Avaya Identity Engines Ignition Analytics

Avaya Identity Engines Ignition Server
Release 8.0

Document Status: **Standard**

Document Number: **NN47280-601**

Document Version: **03.01**

Date: **April 2012**

Avaya Identity Engines Ignition Server

Release: 8.0

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support

TABLE OF CONTENTS PAGE

INTRODUCTION **5**

ABOUT THE PRODUCT GUIDE 5
ABOUT THE IDMS BASED PRODUCT – IGNITION ANALYTICS 5

CHANGES IN IGNITION ANALYTICS RELEASE 8.0.0 .... **5**

INSTALLING THE APPLICATION **6**

BEFORE YOU BEGIN 6
SYSTEM REQUIREMENTS 6
Application Server Hardware *6*
Browser Compatibility *7*
Ignition Server Compatibility *7*
INSTALL THE IGNITION ANALYTICS APPLICATION 7
Install the Third Party Applications *9*
Ignition Analytics *10*
CONFIGURE IGNITION ANALYTICS 10

ACCESSING THE APPLICATION **10**

UPGRADING VERSION 7.0.0 TO 8.0.0 .... **12**

MANAGING YOUR IGNITION ANALYTICS APPLICATION **14**

APPLICATION ADMINISTRATION 15
Administration *15*
Company Settings 15
Company Profile 15
SFTP Settings 16
Data Import Settings 17
Mail Settings 19
Manage Users 20
Manage Roles 21
Manage User Roles 22
Data Switch 22
Repository Management *22*
Setup Identity Engines Ignition Server *24*
Data Import *25*
About the Data Import Process 25
Manage Data Import Schedule 25
The Data Import Scheduler 26
Setup Data Import Schedule 26
Monitor Data Import Events 28
APPLICATION USERS 28
Custom Reports *29*
User Defined Report 29
Select Report Data Elements 29
Summary Options 31
Parameters 31
Report Preview 32

Schedule User Defined Report ... 33
Analytics ... 33
Select Analytic Criteria ... 33
Parameters ... 36
Schedule Analytic ... 37
Reports Management ... *38*
Manage the Report Generation Schedule ... 38
Schedule Report Generation ... 38
Set up a Report Generation Schedule ... 38
Monitor Report Generation Events ... 42

APPENDIX A ... 43

TERMINOLOGY ... 43
SYMBOLS AND TYPEFACES ... 43

APPENDIX B ... 45

TROUBLESHOOTING TIPS ... 45
During Application Installation ... *45*
During Application Access ... *45*
CopSSH Setup ... *47*

APPENDIX C ... 48

SAMPLE REPORTS ... 48

INTRODUCTION

ABOUT THE PRODUCT GUIDE

This Product Guide provides an overview for the management of this iDMS based product, providing information for installation, configuration and maintenance of the iDMS based product and its operations. This information is intended to be used as a reference for your product documentation.

ABOUT THE IDMS BASED PRODUCT – IGNITION ANALYTICS

Avaya Ignition Analytics (Ignition Analytics) is an iDMS based product (The Application) which presents Avaya Ignition Server's (Ignition Server) network authorization and authentication information in a variety of summary and detail reports in the areas of audit, compliance, security and usage.

Ignition Analytics is a web based application installed on a server and accessed via a web browser for management, reporting and analysis of information.

Ignition Analytics receives Access logs from Ignition Server and processes these logs for delivering standard and custom reports. The Application's core functions include flexible scheduling, delivery and distribution methods. Reports can be generated in PDF, HTML, rich text, and MS Excel file formats and delivered to users' via email or accessed and shared within The Application.

The key benefits of Ignition Analytics are that it can be used to monitor and plan changes and the growth of your current networking environment. The reports can be used to improve decision making and business analysis. The benefits of Ignition Analytics include:

- Assist in capacity planning - Are we meeting the networking needs/service level of our organization?
- Identify device usage - Who are the top users?
- Create audit trails – Look for trends of usage, users, and devices
- Increase visibility into activity level over time, identifying peak usage, lowest usage

(See "Appendix C" for sample reports)

CHANGES IN IGNITION ANALYTICS RELEASE 8.0.0

Avaya Ignition Analytics Release 8.0.0 changes include the following:

1. IA8.0.0 support the addition of 5 attributes to the Access log:
   - The Ignition Server Export Log files parsed and processed by Ignition Analytics has the following filename convention: "<ipaddress>_Access_<year><month><day>_<hour><minute>_<starting recordId>.csv"
   - Ignition Analytics does not process any other Ignition Server Log Export files that may have been exported to the Ignition Analytics server.
   - Following are the additional device profiling attributes being sent as part of the Ignition Server release 8.0:
     - DeviceMAC
     - DeviceOSType
     - DeviceOSVersion
     - DeviceSubType
     - DeviceType

2. These attributes are added to the following two standard usage reports:
   - Usage Detail by Selected User
   - Usage Detail by User

3. The following GUI items are updated:
   - Update GUI look and feel.
   - Add “Ignition Analytics” at header

4. Add to report period selection the following two additional options:
   - “Year to Date”
   - “Last Year”

5. Data in sample database is updated to year 2011.

INSTALLING THE APPLICATION

The Application server performs information processing, report generation and delivery.

BEFORE YOU BEGIN

To install, you need:

- A PC running a supported Microsoft Windows Operating System with an NTFS file system partition. You will install Ignition Analytics and its supporting components on this PC. Ignition Analytics is currently supported on Microsoft Windows XP SP3 32-bit, Windows Server 2003 32-bit and Windows Server 2008 32-bit.
- The Ignition Analytics product, which contains:
    - Java SE Runtime Environment (JRE) Version 6
    - Apache Tomcat 6.0
    - PostgreSQL 8.3
    - CopSSH 3.1.1
    - Jasper Server 3.0
    - iDMS 3.1
    - Ignition Analytics

NOTE: Be sure that you are logged in as an Administrator with full administrative rights on the system.

NOTE: It is required that Ignition Analytics will be installed on its own dedicated Windows server. The Ignition Analytics does not support installation of other Identity Engines applications on the same server as Ignition Analytics.

SYSTEM REQUIREMENTS

APPLICATION SERVER HARDWARE

Minimum recommended hardware requirements for the application server machine that hosts the Application:

- 2+ GHz processor
- 2 GB RAM
- 3 GB minimum available hard drive space

NOTE: The hard drive space reflected above is only for the installed application. Be sure to increase the hard drive space based on storage requirements for data logs and level of application usage.

Browser Compatibility

The Application is compatible with the following Web browsers:

- Microsoft Internet Explorer, version 6.0 or later, running on Windows
- Firefox 1.5 or later, running on Windows

Ignition Server Compatibility

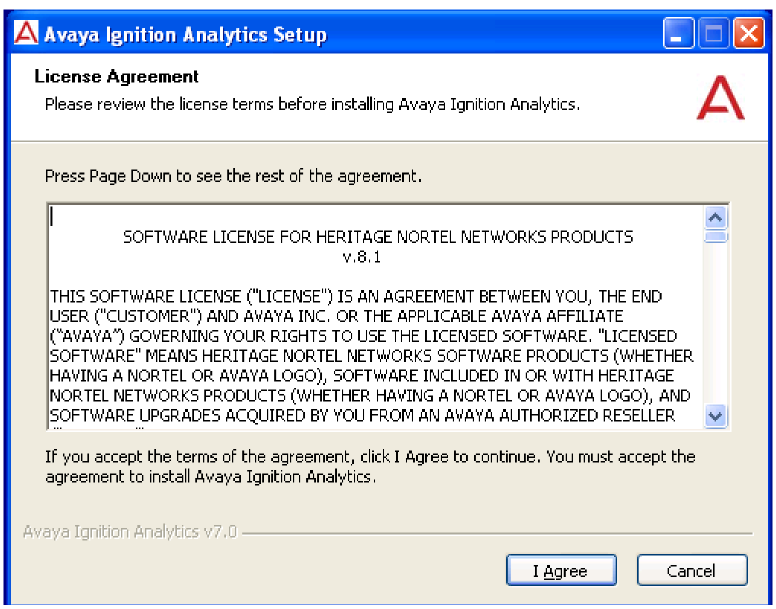
Ignition Analytics version v8.0.0 is compatible with Ignition Server version v8.0, Note that Ignition Analytics is not compatible with Ignition Server 7.0 release.

Install the Ignition Analytics Application

To install the Application, launch the executable file; the installer will guide you through the installation of required third party applications and The Application.

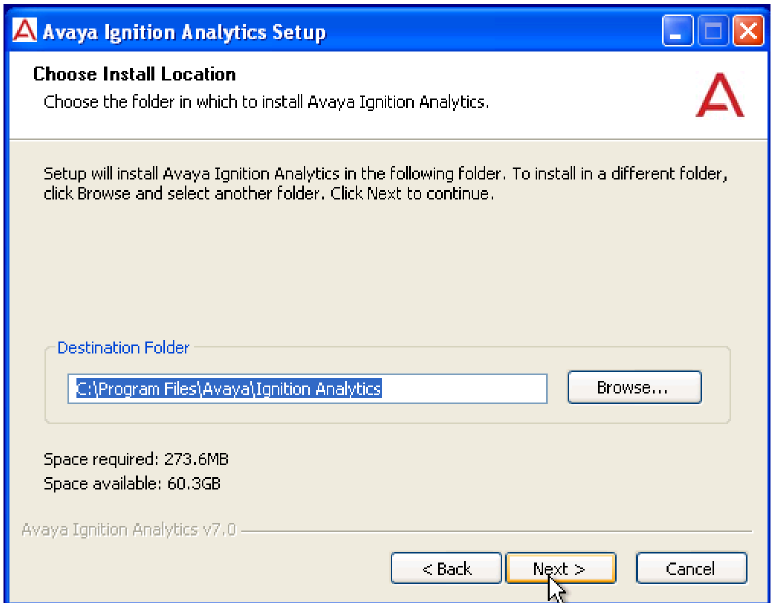
NOTE: It is advised that you save all other open application files and close these applications prior to beginning this installation.

You must accept the license agreement terms to proceed with the installation of the Application. After reading the license agreement, click the "I Agree" button to accept the license agreement to continue with the installation.

