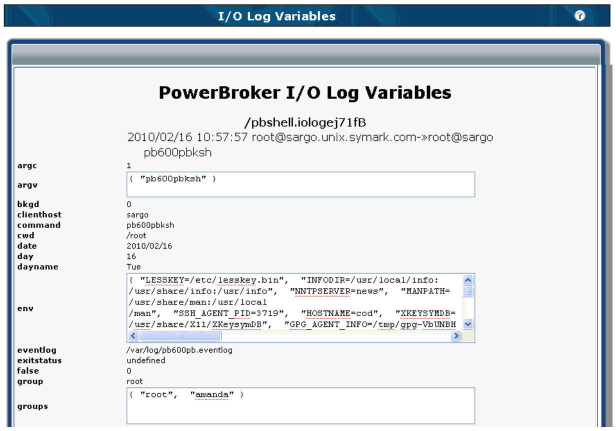
I/O Log Variables Page

The **I/O Log Variables** page is opened from the **I/O Log Viewer** page by clicking **Show Variables**. This page displays detailed information for a specific I/O log. This page shows the same information for a listing as the **I/O Log Viewer** page as well as all of the additional variables that were set for the command. The information is similar to that displayed by running **pbreplay -av** from the command line.

The top of the page displays the:

- Name of the I/O log
- The date and time
- The submitting user and submitting host
- The run user and run host
- The command that was run

Click **Close** to exit the **I/O Log Variables** page.



PowerBroker I/O Log Variables

/pbshell.iologej71fB
2010/02/16 10:57:57 root@sargo.unix.symark.com->»root@sargo
pb600pbksh

```
argc         1
argv         { "pb600pbksh" }
bkgd         0
clienthost   sargo
command      pb600pbksh
cwd          /root
date         2010/02/16
day          16
dayname      Tue
env          { "LESSKEY=/etc/lesskey.bin",  "INFODIR=/usr/local/info:
             /usr/share/info:/usr/info",  "NNTPSERVER=news",  "MANPATH=
             /usr/share/man:/usr/local
             /man",  "SSH_AGENT_PID=3719",  "HOSTNAME=cod",  "XKEYSYMDB=
             /usr/share/X11/XKeysymDB",  "GPG_AGENT_INFO=/tmp/gpg-VbUNBH
eventlog     /var/log/pb600pb.eventlog
exitstatus   undefined
false        0
group        root
groups       { "root",  "amanda" }
```

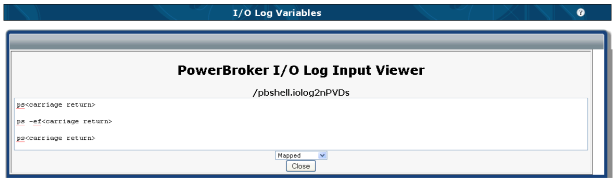
Use the I/O Log Input Viewer Page

Clicking **Show Input** in the **I/O Log Viewer** page opens the **I/O Log Input Viewer** page. The **I/O Log Input Viewer** page displays the keystroke input stream. In other words, it shows what the user typed. The information that is presented is similar to that displayed when running **pbreplay -i** from the command line.

Note: *Clicking **Show Input** displays the input only up to a given point in the I/O log file and that point must have already been navigated to with the browser.*

Select an input type from the list to set the format of the input data: **Hexadecimal**, **Octal**, and **Mapped**. The **Mapped** option replaces unprintable characters with descriptive tags.

Click **Close**.



```
ps<carriage return>

ps -ef<carriage return>

ps<carriage return>
```

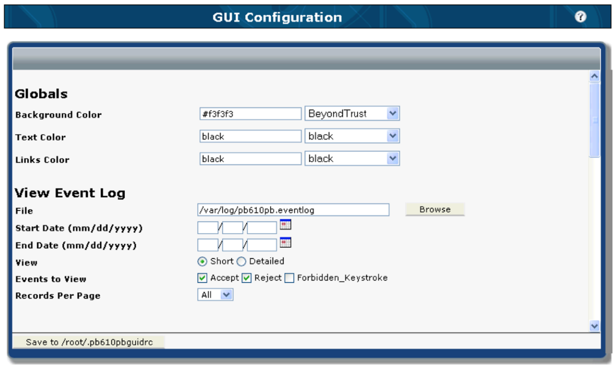
Customize the Privilege Management for Unix & Linux GUI Interface

On the **GUI Configuration** page, you can customize the GUI. Click **GUI Configuration** on the left navigation menu to access this page.

