HP User Behavior Analytics

HP UBA Version 1.0

Powered by SECURONIX

Installation Guide

May 6, 2015

Table of Contents

Chapter 1: About This Guide

Use the Install Guide to learn how to install HP User Behavior Analytics. In this manual, you can find:

1. What is HP User Behavior Analytics
2. Installation components
3. Installation procedure
4. Post-installation activities

About HP User Behavior Analytics

HP User Behavior Analytics is an advanced security analytics solution that uses correlation, algorithms and visualizations to detect new threats, targeted attacks and privileged account misuse.

Who Should Read this Guide

This guide is intended for system administrators, system integrators and deployment teams who need to install the application.

System administrators, responsible for ongoing operations and management should refer to the Administrators Guide. Users of the HP UBA application (security operations, information security professionals, security analysts, risk and compliance officers and IT specialists who need to use the functionalities within the product) should refer to the HP UBA User Guide. If you are responsible for integrating data sources refer to the HP UBA Administrator Guide/Importing Data.

Chapter 2: Installation and Configuration

Installation Components

The simplest deployment is the one you get by default when you install HP UBA: database and application running on the same server. Data comes in from the sources you've configured, and you log into the HP UBA web interface on this same server to monitor and analyze data.

Depending on your needs, HP UBA can be deployed in a Master – Child configuration or on a single node. This guide describes installing HP UBA on a single node.

Following components are involved in the deployment:

- Configuration folder – The application reads configuration data from files stored under the [application]_home folder. The [application]_home folder stores certain files required during application startup, configuration and running of the application.
- Relational database – The application uses a relational database to store data. HP UBA supports the MySQL database.
- Universal forwarder node* – universal forwarders provide the capability to import and analyze activities and security events. They typically run on a separate computer then the computer running the application. They utilize the same database as the HP UBA application for storage of event data.
- Child node* – Child nodes provide the capability to import and analyze activities and security events. They typically run on a separate computer from the computer running the application. They utilize a different database than the application.
- Syslog forwarder – Syslog forwarders are light-weight forwarders that have the capability to read log files incrementally and forward the logs as syslog to the HP UBA application or Real Time Analyzers.
- TPI aggregator – A text indexing engine used to index and store data aggregated from threat intelligence sources. Provides quick search and retrieval.

These components are part of a master child deployment. They are not required for a single node deployment

Checklist

Before you get started with the deployment, make sure that you have the following details ready:

- HP User Behavior Analytics software
- License files and license key
- Deployment environment(s) – capacity planning, hardware, software, browser and port requirements as discussed above
- Database server (HP UBA supports the MySQL 5.6 database)
- Source of identity data (human resource management system, LDAP source, database, others)
- Source of activity/event data (syslog server, audit tables, log management, SIEM, database monitoring, DLP, others)
- Email server configuration with an email account to send emails
- Roles and associated privileges needed by users of the HP User Behavior Analytics platform

Minimum Hardware Specifications

HP UBA is a high performance application and the system should meet the recommended hardware specification for an optimal experience

	Minimum (test environment)	**Mid-Range** (POC or small implementations)	**Optimum**	**High Performance**
RAM	16 GB	32 GB	64 GB	128GB
Processors	8 cores	16 cores	32 cores	64 cores
Hard Disk	500 GB	1TB	2TB	4TB
Architecture	64-bit architecture recommended.			

Supported OS

The application supports Red Hat Enterprise Linux (RHEL) v6.5 and CentOS Linux v6.5.

Supported Browsers

The application can be launched using any of the following browsers:

- Firefox 10.x and latest
- Internet Explorer 9, 10, 11
- Safari (latest)
- Chrome (latest)

Note: If you are using Internet Explorer 10, please turn off compatibility mode

Required Communication Ports

1. Port for MySQL – Default port for MySQL is 3306
2. Tomcat Application Server Port – Default port for HTTP is 8080 and HTTPS is 8443
3. Optional Ports:
   - SSH port (Optional) – Port 22
     - UDP/TCP 53: DNS host name lookup – DNS is used for name lookup and event enrichment.
     - DHCP/port 67: DHCP/bootstrap protocol server is not needed when static IP addressing is used
     - UDP 514 used for syslog server set up.
     - ICMP type 8 only for server monitoring.
     - Get identity data from systems: connectivity varies by identity store, for example: LDAP/389 LDAPS/636 to Active Directory

Prerequisite – MySQL Installation

Before running the HP UBA product installer (HPUBA10.bin), please make sure MySQL is pre-installed and configured on the Linux server (RHEL and CentOS 6.5). If some of these items are not installed or misconfigured, the installer will let you know during installation.

Install MySQL 5.6

- `root> wget http://dev.mysql.com/get/mysql-community-release-el6-5.noarch.rpm`
- `root> rpm –Uvh mysql-community-release-el6-5.noarch.rpm`
- `root> yum install mysql-server`

Set up MySQL to Start at Boot Time

- `root> chkconfig mysqld on`

Modify my.cnf file

- `root> vi /etc/my.cnf`

  Add the following lines in the [mysqld] section:

  - `lower_case_table_names=1`

    If set to 0, table names are stored as specified and comparisons are case sensitive. If set to 1, table names are stored in lowercase on disk and comparisons are not case sensitive. If set to 2, table names are stored as given but compared in lowercase.

  - `innodb_file_per_table = 1`

Start MySQL

- `root> service mysqld start`

Enable MySQL Connections from Specific IP Addresses or Hostnames

Note: replace terms with those specific to your configuration:

- `grant all on *.* to ‘root’@‘192.168.1.1’ identified by ‘password’;`

or

- `grant all on *.* to ‘root’@‘myhostname’ identified by ‘password’;`

After either grant statement, above, run “`flush privileges;`”.

Change MySQL Data Directory

If MySQL has previously been installed on the hardware, or if you need to allocate more disk space for MySQL, please follow the steps described below (commands are shown running as root):

1. Shutdown MySQL

   ```
   >> service mysqld stop
   ```

2. Create a backup of my.cnf

   ```
   >> cp /etc/my.cnf /home/securonix/my.cnf.bak
   ```

3. Create a folder called “data” in /storage

```
>> chmod 755 /storage
>> mkdir /storage/data
```

4. Move contents of MySQL to the new data storage

```
>> mv /var/lib/mysql /storage/data/
```

5. Change ownership of the “data” folder to mysql (recursively)

```
>> chown -R mysql:mysql /storage/data
```

6. Change the data directory and socket to the new location in /etc/my.cnf
7. Start MySQL

```
>> service mysqld start
```

Recommended Best Practice

Configure the host name and ensure it resolves in DNS. HTTPS/SSL certificates are recommended for secure access, and must exactly match the host name during connectivity. Using the hostname will allow for IP address changes later without re-configuration of SSL certificates.

Installation Steps

The HP UBA software should be installed by a non-root user. To create a non-root user, open a terminal session and run the following commands:

1. `useradd HPUBAuser` (for example – user whatever user name you want)
2. `passwd HPUBAuser` (give your non-root user a password)

In order for Syslog-ng installation to proceed, the user needs to provide the SUDO password in installer screen. Since the installation binary is started as non-root user, this information needs to be provided in the sudoers file

3. Login as root and go to /etc/

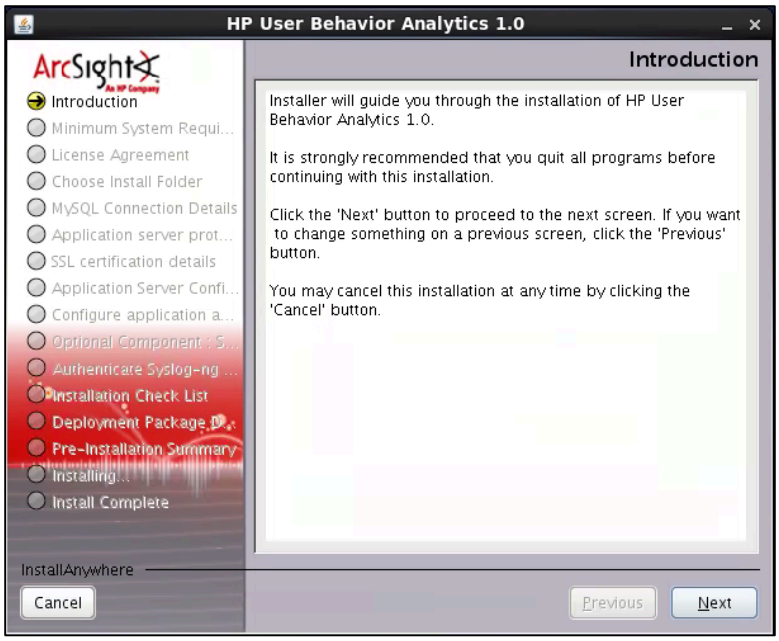
   ```
   vi sudoers
   ```

4. Scroll down through the sudoers file to the section below, add the user information for the non-root user that will start the installer (HPUBAuser from our example above) and save the file. Provide the non-root user password as `sudo` password on the installer screen.