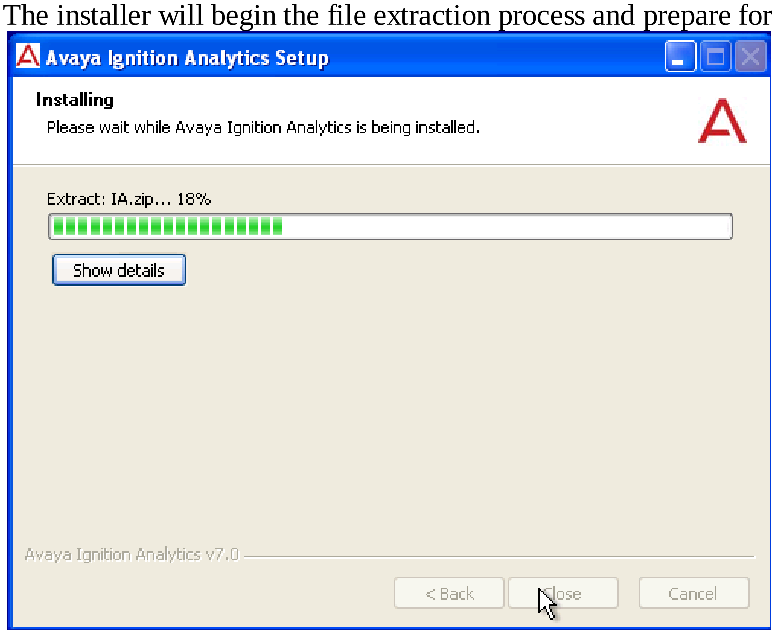


The default installation path for the Application is specified.

Click the Next button to continue with the installation.

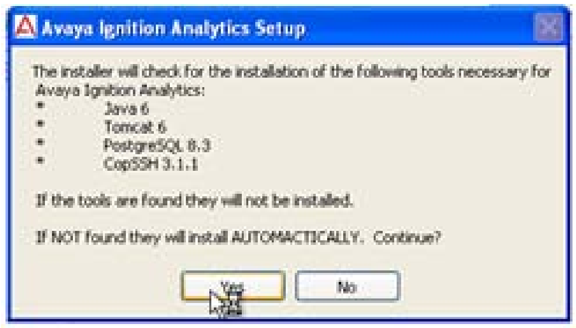


The installer will begin the file extraction process and prepare for installation.



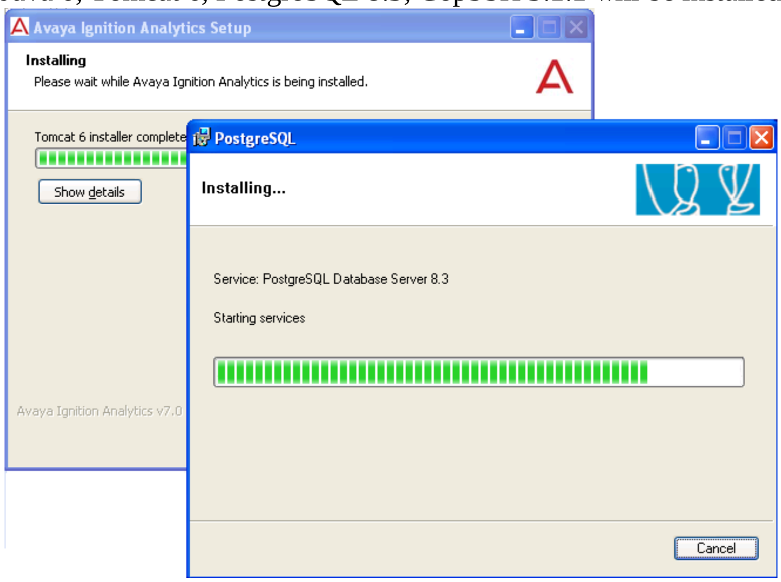
An information window will notify you of the third party applications it will search for.

Click Yes to continue.



INSTALL THE THIRD PARTY APPLICATIONS

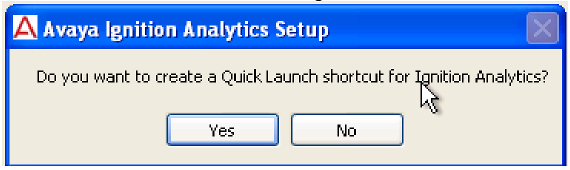
Java 6, Tomcat 6, PostgreSQL 8.3, CopSSH 3.1.1 will be installed in silent mode.



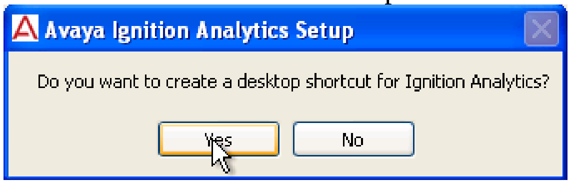
IGNITION ANALYTICS

The installer will continue with the remaining installation.

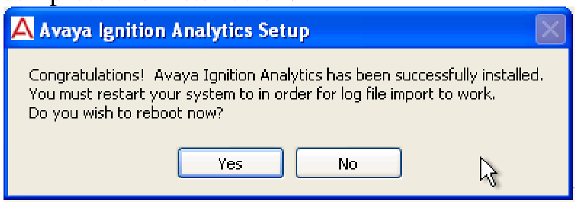
Click Yes to continue if a quick launch shortcut is desired on the taskbar.



Click Yes to continue if a desktop shortcut is desired.



Upon completion of the Ignition Analytics installation process, you will be asked to reboot your system. A system reboot is required for log file import to work. Select Yes to complete the installation.



CONFIGURE IGNITION ANALYTICS

There are several configurations specific for your system that will need to be set through The Application. Refer to Company Settings to set the configurations for The Application.

ACCESSING THE APPLICATION

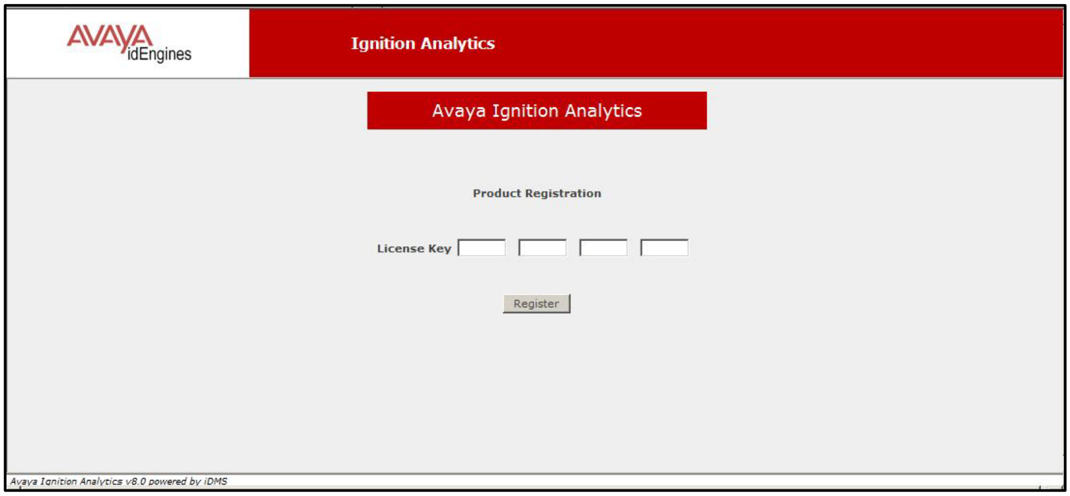
Connect to The Application and log in using the Username and Password provided. To connect and log in:

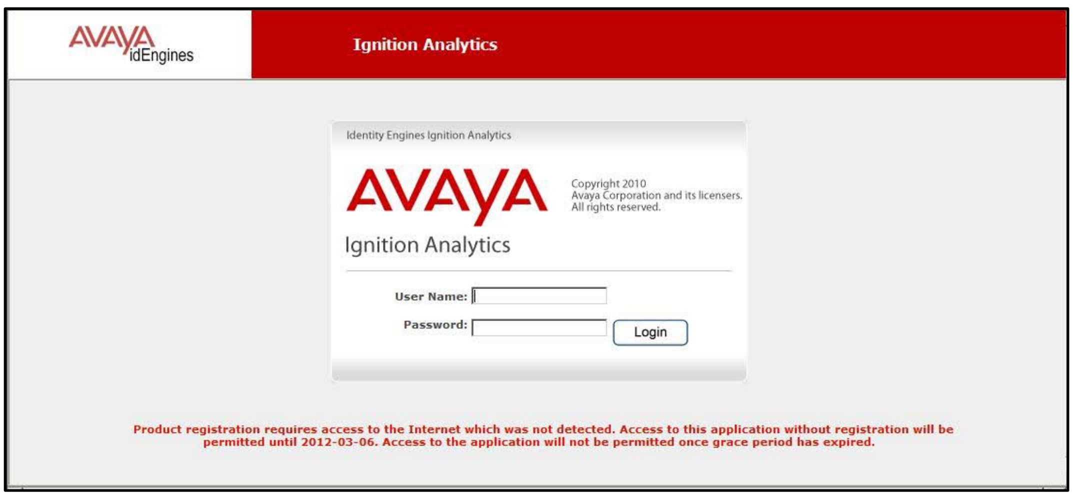
If you are connecting directly from the host system, click on the quick launch shortcut on the toolbar, or click on the desktop shortcut, or open a web browser and go to URL http://localhost:8080/IA

Or

If you are connecting from any other system, open a web browser, point the browser at the Tomcat server URL, and add "/IA" to the URL.

NOTE: If the system is newly installed, you will be prompted to enter your license key to register the application before you can access the application. **The system will need to be able to access the internet in order to complete the license key registration**, or device without internet access can access Ignition Analytics application before registration for 15 days.