GUI Configuration Page

The **GUI Configuration** page consists of several sections. Each section represents a configuration category.

All settings are described in this section. This page has the following buttons, links, fields, check boxes, and dropdowns:



GUI Configuration

Globals

Background Color: #f3f3f3 | BeyondTrust

Text Color: black | black

Links Color: black | black

View Event Log

File: /var/log/pb610pb.eventlog [Browse]

Start Date (mm/dd/yyyy): __/__/____

End Date (mm/dd/yyyy): __/__/____

View: ● Short ○ Detailed

Events to View: ☑ Accept ☑ Reject □ Forbidden_Keystroke

Records Per Page: All

[Save to /root/.pb610pbguidrc]

Setting	Description
Save to path button	Saves the GUI configuration to the **.pbguidrc** file in the user's home directory.
Background Color field	Specifies the default background color for all pages. Valid values are a color name or RGB value entered in the format **#RRGGBB**.
Text Color field	Specifies the default text color for all pages. Valid values are a color name or a RGB value entered in the format **#RRGGBB**.
Links Color field	Specifies the color of links (typically for online help) for all pages. Valid values are a color name or a RGB value entered in the format **#RRGGBB**.
View Event Log	Specifies the name of the event log file to view by default. Specifies the default starting date of a date range for the records to view.
File field	Click **Browse** to select the file with the file browser.
Start Date field	Leave this field blank if you do not want a default start date.
End Date field	Specifies the default end date of the date range for the records to view. Leave this field blank if you do not want a default end date. Specifies the default view:
View options	**Short** displays an abbreviated form of the record in the **Event Log** page. **Detailed** displays all of the record fields in the **Event Log Detail** page.
Events to View options	Specifies the type of log records (accept, reject, or forbidden keystroke) to display in the **Event Log** page. Select those that you want to enable by default.

Records Per Page dropdown	Specifies the number of log records to display by default on a page
View I/O Log	Specifies the name of the I/O log file to view by default.
File field	Click **Browse** to select this file with the file browser.
Terminal Foreground dropdown	Specifies the default terminal foreground color
Terminal Background dropdown	Specifies the default terminal background color
Pause for Play Mode field	Specifies the default time, in milliseconds, that the screen pauses before going to the next line during playback
Input History field	Specifies how many lines of the input to display by default
Policy File Selection	Specifies the name of the policy file to open by default.
Policy File field	Click **Browse** to select this file with the file browser.
Policy Editor	In version 3.5 and before, the field is not available. In version 4.0+, the field is available.
Color for selected items field	Specifies the default color of highlighted text in the Policy Editor. Valid color values are color names or an RGB value (the format is #RRGGBB). In version 3.5 and before, the field is not available.
Netgroup Lookup options	Specifies sources for netgroup names .
Select List Limit field	Specifies the maximum number of items to display in the user and group selection lists of the Policy W5 Editor. Set to **0** for no limit.
Inactivity Timeout field	Specifies the number of minutes of inactivity before the Policy Editor times out.
Policy Editor TCP Port field	Specifies a user-defined port number. For enhanced security, this value should be left at **0** (default), which randomly picks a valid TCP port number for the Policy Editor. It should be changed only when firewall settings prevent the editor from working. Specify a valid and unused TCP port number.
Task Manager	In versions 6.0.1+, this section is not available.
Inactivity Timeout (min) field	Specifies the number of minutes of inactivity before the Task Manager Console times out.
Console TCP Port field	Specifies a user-defined port number. For enhanced security, this value should be left at **0** (default), which randomly picks a valid TCP port number for the Task Manager Console. It should be changed only when firewall settings prevent the editor from working. Specify a valid and unused TCP port number.
Prompt color: User fields	Specifies the text color for the user portion of the command line prompt in the response area of the Task Manager Console. Valid color values are color names or an RGB value (the format is **#RRGGBB**).
Prompt color: Host fields	Specifies the text color for the host portion of the command line prompt in the response area of the Task Manager Console. Valid color values are color names or an RGB value (the format is **#RRGGBB**).
Text color fields	Specifies the text color for the commands and responses in the response area of the Task

	Manager Console. Valid color values are color names or an RGB value (the format is **#RRGGBB**).
Response Timeout (sec) field	Specifies the number of seconds the **Task Manager Console** waits for a response from the run host before returning control to the user.
User defined HTML Request Menu field	Specifies the path and file name of the HTML snippet that defines the top, or command, area of the Task Manager Console. Click **Browse** to select this file with the file browser.