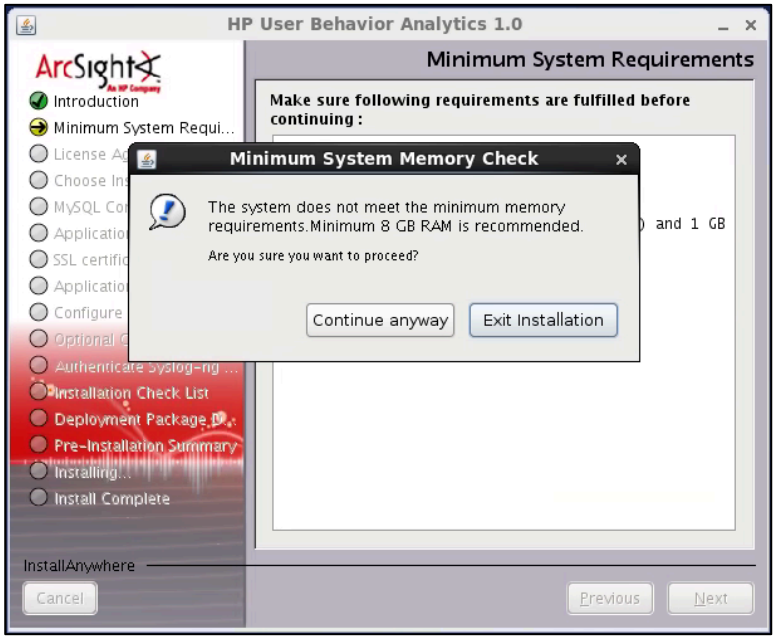
   ```
   ## Allow root to run any commands anywhere
   root ALL=(ALL) ALL
   HPUBAuser ALL=(ALL) ALL

   ## Allows members of the 'sys' group to run networking, software,
   ## service management apps and more.
   # %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE,
   DRIVERS

   ## Allows people in group wheel to run all commands
   ```

5. In order to begin the installation of HP UBA application, open a terminal and execute the following command:

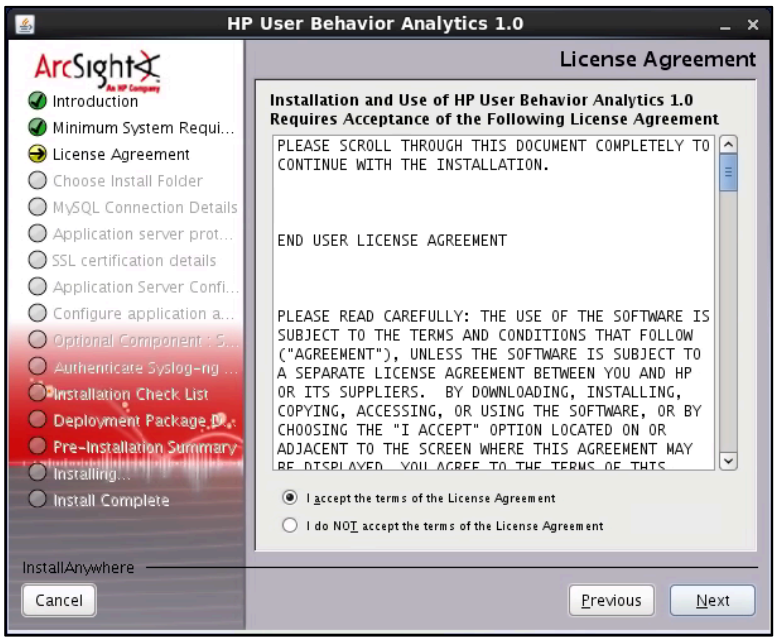
   ```
   ./HPUBA10.bin
   ```



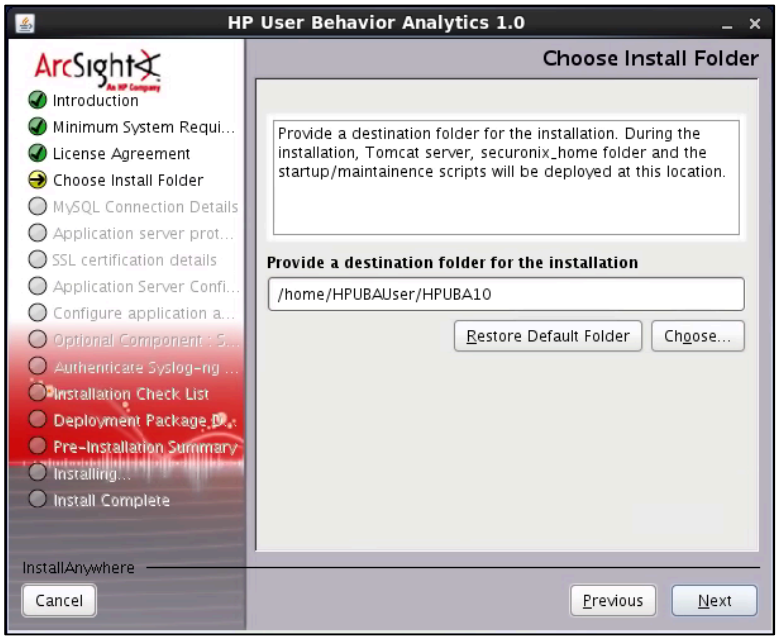
6 Review system requirements, and continue. If your system does not meet minimum requirements, you may accept the risk, but the installation may not be supported. The following warning screen will appear.



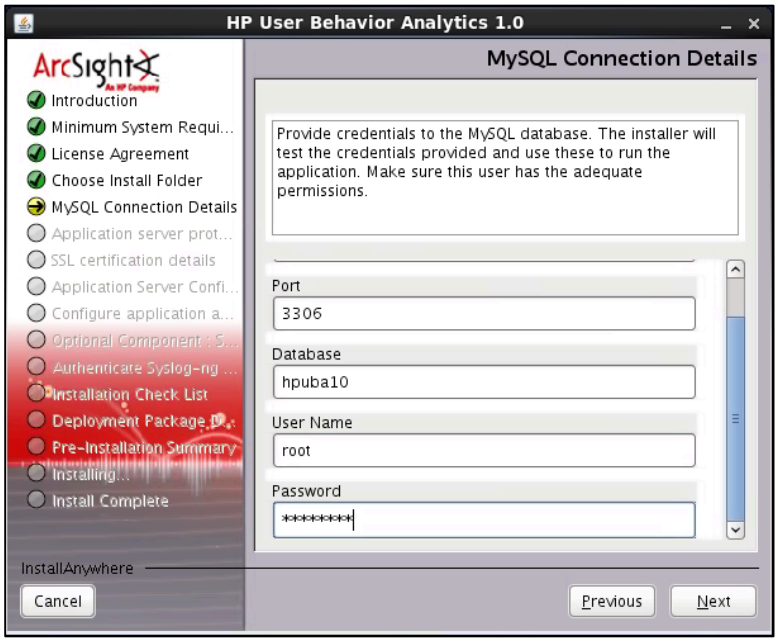
7 On the license screen, read and scroll to the bottom of the license, to enable and check the “I accept…” button.



8 Select the location to install the files to and click **Next**. The default will install files to an HPUBA subdirectory in the home directory of the currently logged in user.