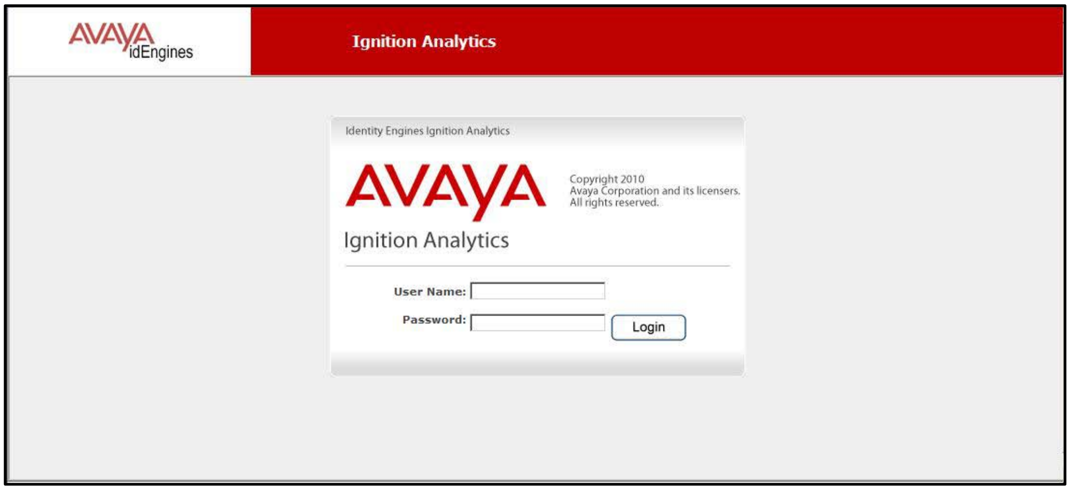




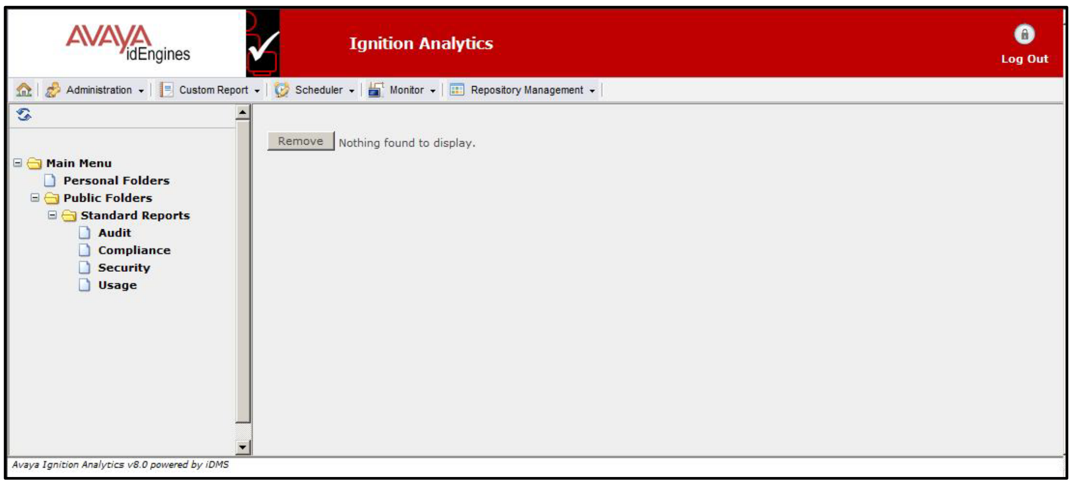
Enter the login credentials of the Administrator. By default, these are as follow, and can be modified using manage user function under administrator.

Username: **admin**

Password: **admin**



Click **Login**. The Ignition Analytics window appears and you are successfully logged into Ignition Analytics as the Administrator.

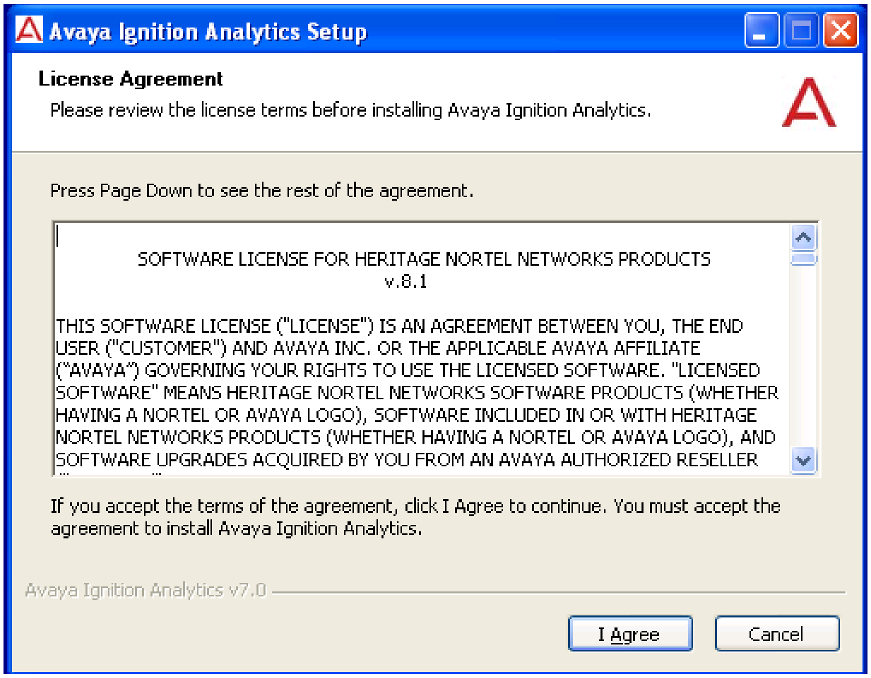


UPGRADING VERSION 7.0.0 TO 8.0.0

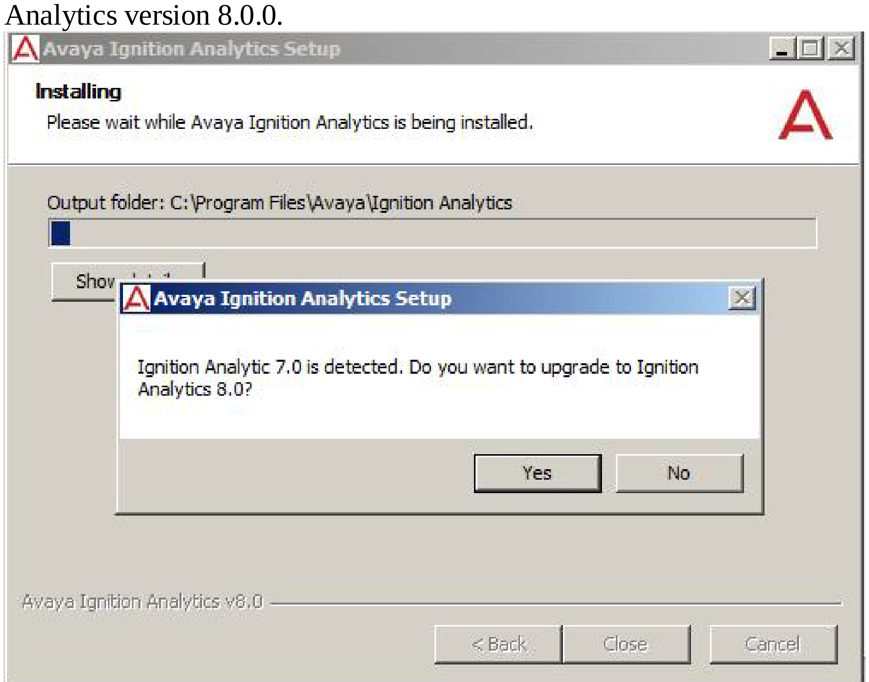
To upgrade from Ignition Analytics version 7.0.0 to Ignition Analytics version 8.0.0, launch the executable file; the installer will guide you through the upgrade.

NOTE: It is advised that you save all other open application files and close these applications prior to beginning this installation.

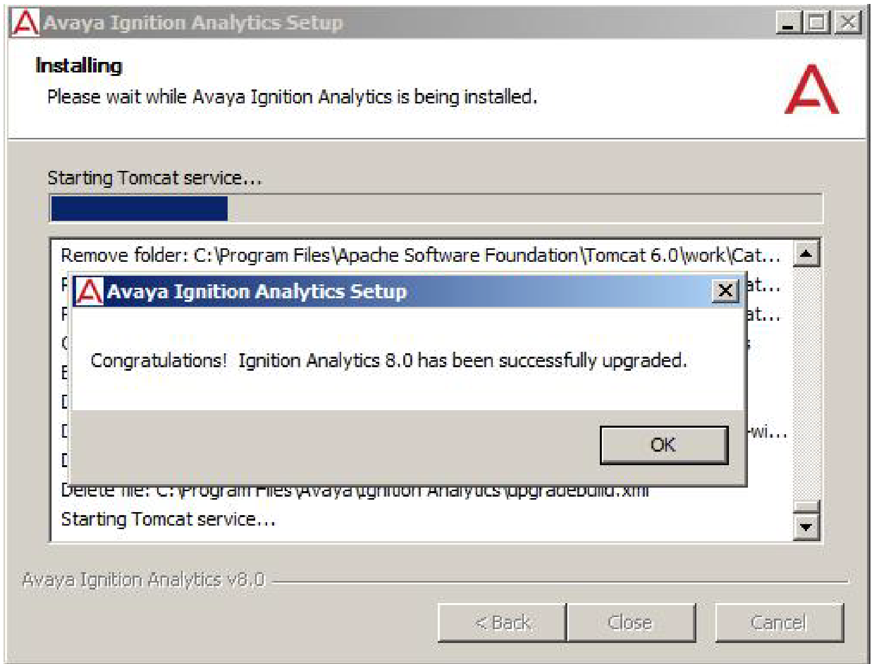
You must accept the license agreement terms to proceed with the installation of the Application. After reading the license agreement, click the “I Agree” button to accept the license agreement to continue with the installation.



The installer will indicate that Ignition Analytic 7.0.0 is detected. Click yes to continue the upgrade to Ignition Analytics version 8.0.0.



Upon completion of the Ignition Analytics upgrade process, following notification will be shown.



MANAGING YOUR IGNITION ANALYTICS APPLICATION

The administrative functions of The Application are accessible through the toolbar. Only users that are a member of the Administrator role will be able to see and access all the following options. Administrator only options are identified below with an ( )

Home	Home returns the user to the main home page.
Administration	Administration includes all application configuration options to setup external connections, define user access and role access.
Repository Management	Repository management contains the access permissions defined for all folder items in the tree.
Custom Report	Users with the assigned privileges to create their own reports will have access this option to create their own User Defined Reports and Analytics.
Scheduler	Scheduler displays a listing of all items available to be scheduled. This includes the scheduling for available reports and for Administrators, the data import process.
Monitor	Monitor captures logs for scheduled activity that is not executed successfully where information is available.

This section will address the application administrator features of the application, including how to configure the application, followed by the features available for application users.

APPLICATION ADMINISTRATION

The application administrator is responsible for:

- **Administration** which includes application configurations.
- **Repository Management** for folder management and establishing who can access folders.
- **Setup Avaya Ignition Server** for export of Access logs via SFTP.
- **Data Import** to process Access logs received from the Avaya Ignition Server.