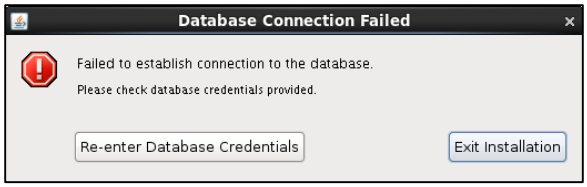


9 Modify your MySQL settings to include the system DBA user and password and port modifications as necessary, and click **Next**. The database will be created on the MySQL instance specified.

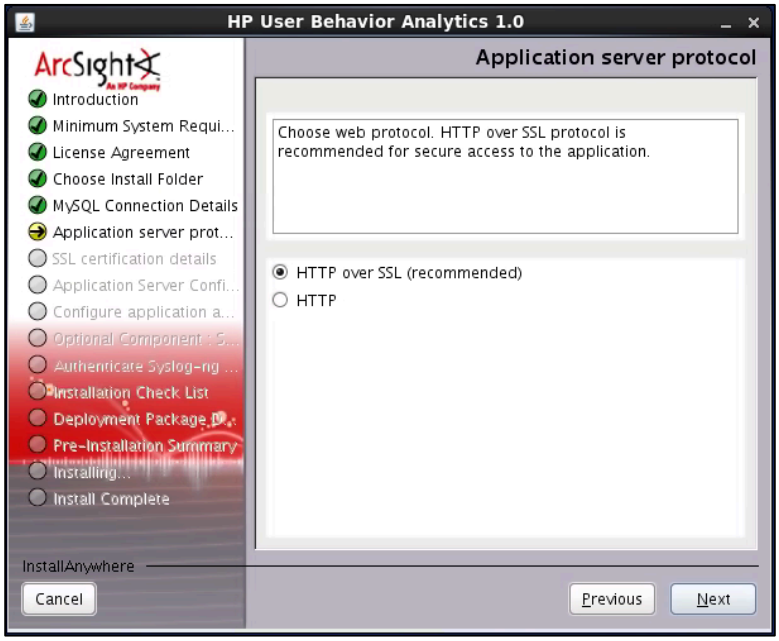


The credentials supplied will be tested for valid connectivity.

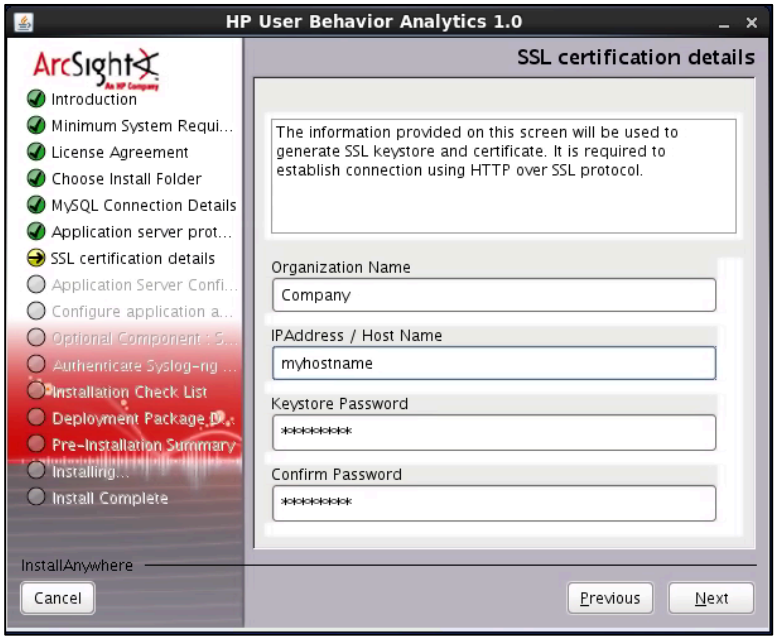
You will receive the following screen if the connection to MySQL fails. Correct the host/user/password as needed and re-enter the credentials to proceed.



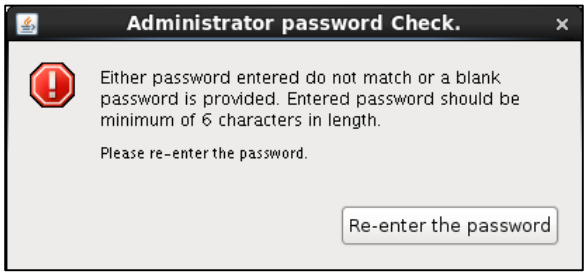
10 Select the connection protocol to be used. HTTPS is recommended for secure communications.



11 Enter the credentials for the HP UBA administrative user (this account will be used for login using a browser).

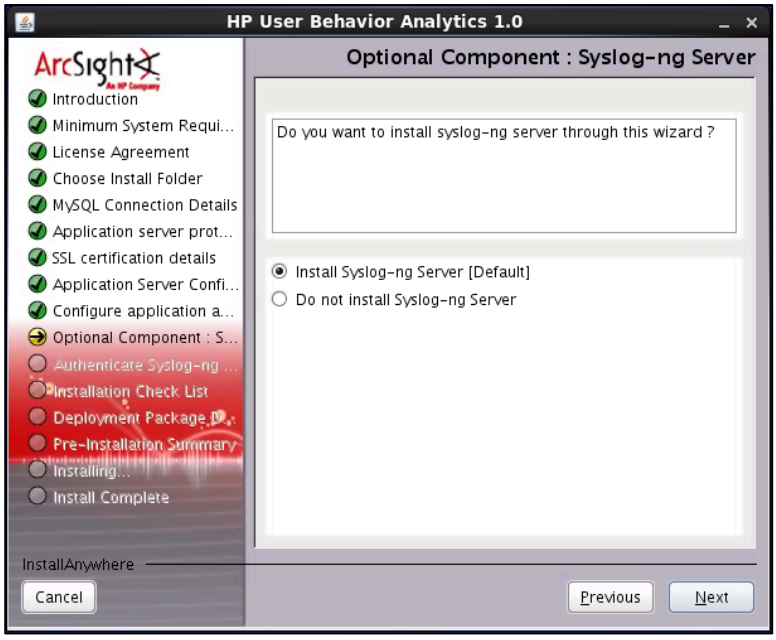


12 Password must be a minimum of 6 characters. You will get an error screen if you do not meet this requirement:

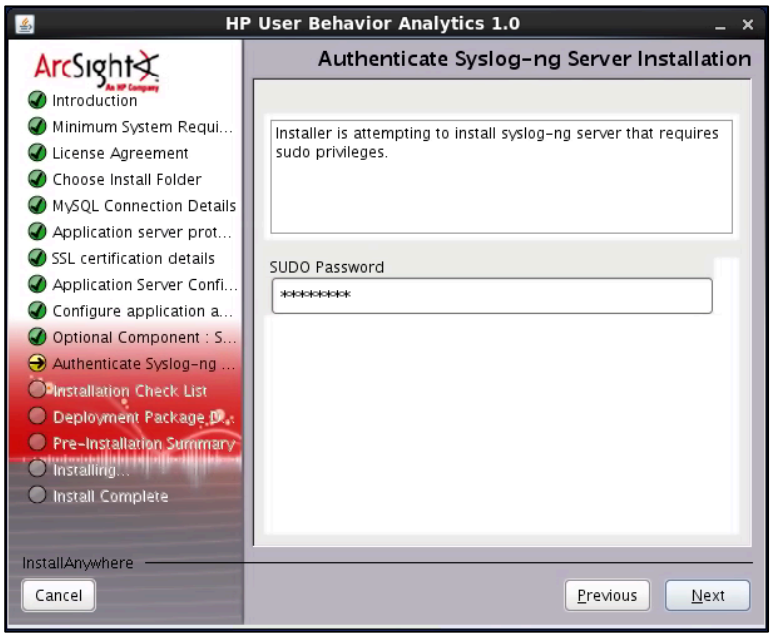


13 Configure Syslog-NG

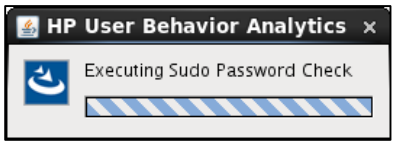
HP UBA requires Syslog-ng server to be running. If you do not already have it installed, the installer will install it by default as part of the process.



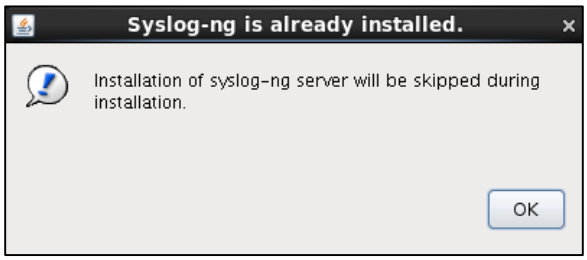
14 Enter the SUDO password (required to configure a service).



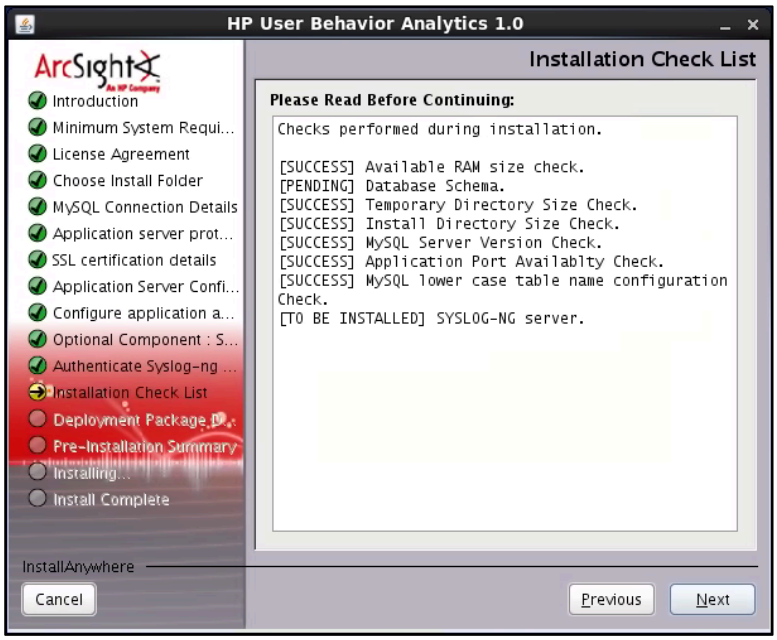
15 The installer will check the SUDO password before continuing:



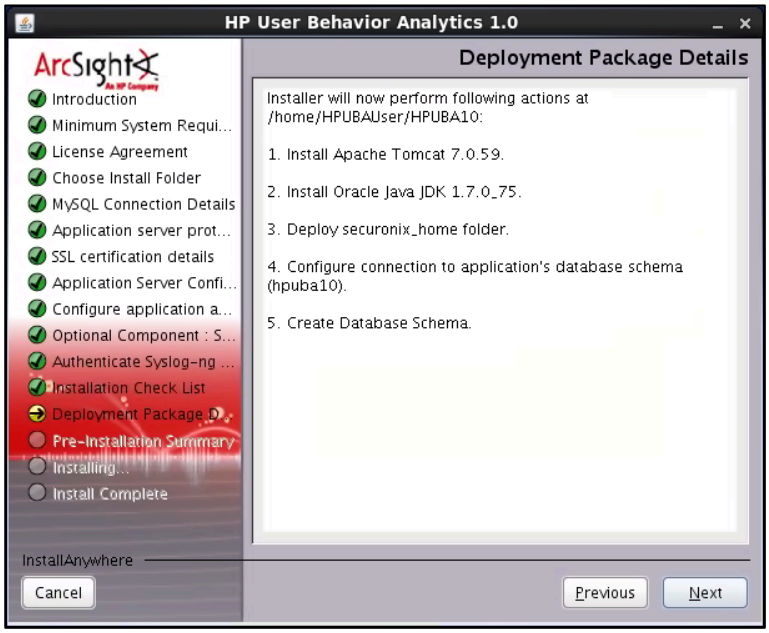
16 If syslog has already been installed, the system will show the following screen, and this step can be skipped.



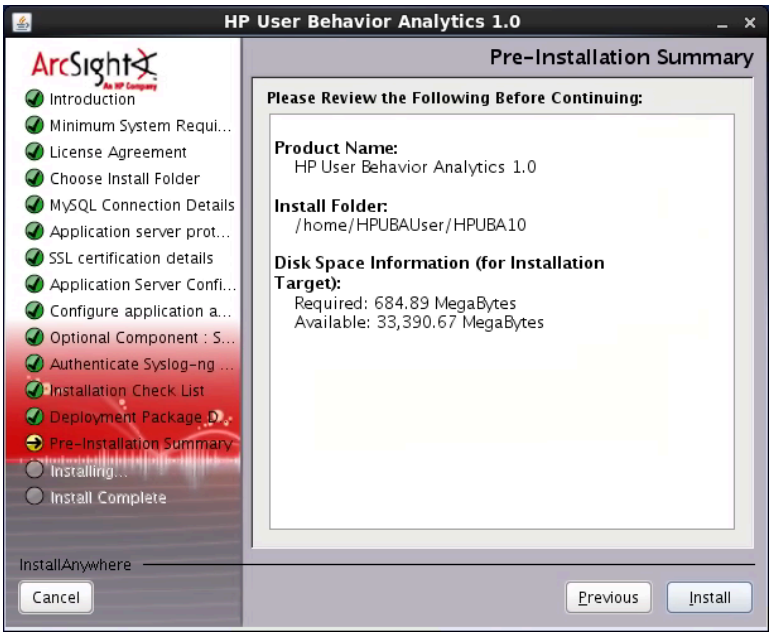
17 The system will show a summary of installation checks. Select **Next** to continue.



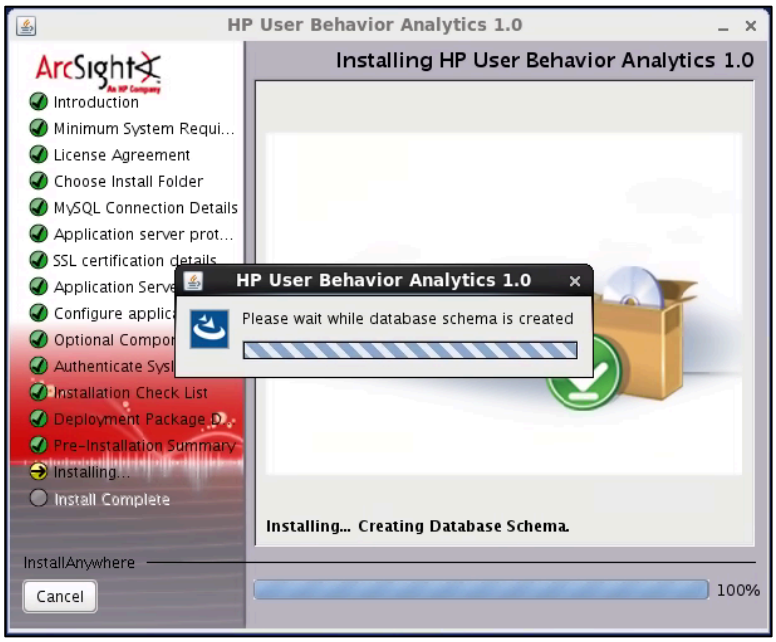
18 A final check screen will appear showing scripts and configurations to be executed. Select **Next** to continue.