ADMINISTRATION

Administration includes all application configuration options to setup external connections, define user access and role access.

- **Company Settings** contains all the configurations for the Ignition Analytics application
- **Manage Users** identifies the users that are authorized to access the application
- **Manage Roles** identifies the sets of permissions for functions and objects (i.e. folder access)
- **Manage User Roles** provides a summary view of users and their assigned roles as well as enables mass updates for assignments.

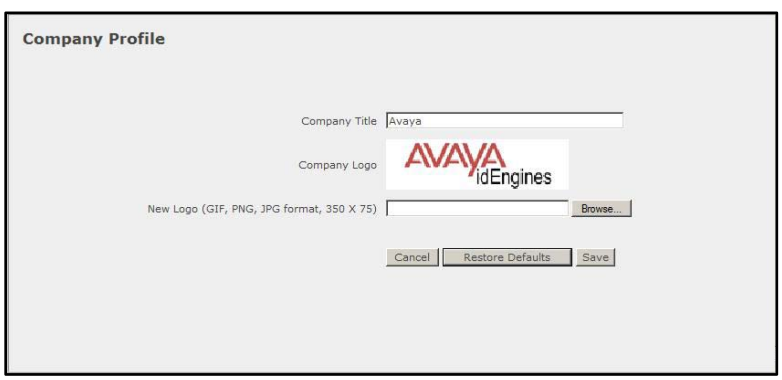
COMPANY SETTINGS

Company Settings contains the configurations for your Ignition Analytics application. There are 4 configurations:

- Company Profile
- SFTP Settings
- Data Import Settings
- Mail Settings

COMPANY PROFILE

Company Profile contains information relating to your organization. To view and maintain your company information, go to the Company Settings option of the Administration toolbar. From the Company Settings main page, select **Company Profile** from the drop-down menu. This includes the company logo to be displayed on reports.
NOTE: The Company Logo image size should be approximately 350x75 pixels or greater



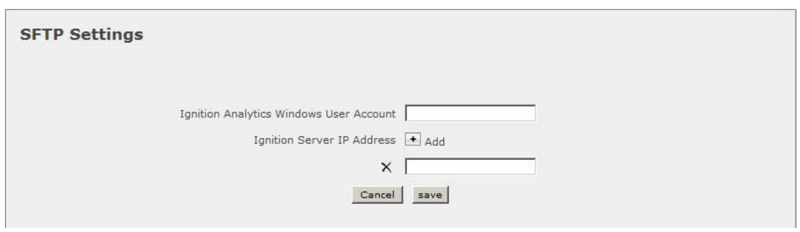
SFTP SETTINGS

SFTP Settings identify the devices for which SFTP connection is enabled for log transfers. For each Ignition Server specified, Ignition Analytics will be open to receive logs being transferred via SFTP from the Ignition Server(s) to Ignition Analytics.

NOTE: Access logs are pushed from Ignition Server and received by Ignition Analytics via the bundled SFTP server installed with Ignition Analytics. Ignition Server should be configured to send Access logs to Ignition Analytics. (See “Setup Identity Engines Ignition Server”)
To configure Ignition Analytics to receive Access logs from Ignition Server, go to the Company Settings option of the Administration toolbar. From the Company Settings main page, select **SFTP Settings** from the drop-down menu.

- **Ignition Analytics Windows User Account** – Enter the user name of the Windows User to whom the SFTP connection should be established. This must be set to a specified Windows User to replace the SYSTEM user reflected at installation.

- **Ignition Server IP Address** – Enter the IP address for each Ignition Server that you would like to enable to connect to this system for log transfers. Click the “+ Add” button to add additional fields to specify additional IP Addresses.



(See “**Error! Reference source not found.**” and “Ignition Analytics receives Access Export Log files (in CSV format) from the Ignition Server via SFTP whereby Ignition Server pushes the Access logs to the SFTP root directory on the Ignition Analytics host.

The Ignition Analytics will only process Export Logs of type Access with filename naming convention: “*_Access_*.csv”. Other Export Logs from the Ignition Server will be skipped and moved into an archive folder and their filename will be modified to start with “_np” representing “not processed”.

The following is a quick overview of the steps required to setup the log export from Avaya Ignition Server. (Refer to the Avaya Identity Engines Ignition Server Administration Guide for more detailed instructions for scheduling Ignition Server log exports)

1. Go to Ignition Dashboard and click Configuration to show the configuration view.

2. Click the name of your site in the tree.

3. Click the Logging tab, and click the Export Logs sub-tab. Click Edit.

4. Setup the export for the Access log channel content at regular time intervals

   a. Go to the Access log channel row and set the Export Periodically dropdown to the desired export interval of Hourly, Daily, or Weekly. It is recommended that this be set to Hourly for very active systems.

5. Set the Start Periodic Export column to the desired time for when the first export is to occur.

6. In the Log Export Host Settings fields, specify the SFTP server that is to receive the log exports.

   a. In the Export to Host field, specify the machine name or IP address of the Identity Engines Ignition Analytics host as the destined SFTP server

   b. Set Login Name as the Windows User Account specified on the SFTP Settings page of Ignition Analytics (See "SFTP Settings")

   c. Set and reconfirm the Password as the windows password for the user identified in the Windows User Account specified on the SFTP Settings page of Ignition Analytics (See "SFTP Settings")

7. Click Save.

DATA IMPORT

" for related configurations)

DATA IMPORT SETTINGS

Data Import Settings identify the location where Access logs are received from Ignition Server. Access logs will be retrieved from the specified Log File Location for data import processing.

To configure Ignition Analytics to retrieve Access logs from the root directory for the Windows User identified in section **Error! Reference source not found.**, go to the Company Settings option of the Administration toolbar. From the Company Settings main page, select **Data Import Settings** from the drop-down menu.

- **Log File Location** – Enter the root directory for COPSSH installation. (NOTE: Ignition Server pushes the log files to the root directory for the specified SFTP host, e.g. c:\Program Files\ICW)

(See "**Error! Reference source not found.**" and "Ignition Analytics receives Access Export Log files (in CSV format) from the Ignition Server via SFTP whereby Ignition Server pushes the Access logs to the SFTP root directory on the Ignition Analytics host.

The Ignition Analytics will only process Export Logs of type Access with filename naming convention: "*_Access_*.csv". Other Export Logs from the Ignition Server will be skipped and moved into an archive folder and their filename will be modified to start with "_np" representing "not processed".

The following is a quick overview of the steps required to setup the log export from Avaya Ignition Server. (Refer to the Avaya Identity Engines Ignition Server Administration Guide for more detailed instructions for scheduling Ignition Server log exports)

8. Go to Ignition Dashboard and click Configuration to show the configuration view.

9. Click the name of your site in the tree.

10. Click the Logging tab, and click the Export Logs sub-tab. Click Edit.

11. Setup the export for the Access log channel content at regular time intervals

    a. Go to the Access log channel row and set the Export Periodically dropdown to the desired export interval of Hourly, Daily, or Weekly. It is recommended that this be set to Hourly for very active systems.

12. Set the Start Periodic Export column to the desired time for when the first export is to occur.

13. In the Log Export Host Settings fields, specify the SFTP server that is to receive the log exports.

    a. In the Export to Host field, specify the machine name or IP address of the Identity Engines Ignition Analytics host as the destined SFTP server

    b. Set Login Name as the Windows User Account specified on the SFTP Settings page of Ignition Analytics (See "SFTP Settings")

    c. Set and reconfirm the Password as the windows password for the user identified in the Windows User Account specified on the SFTP Settings page of Ignition Analytics (See "SFTP Settings")

14. Click Save.

DATA IMPORT

” for related configurations)

MAIL SETTINGS

Mail Settings enable Ignition Analytics to connect to a specified corporate mail server for email distribution of reports.
To configure Ignition Analytics to connect to a corporate mail server, go to the Company Settings option of the Administration toolbar. From the Company Settings main page, select **Mail Settings** from the drop-down menu.

Field Name (* required field)	**Description**
* Host	Hostname of the mail server
Protocol	SMTP is required
* Port	The port is defaulted to 25. If the port for your mail server is not port 25, update this field.
* From Email	The email address which will display in the email “From” line
* Mail Server Authentication	*Select the application option:* No – No authentication req’d on the mail server Yes – Authentication req’d on the mail server
If “Yes” is selected then: Username Password	 Enter the username for the mail server Enter the password for the mail server

MANAGE USERS

Users identify who can access the Ignition Analytics application. The roles to which a user is assigned determine what functions they can perform and what they can access. Users can be assigned to more than one (1) role.

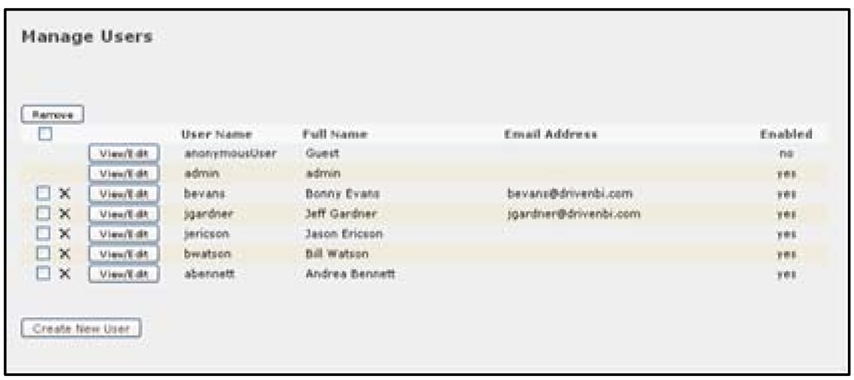
To view and manage users, go to the Administration toolbar and select **Manage Users** from the drop-down menu to view and maintain users.

NOTE: Ignition Analytics has a pre-defined user (admin) that cannot be removed. This user is the default Administrator for The Application. It is recommended that the password for this user is changed. Be sure to note this password for future reference.

Create New User To create a new user, select the Create New User button from the Manage Users display page. This will take you to the User display page to continue the new user setup.

View/Edit To view or update an existing user, select the View/Edit button next to the user record on the Manage Users display page. This will take you to the User display page to continue updating the existing user setup.

Remove To remove user(s), select the checkbox(es) next to the user name(s) and click the Remove button. Generally, if a user should no longer have access to the application, the "Enabled" checkbox should be deselected. Only users that do not have any content in their personal folder can be removed.



The following are the fields and definitions that are populated when you perform a **Create New User** action or a **View/Edit** action on an existing user:

Field Name (* required field)	**Description**
* User Name	User Name to identify the user at login
* Full Name	The user's Full Name
* Password	Password to be used for login verification of the user
* Confirm Password	Reconfirm the password entered in the password field
E-mail Address	User's e-mail address
Enabled	Select this checkbox to activate this user account
Roles	Select the applicable roles for this user

MANAGE ROLES

Roles are the access groups established to regulate application functions and folders, defining what users can see or do. Users can be assigned to more than 1 role. The permissions assigned to Folders and objects in Repository Management determine what can be accessed by each role.

To view and manage roles, go to the Administration toolbar and select **Manage Roles** from the drop-down menu to view and maintain roles.

NOTE: Ignition Analytics has several pre-defined roles that cannot be removed:

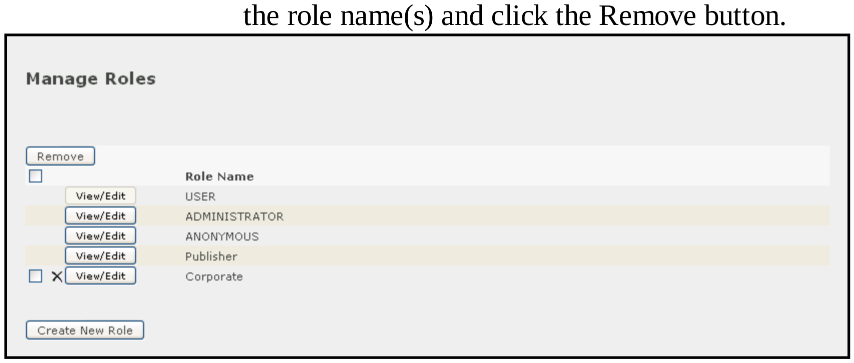
> **USER** role is required to log in. All users must be assigned to this role in order to log in to the Ignition Analytics application. This role is pre-assigned when creating a new user and cannot be removed.
>
> **ADMINISTRATOR** role gives users full access to the application to perform all administrator functions as encompassed in this product guide. For example, an administrator may create new Users, create new roles, configure application connections, schedule data imports.
>
> **ANONYMOUS** role is an available role that can be customized for guest access. This role does not have permissions to access any folders initially and can be edited by the Administrator to establish guest permissions as desired.
>
> **Publisher** role regulates access to creating Custom Reports. Users assigned to this role will be able to create their own Custom Reports.

There are two steps to Manage Roles:

STEP (1) Create/Maintain Roles

Maintain the role itself through the Role display page.

Create New Role	To create a new role, select the Create New Role button from the Manage Roles display page. This will take you to the Role display page to complete Step 1. Upon completion of Step 1, you will be returned to the Manage Roles display page. Once the new role is created, you will need to assign folder permissions through the Repository Management option of the toolbar to complete Step 2.
View/Edit Role:	To view or update who has been assigned to the existing Role, select the View/Edit button next to the role on the Manage Roles display page. This will take you to the Role display page.
Remove	To remove role(s), select the checkbox(es) next to the role name(s) and click the Remove button.



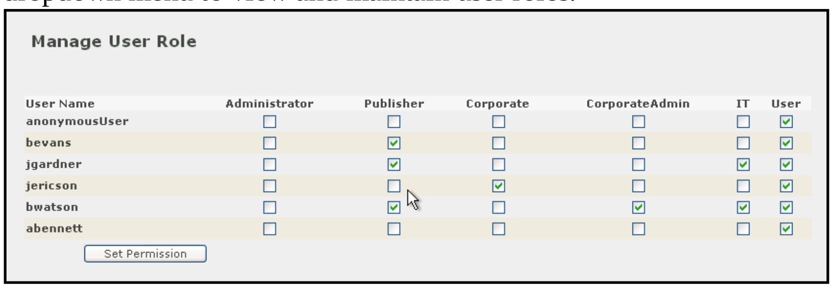
The following are the fields and definitions to **Create New Role** or **View/Edit** an existing role:

Field Name (* required field)	**Description**
* Role Name	Name of the role created
Users with this Role	Select the applicable user(s) who have access as defined for the role

STEP (2) Assign folder permission to the Role
Maintain folder permissions assigned to the role through the Repository Management option of the toolbar (See "**Error! Reference source not found.**")

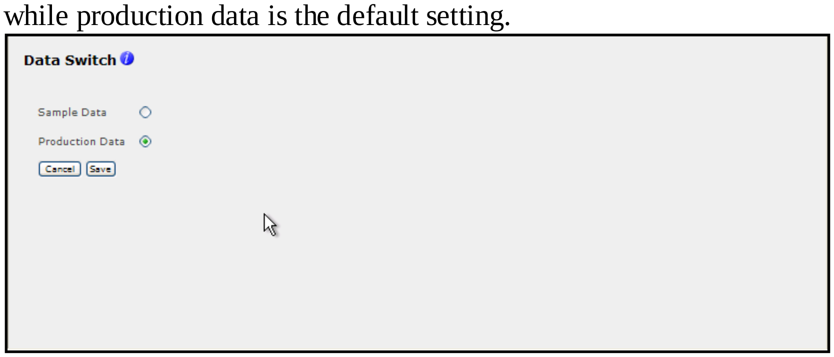
MANAGE USER ROLES

Manage User Roles provides a means to update the roles assigned to users. From the Roles & Permissions toolbar, select **Manage User Roles** from the dropdown menu to view and maintain user roles.



DATA SWITCH

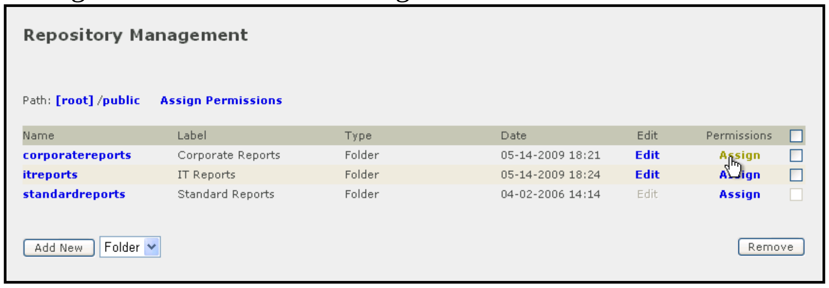
Data switch provides a means to switch between sample data and production data. Sample data has been pre-populated for standard reports as examples, while production data is the default setting.



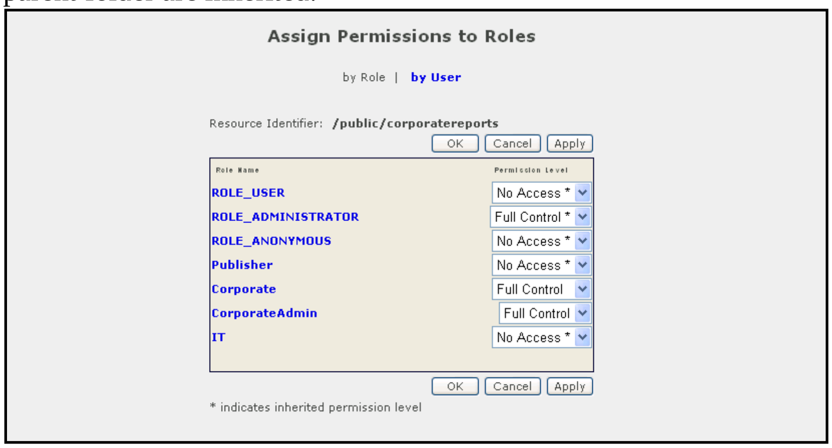
REPOSITORY MANAGEMENT

Repository management establishes what folders are accessible based on permission levels established for each role. New shared folders can be created and permissions assigned for applicable roles.

To assign a permission level for a folder, navigate to the desired folder from Repository Management and select the "Assign" link for the desired folder.



For each role, specify the desired permission level. By default, the permissions from the parent folder are inherited.



The following describes the permissions that can be assigned to folders for each role:

No Access Roles with No Access as the permission level specified for the folder will not have access to the folder and its contents. The folder will not display in the navigation tree

Full Control Roles with Full Control as the permission level specified for the folder will be able to execute all available actions for items within the folder (refer to Note 2 below)

View Roles with View as the permission level specified for the folder will be able to view the folder and its contents as well as execute available actions for applicable items within the folder (refer to Note 1 below)

Delete Do Not Select this permission level - This option is not applicable for The Application at this time

Publish Do Not Select this permission level - This option is used by the Publisher role for The Application

NOTE 1: Role permissions for Standard Reports - For roles that should have access to Standard Reports or subfolders within standard reports, specify "View" as the permission level to enable access to schedule Standard Reports. DO NOT set permission levels for Standard Reports to "Full Control" as this will enable standard reports to be deleted from the system.

NOTE 2: For new folders that are created, specify "Full Control" as the permission level to enable users to view shared report output and shared custom reports. Only the originator of the report output or custom report can delete these; “Full Control” enables users to view and share report output and custom reports for specified folders.

SETUP IDENTITY ENGINES IGNITION SERVER

Ignition Analytics receives Access Export Log files (in CSV format) from the Ignition Server via SFTP whereby Ignition Server pushes the Access logs to the SFTP root directory on the Ignition Analytics host.

The Ignition Analytics will only process Export Logs of type Access with filename naming convention: “*_Access_*.csv”. Other Export Logs from the Ignition Server will be skipped and moved into an archive folder and their filename will be modified to start with “_np” representing “not processed”.

The following is a quick overview of the steps required to setup the log export from Avaya Ignition Server. (Refer to the Avaya Identity Engines Ignition Server Administration Guide for more detailed instructions for scheduling Ignition Server log exports)

15. Go to Ignition Dashboard and click Configuration to show the configuration view.

16. Click the name of your site in the tree.

17. Click the Logging tab, and click the Export Logs sub-tab. Click Edit.

18. Setup the export for the Access log channel content at regular time intervals

    a. Go to the Access log channel row and set the Export Periodically dropdown to the desired export interval of Hourly, Daily, or Weekly. It is recommended that this be set to Hourly for very active systems.