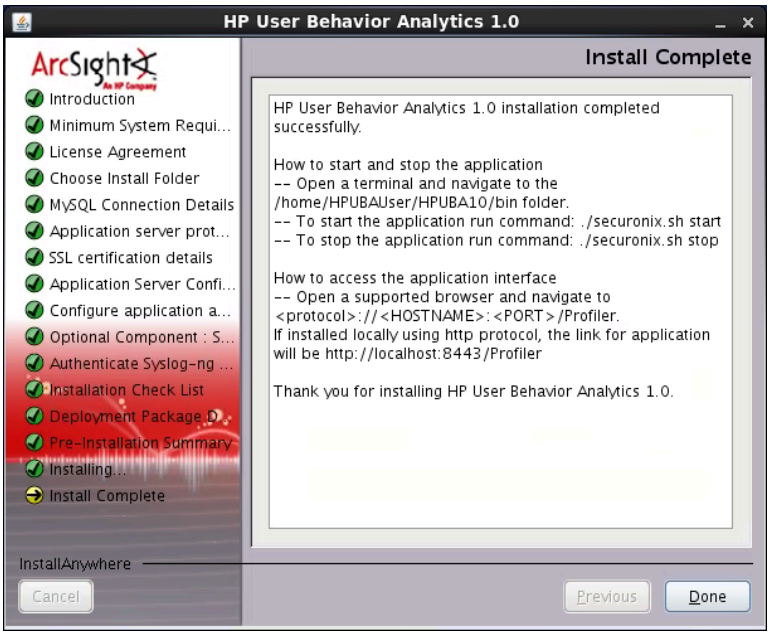
19 Final installation screen. Select **Next**.



20 Additional components will be installed. After the status bar shows 100% you should see an installation complete screen. The HP UBA database and schema will be created. The time required will vary based on hardware performance.



21 Successful installation – Summary Screen. Click **Done** to continue.



22 Start the HP UBA application from a command line, by running:

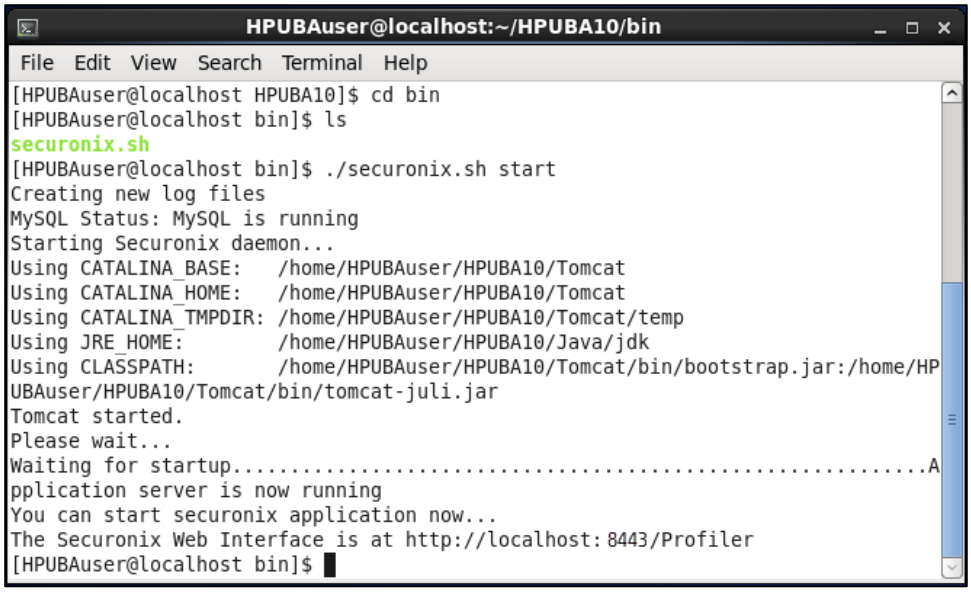
```
./securonix.sh start
```

Start, stop or restart the application with the commands as shown below:

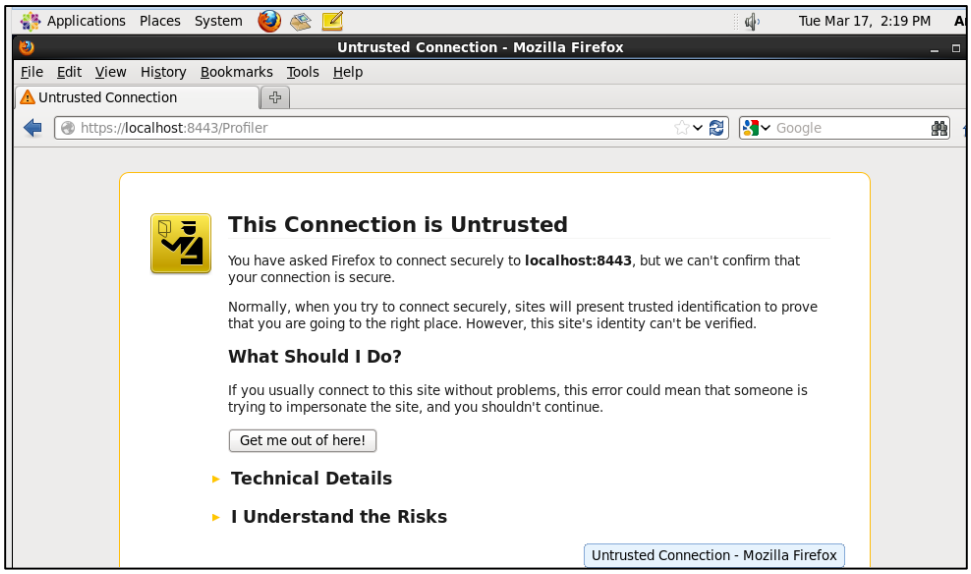
```
[HPUBAUser@localhost bin]$ ./securonix.sh
Usage : To start Securonix Application   - ./securonix.sh start
        To stop Securonix Application    - ./securonix.sh stop
        To restart Securonix Application - ./securonix.sh restart
[HPUBAUser@localhost bin]$
```

When startup has completed, you should see the following message:

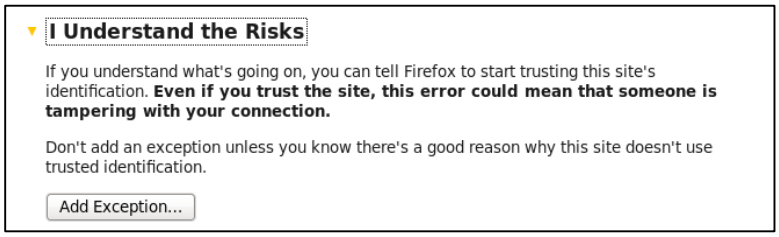
The Securonix Web Interface is at …

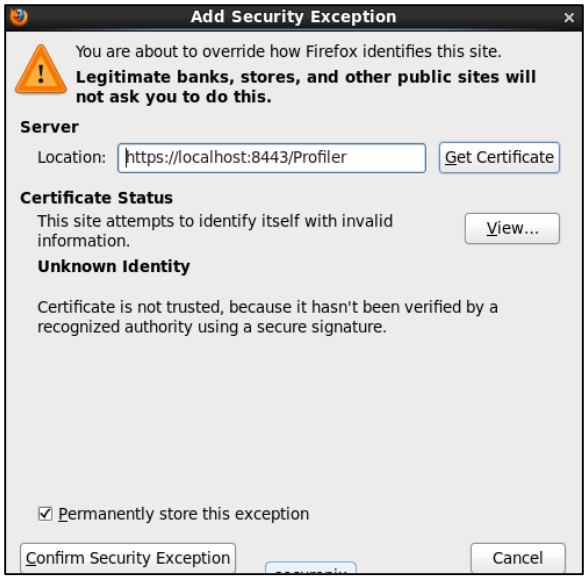


23 Validate the installation by connecting to the URL shown at the end of the startup script.

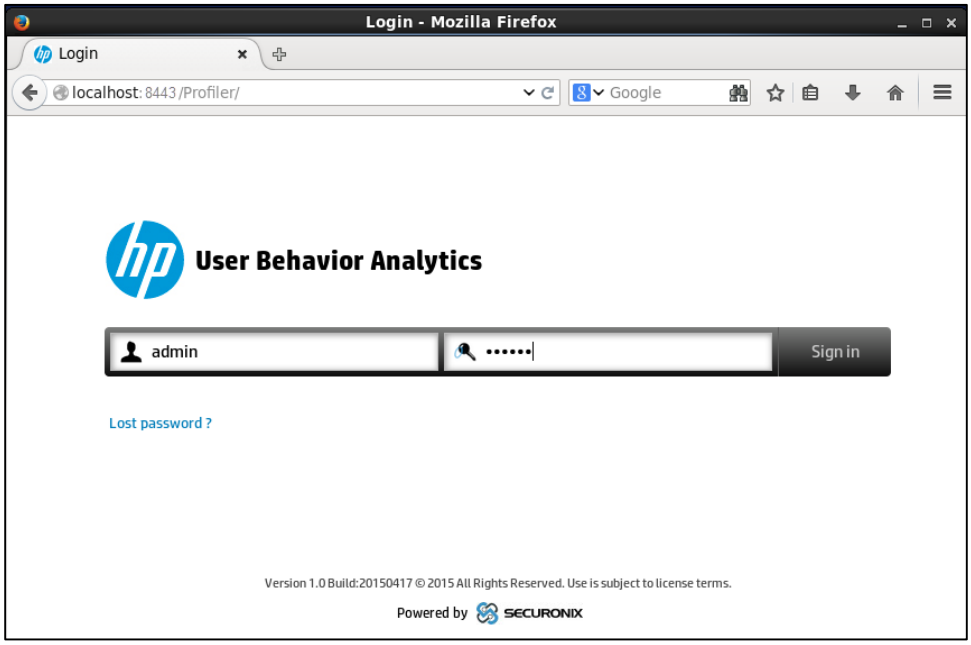


24 Accept and add an exception for the self-signed certificate of the host you have just configured.

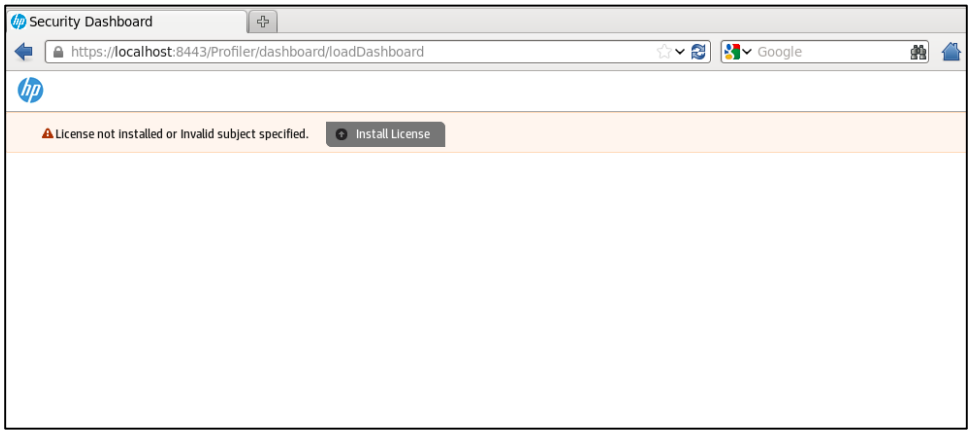




25 Login to the system using the admin user and password configured earlier during the installation.



26 On the first installation you should see the following screen. You will need to install the license provided to continue. Select the **Install License** option.



27 Select the *.lic file provided with your licensing agreement

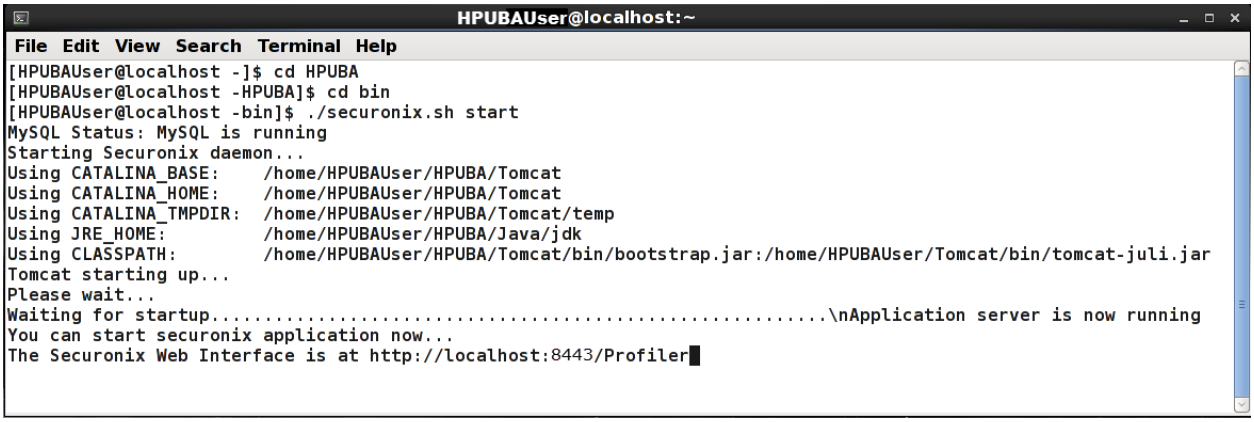
28 After installing the license, you'll be returned to the login screen.

Chapter 4: Post Installation Activities

Start Using the Application

Open a terminal, and navigate to the /bin/ folder of your UP UBA installation. (In our installation sample, that folder is **/home/testus/HPUBA/bin**.)

Start the application with the command **./securonix.sh start**



Once the application starts, you can open your favorite browser and navigate to **http://ipaddress:portnumber/Profiler**

Chapter 5: Uninstall HP UBA

Should you need to uninstall the application, follow these steps:

1 To remove the application, first be certain that you have stopped the application.

(**Note**: if you would like the uninstaller to delete the database schema as well, please make sure to keep MySQL running.)

2 To stop the HPUBA application, log out of any open web sessions, open a terminal session and type:

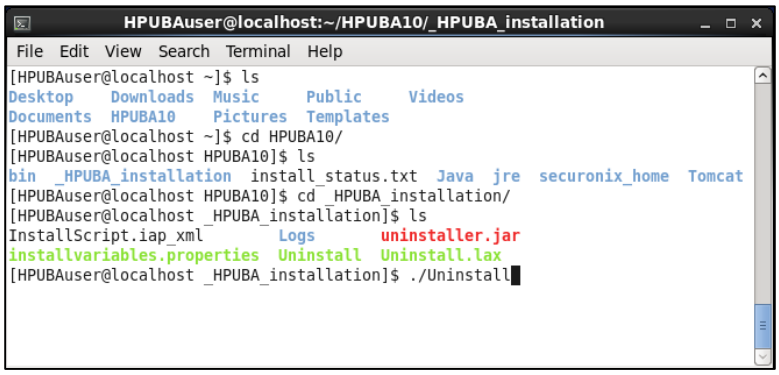
```
./securonix.sh stop
```

3 Next, navigate to the folder where the application is installed, then to the **_HPUBA_installation** (if you accepted the defaults during installation) folder. Example:

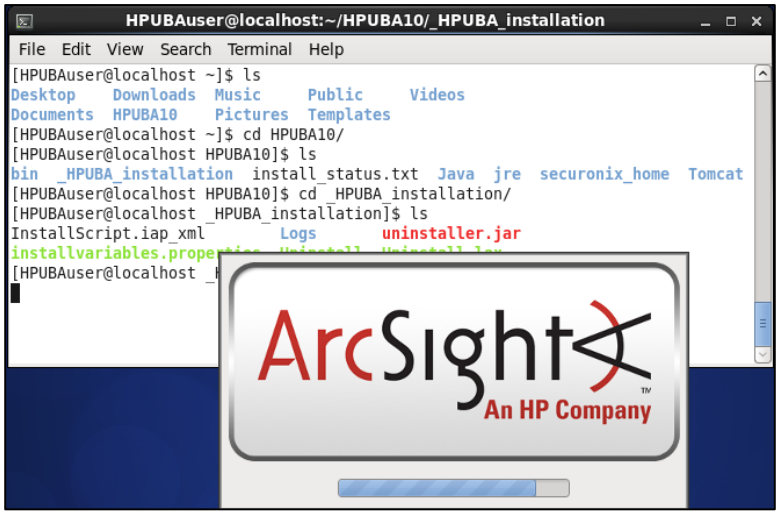
```
cd HPUBA
cd _HPUBA_installation
```

Issue the following command:

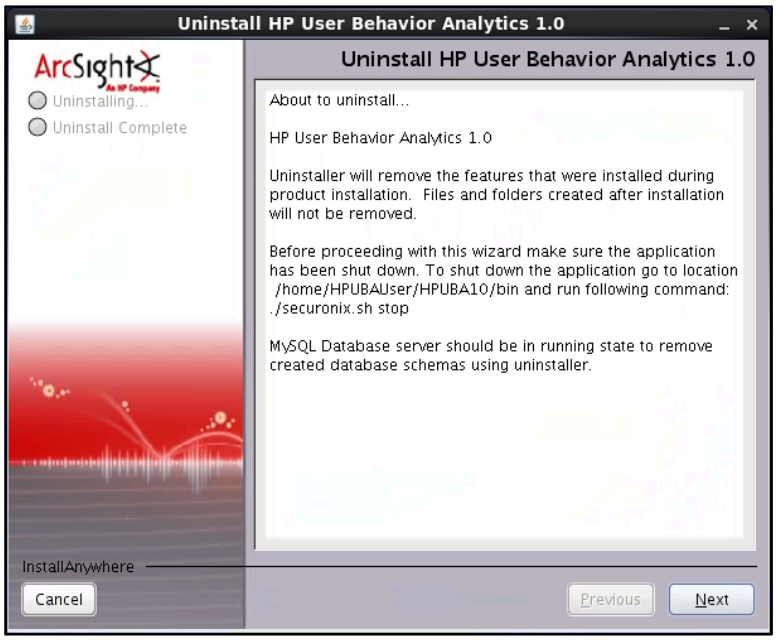
```
./Uninstall
```



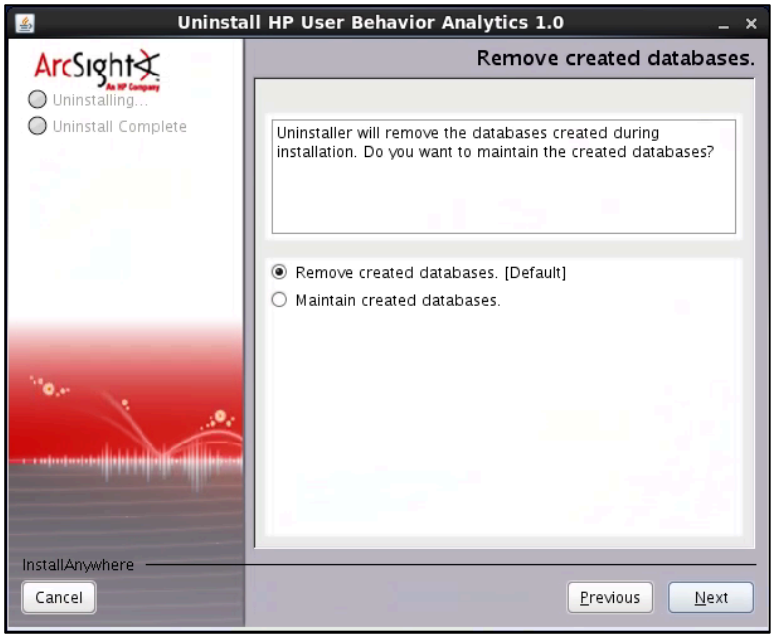
This will start the uninstallation wizard:



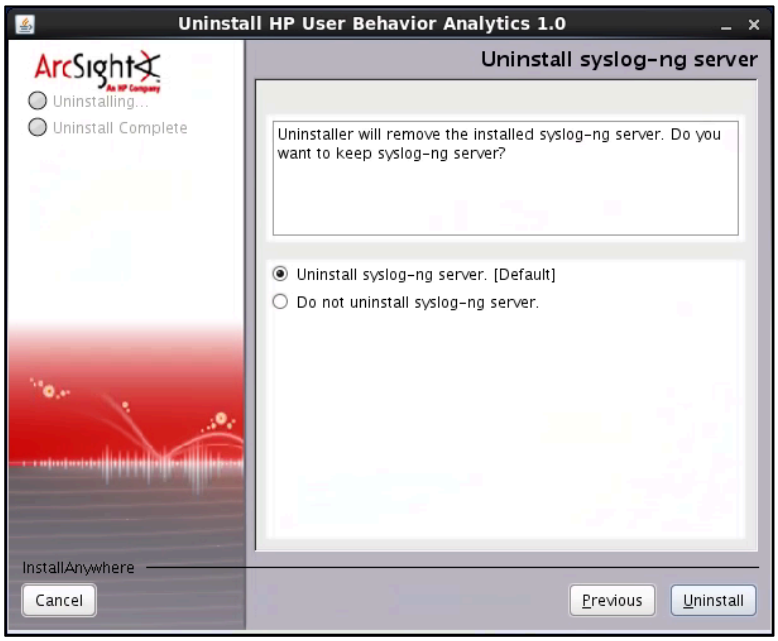
4 Click **Next** to start the uninstall process.



5 Select the option to remove or keep databases as part of the uninstall process.

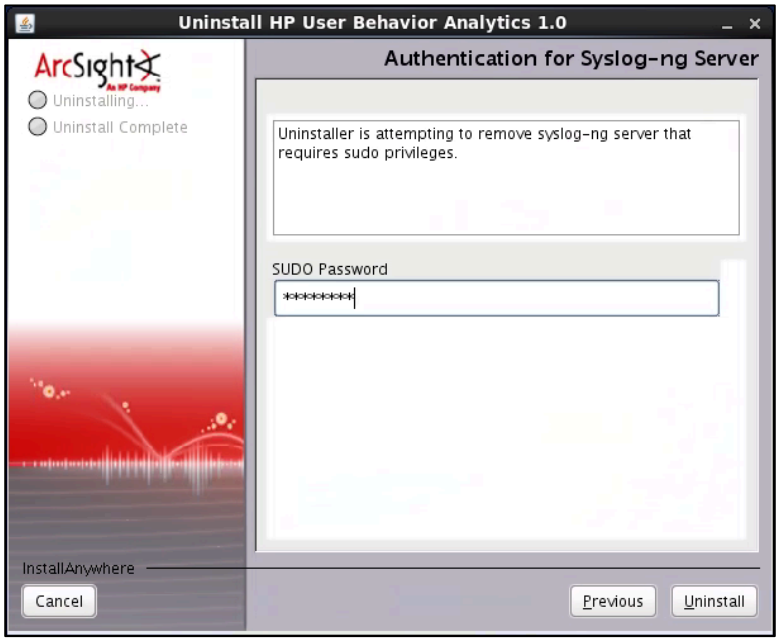


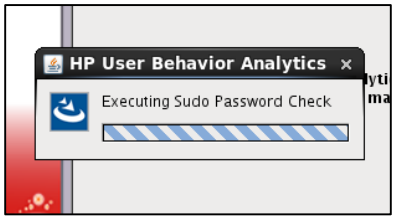
6 Select the option to remove Syslog or leave it in place during the uninstall process.

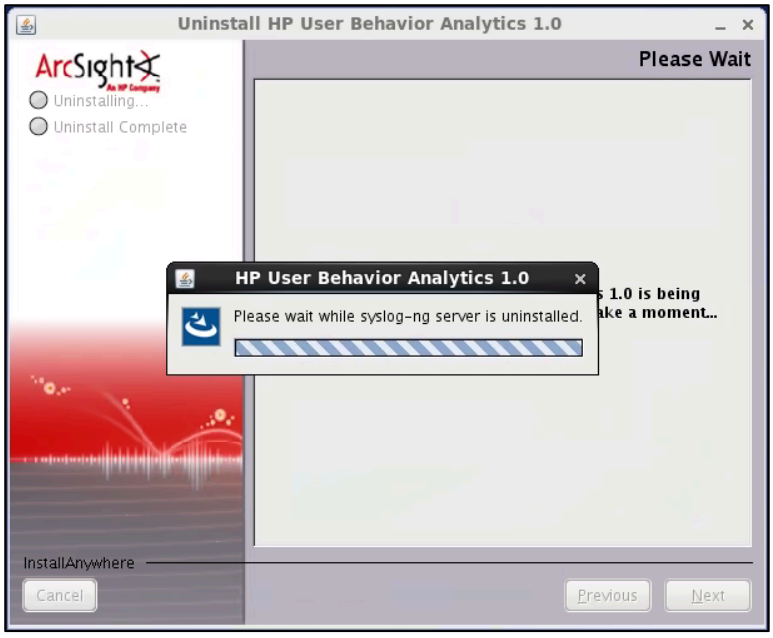


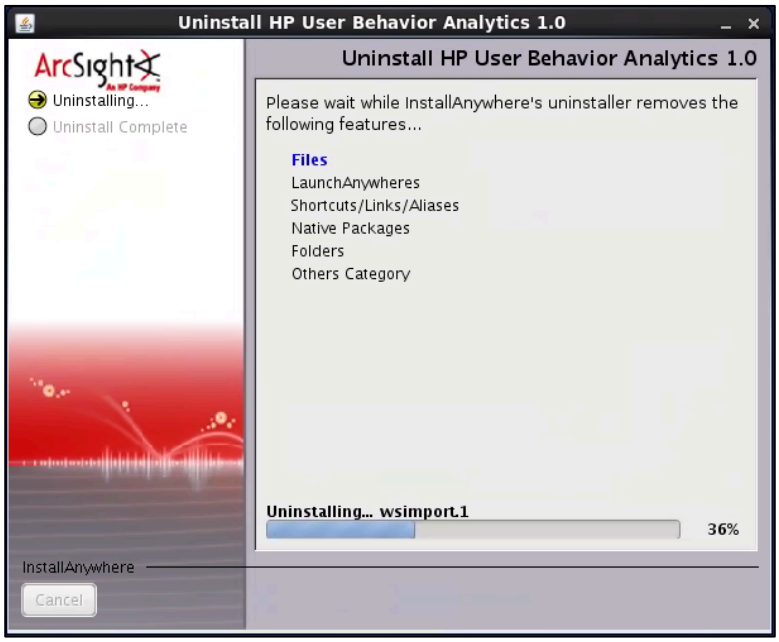
7 Click **Uninstall** to execute.

8 The uninstaller will ask for and verify the SUDO password. Enter it and click **Uninstall**.

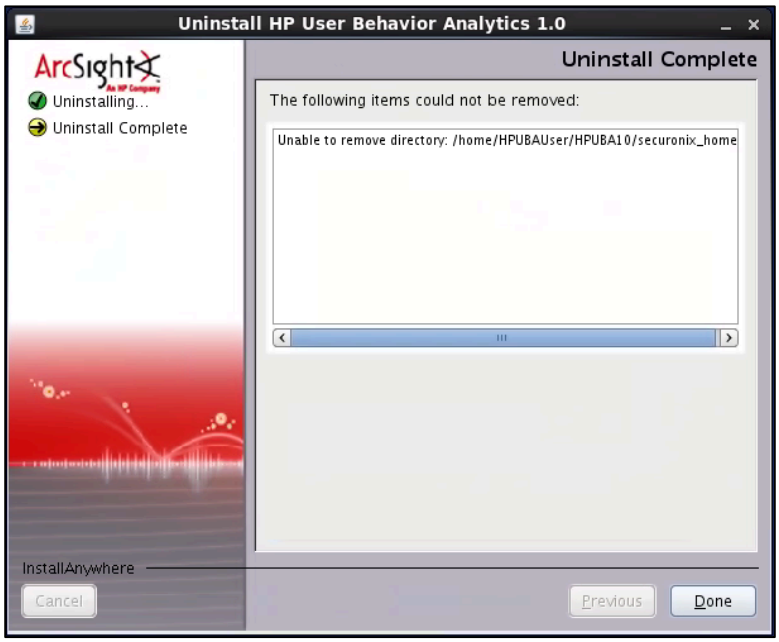





Uninstall HP User Behavior Analytics 1.0
ArcSight
Uninstalling...
Uninstall Complete
Please Wait
HP User Behavior Analytics 1.0
Please wait while syslog-ng server is uninstalled.
InstallAnywhere
Cancel
Previous
Next


Uninstall HP User Behavior Analytics 1.0
ArcSight
Uninstalling...
Uninstall Complete
Uninstall HP User Behavior Analytics 1.0
Please wait while InstallAnywhere's uninstaller removes the following features...
Files
LaunchAnywheres
Shortcuts/Links/Aliases
Native Packages
Folders
Others Category
Uninstalling... wsimport.1
36%
InstallAnywhere
Cancel

9 When the process is complete, you can remove the HPUBA10 and any underlying folders manually.



Appendix A: Tuning MySQL Configurations

Consider the following parameters when tuning your MySQL configuration:

Key_buffer

Change this parameter based on the amount of RAM in the system. Ideally, it should set at 20% of free memory available.

Key_buffer_size

Change this parameter based on the amount of RAM in the system. Ideally, it should set at 20% of free memory available.

Sort_buffer_size

This is a memory buffer used when ordering is required (Group By, Order By). Increasing the sort_buffer_size means allowing more memory to be used for the sorting process. However, increasing the sort_buffer_size can be detrimental to performance because the full size of the sort buffer is allocated for each thread that needs to do a sort, even if a large sort buffer is not required.

Read_buffer_size

This parameter is used for caching the indexes in a temp file when sorting rows, bulk insert into partitions or caching results of nested queries. Set to a value in multiples of 4. If you do many sequential scans, you might want to increase this value from the default value which is 131072.

Read_rnd_buffer_size

Setting the variable to a large value can significantly improve ORDER BY performance. Change the variable only from within those clients that need to run large queries.

Join_buffer_size

This is the minimum size of the buffer that is used for plain index scans, range index scans and joins that do not use indexes and thus perform full table scans. Increase the value of join_buffer_size to get a faster full join when adding indexes is not possible.

max_heap_table_size:

This parameter should be set at the available RAM divided by the maximum number of connections (max_connections).

Tmp_table_size:

This parameter should be set at the available RAM divided by the maximum number of connections (max_connections).

Myisam_sort_buffer_size

This is the size of the buffer allocated when sorting indexes during a REPAIR TABLE or when creating indexes with CREATE INDEX or ALTER TABLE. The default size is 8 MB and the max size is platform dependent.

Query_cache_size

This is the amount of memory allocated for caching query results. The default value is 0, which disables the query cache. The permissible values are multiples of 1024.

Thread_concurrency

This function enables application to give the threads system a hint about the desired number threads that should be run at the same time.

Innodb_buffer_pool_size

The size in bytes of the memory buffer InnoDB uses to cache data and indexes of its tables. The default value is 8MB. The larger you set this value, the less disk I/O is needed to access data in tables. On a dedicated database server, you may set this to up to 80% of the machine's physical memory size. However, do not set it too large because competition for physical memory might cause paging in the operating system. In addition, the time to initialize the buffer pool is roughly proportional to its size.

innodb_additional_mem_pool_size

The size in bytes of a memory pool InnoDB uses to store data dictionary information and other internal data structures. The more tables you have in your application, the more memory you need to allocate here. The default value is 1MB.

innodb_flush_log_at_trx_commit

- If the value of innodb_flush_log_at_trx_commit is 0, the log buffer is written out to the log file once per second and the flush to disk operation is performed on the log file, but nothing is done at a transaction commit.
- When the value is 1 (the default), the log buffer is written out to the log file at each transaction commit and the flush to disk operation is performed on the log file.
- When the value is 2, the log buffer is written out to the file at each commit, but the flush to disk operation is not performed on it. However, the flushing on the log file takes place once per second also when the value is 2.
- The default value is set to 1.

innodb_file_per_table

If innodb_file_per_table is disabled (the default), InnoDB creates tables in the shared tablespace. If innodb_file_per_table is enabled, InnoDB creates each new table using its own .ibd file for storing data and indexes, rather than in the shared tablespace.

Max_allowed_packet

It is safe to increase the value of this variable because the extra memory is allocated only when needed. For example, mysqld allocates more memory only when you issue a long query or when mysqld must return a large result row. The small default value of the variable is a precaution to catch incorrect packets between the client and server and to ensure that you do not run out of memory by using large packets accidentally. The default value is 16MB and can go up to 1GB.