19. Set the Start Periodic Export column to the desired time for when the first export is to occur.

20. In the Log Export Host Settings fields, specify the SFTP server that is to receive the log exports.

    a. In the Export to Host field, specify the machine name or IP address of the Identity Engines Ignition Analytics host as the destined SFTP server

    b. Set Login Name as the Windows User Account specified on the SFTP Settings page of Ignition Analytics (See “SFTP Settings”)

    c. Set and reconfirm the Password as the windows password for the user identified in the Windows User Account specified on the SFTP Settings page of Ignition Analytics (See “SFTP Settings”)

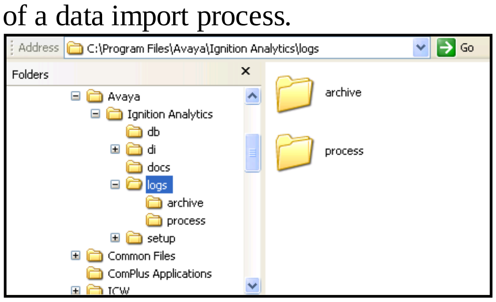
21. Click Save.

DATA IMPORT

Ignition Analytics periodically processes Access log data received via SFTP from the Ignition Server. When Ignition Analytics generates a report, it uses the accumulated data from all Access logs processed through the data import process and stored in the data warehouse. As administrator, you use the Data Import section of the application to specify when and how frequently Ignition Analytics will process the Access log data received from the Ignition Server. (See "**Error! Reference source not found.**" and "**Error! Reference source not found.**" for data import related configurations)
Data imports should be scheduled at recurring intervals. On an as needed basis, this can also be initiated ad hoc. There is a monitoring facility that lets you review the status for processed logs. The retrieval of Ignition Server logs occurs at intervals independent of the report generation schedules.
You should set the data import to occur as frequently as needed, based on the volume of Ignition Server traffic. It is recommended that you set the Data Import schedule to execute at off peak hours once a day so that data processing does not impact performance for The Application for reporting.
NOTE: Do not confuse *data import schedules* with *report generation schedules*. (See "**Error! Reference source not found.**").

ABOUT THE DATA IMPORT PROCESS

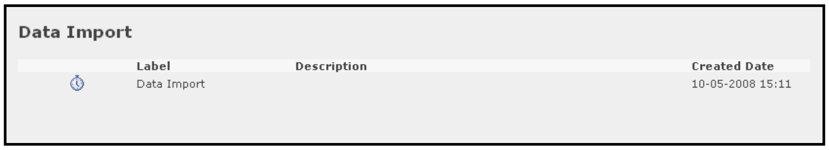
The data import process refers to the log file location as configured in Data Import Settings (See "**Error! Reference source not found.**"), retrieves all files named with the pattern "*_Access_*.csv" from this location and extract data from these files to populate the Ignition Analytics data warehouse.
There is a \logs subdirectory in the installed location folders for the application where the *_Access_*.csv files are stored during and subsequent to completion of a data import process.



- The directory *\logs\process* contains all *_Access_*.csv log files that are currently being processed via a scheduled data import job. The application manages the files in this directory; please do not add/remove/modify files in this directory.
- Once the log files have been processed, they are archived in the directory *\logs\archive.*

MANAGE DATA IMPORT SCHEDULE

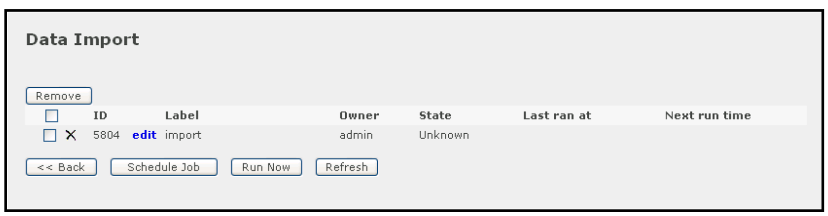
To schedule the intervals for which the Ignition Server logs should be processed, go to the Scheduler toolbar and select **Schedule Data Import** from the dropdown menu to view and maintain data import jobs. Each listed job is scheduled and maintained individually.
Data Import Processes the Ignition Server's Access logs for reporting



THE DATA IMPORT SCHEDULER

The Schedule display page for Data Import lists the schedules that have been created for the data import job(s). To view and maintain the scheduled runtime for a data import job, select the Schedule Data Import icon to go to the Schedule display page. The status and runtime information is also displayed, reflecting when the scheduled job was last executed and when the next scheduled runtime for the job will occur.

- **Refresh Schedule display page:** To refresh the runtime information on the Schedule display page, click the Refresh button.
- **Execute a Data Import Job immediately:** To execute a Data Import job immediately, click the Run Now button on the Schedule display page.
- **Create a New Schedule:** To create a new schedule for a Data Import job, click the Schedule Job button on the Schedule display page and complete all Scheduler Steps.
- **View/Update an Existing Schedule:** To view or update an existing schedule for a Data Import job, click the Edit button next to the schedule record and update Scheduler Steps as needed (section Setup Data Import Schedule)
- **Remove Schedule(s):** To remove schedule(s), select the checkbox(es) next to the data import schedule(s) and click the Remove button.



SETUP DATA IMPORT SCHEDULE

Scheduler Steps: There are two steps to schedule a data import job:

- Create the *job*.
- Set the *schedule*.

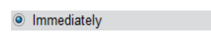
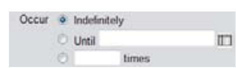
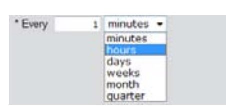
STEP 1 – Job describes the schedule record for the Data Import job.

Field Name (* required field)	Description
Report	System generated identifier for the scheduled job. This field cannot be changed.
* Label	Name of the schedule record.
Description	Details pertaining to schedule record.

STEP 2 – Schedule defines when and how often the Data Import job will be executed. There are three levels of scheduling recurrence available to accommodate varying scheduling complexities: No Recurrence, Simple Recurrence, Calendar Recurrence.

> **No Recurrence:** Schedule will be executed one time only, at the specified Start date.
>
> **Simple Recurrence:** Schedule will be executed at standard recurring intervals.
>
> **Calendar Recurrence:** Schedule will be executed at non-standard recurring intervals where a more complex schedule is required.

The following are the fields and definitions for **Scheduler Step 2 - Schedule:**

Field Name (* required field)		**Description**
*	Start	The schedule's effective start date.  The effective start date for the schedule will be immediately upon completion of this schedule setup.  The effective start date for the schedule will be on the specified date.
*	Recurrence No Recurrence Simple Recurrence	The frequency level at which the schedule will be executed. Schedule will be executed one time only, at the specified Start date. Schedule will be executed at standard recurring frequencies and intervals:  Frequency (Occur) - *Indefinitely*: Schedule will be executed at the specified intervals until this scheduled job is removed. - *Until*: Schedule will be executed at the specified intervals through the indicated date. - *Times*: Schedule will be executed at the specified intervals for the indicated number of occurrences.  Interval (Every)

		- The interval at which this schedule will be executed.
	Calendar Recurrence	Schedule will be executed at non-standard recurring frequencies and intervals where a more complex schedule is required: Frequency - *End Date*: Schedule will be executed at the specified intervals through the indicated end date. If no end date is indicated, the schedule will be executed at the specified intervals until this scheduled job is removed.  Interval - *Minute(s)*: Specify the minute intervals as needed. - *Hour(s)*: Specify the hour intervals as needed. - Days: Specify the days that this schedule will be executed. - *Months*: Specify the months that this schedule will be executed

MONITOR DATA IMPORT EVENTS

Data Import logs are available for monitoring of executed data import jobs. From the Monitor toolbar, select **Monitor Data Import** from the dropdown menu to go to the Monitor Events display page.
The Monitor Events display page lists the logs available for review. The status and runtime information is also displayed, reflecting when each data import job began and ended.
View log details: To review a data import log, click on the Job Name.
View only unread or all logs: To view only unread logs or to view all log records, select the appropriate option from the Show Messages dropdown.
Remove Logs: To remove logs, select the checkbox(es) next to the data import logs and click the Remove button.

APPLICATION USERS

Application users are able to create custom reports and manage reports based on roles to which they have been assigned.

Custom Reports

Users assigned to the Publisher role will be able to create custom reports. Custom Reports enable users to create their own data report or graphical analytic based on available data elements for each report type. There are 2 types of available custom reports,
User Defined Report – Create your own network activity report by selecting the data elements against which you would like to report and specifying report summary options

Analytics – Create graphical displays for trends and establish thresholds to identify network activity exceptions.

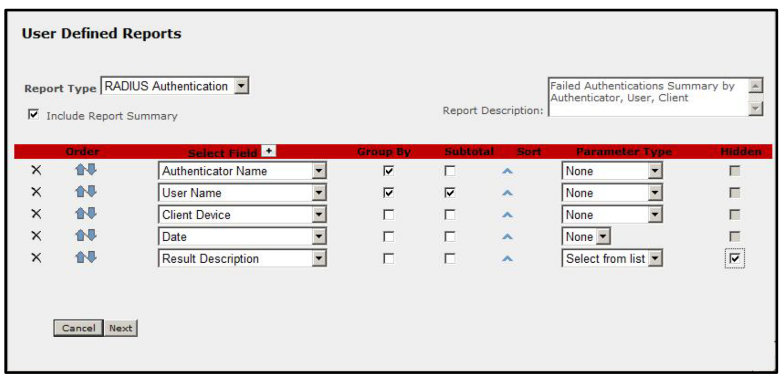
To create custom reports, go to the Custom Reports toolbar and select User Defined Report or Analytics.

User Defined Report

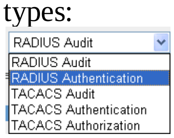
From the Custom Report toolbar, select Custom Reports User Defined from the dropdown menu to begin creating a User Defined Report.

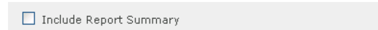
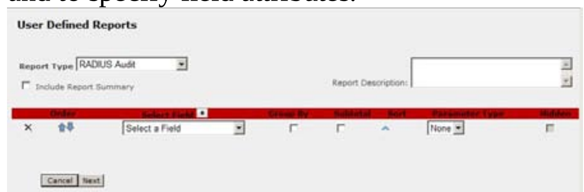
Select Report Data Elements

Specify desired report fields to include in your report. The order in which the fields are displayed determines the order in which data fields will display on the report. (Only fields where the Hidden checkbox is not checked will be included in the data fields displayed on the report; refer to Hidden field for further information.)



The following are the available selections and definitions for creating **User Defined Reports:**

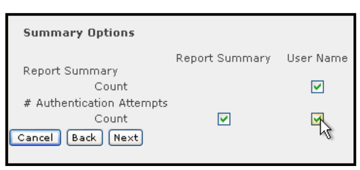
Field Name (* required field)		Description
*	Report Type	The type of data to report against. The available data elements for the user defined report are based on the selected report type. There are 5 available types: 

Report Description	Add a brief description for the report being created. 
Report Summary	To include report level totals for report calculations, select this checkbox. 
Field Attributes	To add report elements, select to add a new field and to specify field attributes. 
Delete	Deletes the selected field and associated field attributes
Order	Move the selected field up or down. The order in which the fields are reflected here determines the order in which data fields will display on the report. (Only fields where the Hidden checkbox is not checked will be included in the data fields displayed on the report; refer to Hidden field for further information.)
Select Field	Select a field to include from the available list of fields. The selection made in the Report Type dropdown field will determine the available data elements for the user defined report; not all data elements are available for all Report Types. 
Group By	Select this checkbox in order to group your report content by this field. 
Subtotal	Select this checkbox in order to specify summary calculations for your report data. Available summary options vary by report type. This checkbox can only be selected for fields where grouping has been specified (the Group By checkbox has been selected). Further summary options can be specified for this field on the Summary Options page. 
Sort	Sort specifies the sort order for content in this field. ^ = ascending order v = descending order 

	Parameter Type	Parameter Type enables you to narrow your report results to include only information based on specific criteria. There are 4 possible Parameter Types available in the dropdown list; only applicable parameter types will be listed for each field – not all Parameter Types are available for all fields. - *Select from list*: The parameters page will display a list of values for this field. Narrow report results based on values selected from a list of values. - *Range*: The parameters page will display from/to fields for you to specify a range for this field. - *Top N/Bottom N*: Indicate a number to identify the top or bottom limits for report results. Desired parameter criteria can be specified for this field on the Parameters page. 
	Hidden	Select this checkbox if you do not wish the selected field to be included in the report data. This checkbox will apply primarily where a field is specified with the intent of selecting a parameter to narrow report results (i.e. failed authentications) 

SUMMARY OPTIONS

Specify desired report summary options from the Summary Options page. The available summary options differ based on the Report Type selected. This page will only display if the Include Report Summary checkbox is checked or the Subtotal checkbox is checked for any fields.

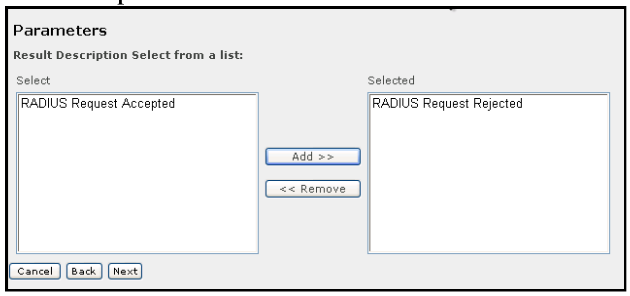


- *Report Summary*: summarizes results at the topmost level across all report results.
- *[Selected Fields]*: summarizes results by the identified grouping level (i.e. in the below, results will be subtotaled by User name)

PARAMETERS

Narrow your report results to include only information based on criteria specified from the Parameters page. This page will only display if a parameter type is selected for any field.

- *Select from list*: Selected from the list of values for this field to narrow report results for the field.

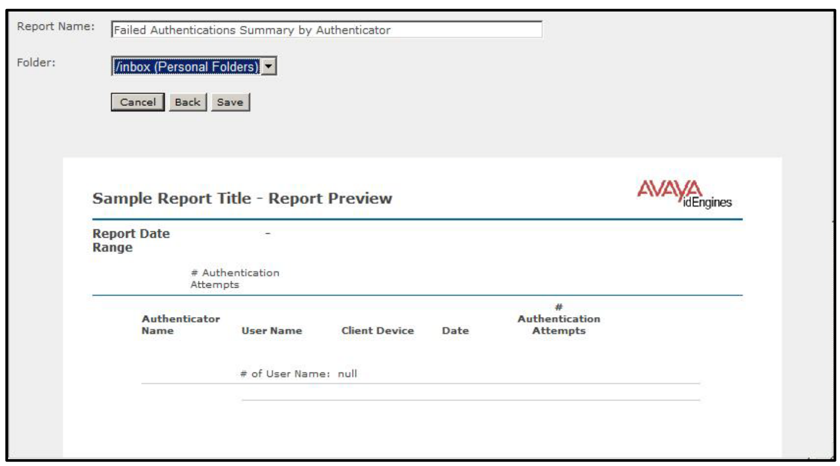


- *Range*: Specify from/to range for this field to narrow report results for the field.

- *Top N/Bottom N*: Specify the top/bottom limits to narrow report results for the field.

REPORT PREVIEW

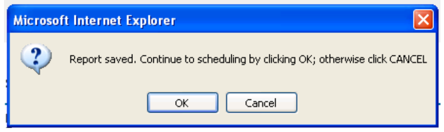
A report preview page allows you to preview the report definition created based on the selections made for your report. The report preview includes the column headers for the fields selected, displays group level borders for specified grouping levels, and identifies the selected summary options for the report.



- *Report Name*: Name the report using alphanumeric characters (only alphanumeric characters can be used)
- *Folder*: Select from the available list of folders in which to store your user defined report. The list of available folders will include only those folders to which you can write to as identified by the role(s) for which you are assigned.

Schedule User Defined Report

Once you have saved your user defined report, you will be prompted as to whether you would like schedule your report. Click OK to proceed to schedule report generation (See “Schedule Report Generation”), or Cancel if you do not wish to schedule your report.

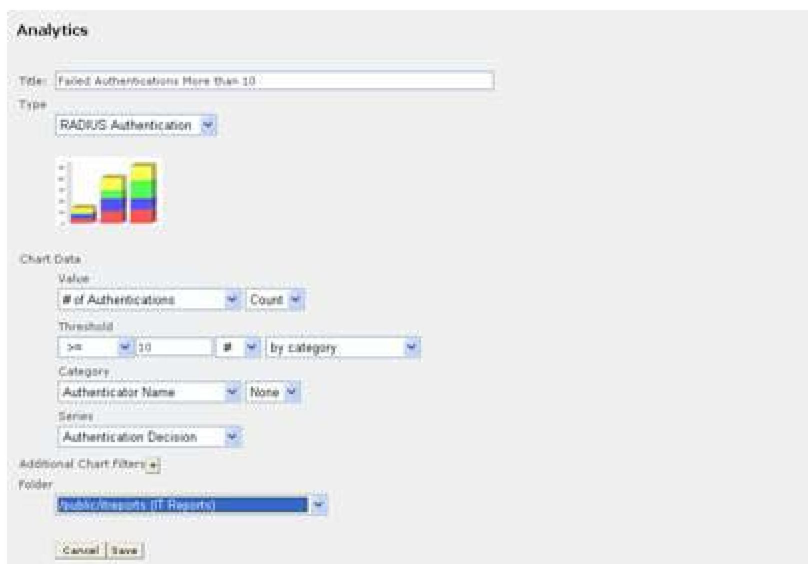


Analytics

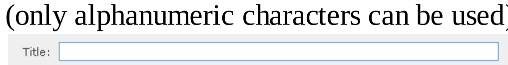
From the Custom Report toolbar, select Custom Reports Analytics from the dropdown menu to begin creating an Analytic.

Select Analytic Criteria

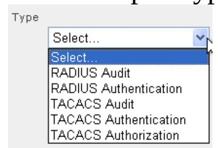
Specify desired analytic criteria to create a graphical summary. The page display for available analytic options will update as criteria is selected.



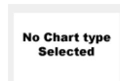
The following are the available selections and definitions for creating an **Analytic:**

Field Name (* required field)		**Description**
*	Title	Name the analytic using alphanumeric characters (only alphanumeric characters can be used) 

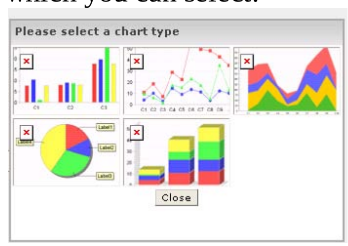
<table>
<tr>
<td>Type</td>
<td>The type of data to report against. The available data elements for the analytic are based on the selected report type. There are 5 available types:



</td>
</tr>
<tr>
<td>Chart Type</td>
<td>Select a chart type for the analytic by clicking on the



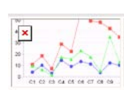
This will display all the available chart types from which you can select:



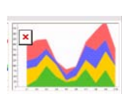
The following is a brief description of each chart type as it relates the Value, Category and Series fields:

- *Bar*: The bar chart will graph the results for the specified Value using vertical bars. The selection specified in Category determines each x-axis grouping while the selection specified in the Series determines subgroups within the Category, represented by each individual color bar.

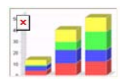
- *Line*: The line chart will graph the results for the specified Value using lines. The selection specified in Category determines each x-axis grouping while the selection specified in the Series determines each colored trend line.

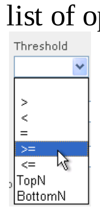


- *Area:* The area chart will graph the results for the specified Value using area blocks. The selection specified in Category determines each x-axis grouping while the selection specified in the Series determines each colored area.


</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>
- Pie: The pie chart will graph the results for the specified Value using pie slices. The selection specified in Category determines each pie slice.

- Stacked Bar: The stacked bar chart will graph the results for the specified Value using vertical bars. The selection specified in Category determines each x-axis grouping represented by each full vertical bar while the selection specified in the Series determines subgroups within the Category, represented by each subsection within a vertical bar.

</td>
</tr>
<tr>
<td></td>
<td>Chart Data</td>
<td>
Chart data specifies the threshold criteria for the analytic results displayed and applicable Value, Category and Series for the chart.
- Value: Select the field and calculation type for the chart values. Available calculation types are based on the selected field.

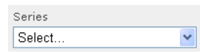

- Threshold: The threshold identifies the criteria used to determine what results to include in the analytic. This is used to enable exception based reporting or a subset of results.
Select a threshold criteria from the available list of options:


Specify the limits for the threshold by indicating the limit value, selecting whether the value refers to a # or % from the dropdown, and whether the limit applies to the category only or the category+series from the dropdown.


- Category: The category identifies each x-axis grouping. Select a data element from the dropdown. You can further limit your results by selecting parameter criteria from the dropdown where applicable.
</td>
</tr>
</table>

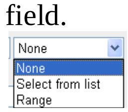
<table>
<tr><td></td><td></td><td>

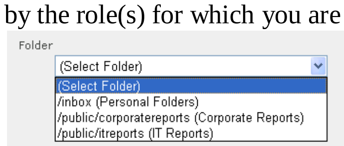
- *Series*: The series identifies a subgroup within each category and applies only to applicable chart types. By default, the series will be the same as the selected data element for category. Select a different data element from the dropdown to apply a subgroup to the category.


</td></tr>
<tr><td></td><td>Additional Chart Filters</td><td>Additional Chart Filters enable you to narrow your analytic results to include only information based additional criteria. To add a chart filter, select .

Select a data element to which the filter will be applied and then select the applicable filter type from the dropdown. There are 2 possible chart filters available in the dropdown list; only applicable chart filters will be listed for each field – not all chart filters are available for all fields.

- *Select from list*: The parameters page will display a list of values for this field. Narrow analytic results based on values selected from a list of values.
- *Range*: The parameters page will display from/to fields for you to specify a range for this field.

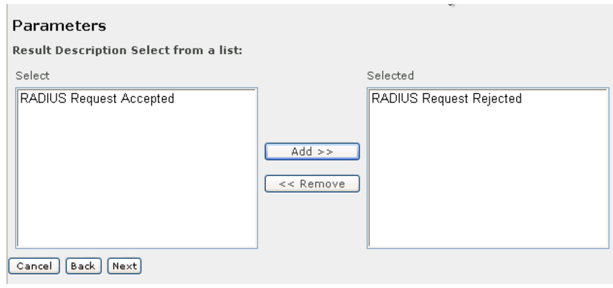

</td></tr>
<tr><td></td><td>Folder</td><td>Select from the available list of folders in which to store your analytic. The list of available folders will include only those folders to which you can write to as identified by the role(s) for which you are assigned.


</td></tr>
</table>

PARAMETERS

Narrow your analytic results to include only information based on criteria specified from the Parameters page. This page will only display if a parameter type is selected for category or additional chart filters.

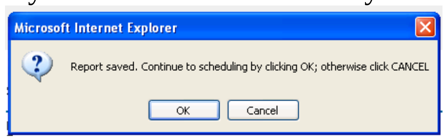
- *Select from list*: Selected from the list of values for this field to narrow results for the field.



- *Range*: Specify from/to range for this field to narrow results for the field.

SCHEDULE ANALYTIC

Once you have saved your analytic, you will be prompted as to whether you would like schedule your analytic. Click OK to proceed to schedule report generation (See "Section Schedule Report Generation"), or Cancel if you do not wish to schedule your analytic.



Reports Management

Application reports are managed through the folders available in the navigation tree. The navigation tree contains a Personal Folder and Public Folders upon installation. Additional folders can be added by the Application's administrator to share generated reports and custom reports with other users.

Report management functions apply to all standard and custom reports and include scheduling the automatic generation of reports at specified recurring intervals, creating custom reports, and sharing reports content.

NOTE: Do not confuse the *report generation schedule* with the *data import schedule*. For details on scheduling data imports, see 0.

Manage the Report Generation Schedule

From the Navigation Tree, navigate to the folder containing the report you would like to schedule. Each report is scheduled and maintained individually.

Schedule Report - Select the Schedule Report icon to go to the Schedule display page and view and maintain scheduled runtime(s) for the report. This is the recommended method to run your report.

View Report – Select the Run Report icon to execute the report immediately. This option should only be used when a report is needed on the occasional on demand basis. It is recommended that Schedule Report be used to run your report.

Run in Background – Select the Run in Background icon to execute the report immediately and store the specified report formats in the report output Navigation Panel for viewing.

Schedule Report Generation

The Schedule display page for your selected report lists the schedules that have been created for the report. The runtime information is also displayed, reflecting when the report schedule was last executed and when the next scheduled runtime for the report will occur.

Refresh Schedule display page: To refresh the runtime information on the Schedule display page, click the Refresh button.

Execute Report immediately: To execute the report immediately, click the Run Now button on the Schedule display page.

Create a New Schedule: To create a new schedule for the report, click the Schedule Job button on the Schedule display page and complete all Scheduler Steps (See "Set up a Report Generation Schedule").

View/Update an Existing Schedule: To view or update an existing schedule for the report, click the Edit button next to the schedule record and update Scheduler Steps as needed.

Remove Schedule(s): To remove schedule(s), select the checkbox(es) next to the report schedule(s) and click the Remove button.

Set up a Report Generation Schedule

Scheduler Steps: There are four steps to schedule report generation: (1) Job. (2) Schedule, (3) Parameter, and (4) Output.

Step 1 – Job describes the schedule record for the report schedule.

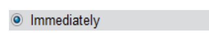
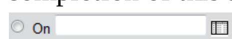
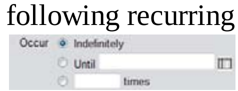
Field Name (* required field)	Description
Report	This is a system generated identifier for the scheduled job. This field cannot be changed.
* Label	Name of the schedule record.
Description	Details pertaining to schedule record.

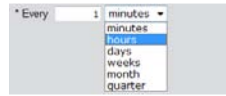
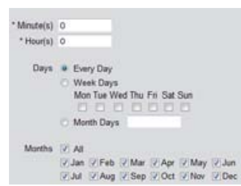
Step 2 – Schedule defines when and how often the report will be executed. There are three levels of scheduling recurrence available to accommodate varying scheduling complexities: No Recurrence, Simple Recurrence, Calendar Recurrence.

No Recurrence: Schedule will be executed one time only, at the specified Start date.

Simple Recurrence: Schedule will be executed at standard recurring intervals.

Calendar Recurrence: Schedule will be executed at non-standard recurring intervals where a more complex schedule is required.

Field Name (* required field)		Description
*	Start	The schedule's effective start date.  The effective start date for the schedule will be immediately upon completion of this schedule setup.  The effective start date for the schedule will be on the specified date.
*	Recurrence No Recurrence Simple Recurrence	The frequency level at which the schedule will be executed. Schedule will be executed one time only, at the specified Start date. Schedule will be executed at standard recurring intervals. Indicate one of the following recurring intervals:  Frequency (Occur) - *Indefinitely*: Schedule will be executed at the specified intervals until this scheduled job is removed. - *Until*: Schedule will be executed at the specified intervals through the specified date. - *Times*: Schedule will be executed at the specified intervals for the

		specified number of occurrences.  Interval (Every) - The interval at which this schedule will be executed.
	Calendar Recurrence	Schedule will be executed at non-standard recurring intervals where a more complex schedule is required. Indicate one of the following recurring intervals: Recurring Period - *End Date*: Schedule will be executed at the specified intervals through the specified end date. If no end date is indicated, the schedule will be executed at the specified intervals until this scheduled job is removed.  Interval - *Minute(s)*: Specify the minute intervals as needed. - *Hour(s)*: Specify the hour intervals as needed. - Days: Specify the days that this schedule will be executed. - *Months*: Specify the months that this schedule will be executed

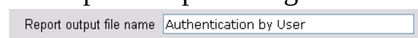
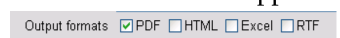
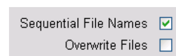
Step 3 – Parameters are specified variables for the report. All reports will include report date range parameters used to specify the data to include in the report. Some reports will include report specific parameters.

Report Date Range Parameters:

If the report is scheduled to run once only, specify the Period Start Date and Period End Date for the report.

If the report is scheduled to run more than once using either the simple recurrence or calendar recurrence, select the radio button by the most appropriate Date Calculation option (i.e. last week, week to date, etc). The report date range will be systematically determined based on the selected date increment.

Step 4 – Output defines the format(s) for the report as well as includes report storage options and e-mail distribution options.

Field Name (* required field)	**Description**
Report Format	
* Report Output Filename	The name of the report to be stored in the Report Output Navigation Panel. 
* Output Formats	Select the format(s) in which the report should be generated. Select as many different formats as applicable. 
Report Storage options	
* Sequential File Names OR Overwrite Files	Select the preferred report storage option.  - *Sequential File Names* stores each executed report separately, retaining the previous versions (if any) that are generated by the schedule. - *Overwrite Files* replaces the previous version of the report (if any) generated by the schedule.
Folder	The folder dropdown lists both your personal folder and shared folders where the report output can be stored. The Shared Report folder(s) are accessible by all users assigned to roles that have access to the shared folder. 
Send to Others	By default, the report output for this schedule will be available in the logged in user's Personal Reports folder. Modify or add additional users to whom the report output for this schedule will be sent by selecting from the available users. The report output for the scheduled report will be available to the selected users in their individual Personal Reports folder.

	
E-mail distribution options	
To	Email addresses for individuals selected in the Send to Others field will automatically be populated here.
Subject	Subject line for the e-mail.
Message Text	E-mail text.
Attach Files	Select the checkbox to include the actual report as an attachment to the e-mail. If you do not select the checkbox, then the e-mail is simply a notification that the report has been generated, and that the recipient may visit the Ignition Analytics application to view the report.

MONITOR REPORT GENERATION EVENTS

Report logs are available for monitoring of executed reports. From the Monitor toolbar, select Monitor Reports from the dropdown menu to go the Monitor Events display page.

The Monitor Events display page lists the logs available for review. The status and runtime information is also displayed, reflecting when the report scheduled was executed.

View log details: To review a report log, click on the Message record.

View only unread or all log records: To view only unread report logs or to view all report logs, select the appropriate option from the Show Messages dropdown below the Monitor Events display page title.

Remove Log Record(s): To remove log record(s), select the checkbox(es) next to the report log record(s) and click the Remove button.

APPENDIX A

Terminology

The following terms are used throughout this guide. Use their definitions to aid your understanding and use of The Application.

Terminology	Definition
Toolbar	User options across the top of the display page, directly below the header
Navigation Tree	User options at the left of the display page.
User Name	Individuals provided with a User name for authorized access to Ignition Analytics.
Role	Roles identify who can use the Ignition Analytics and what the user can access.
Permission	Permissions define what functions are enabled and to which reports the function(s) apply.

Symbols and Typefaces

The following visual cues are used to convey functions within Ignition Analytics.

Image	Function	Image	Function
Toolbar		**Display Pages**	
	Home		HTML Format
	Administration		PDF Format
	Custom Reports		RTF Format
	Scheduler		XLS Format
	Monitor		Schedule Report
	Manage Users		Edit Report
	Manage Roles		Run Report
	Manage User Roles		View Report
	Company Settings		Run in Background
	Data Switch		Remove
	Custom Reports Analytics		
	Custom Reports User Defined		

	Schedule Data Import
	Schedule Reports
	Monitor Data Imports
	Monitor Reports
	Repository Management

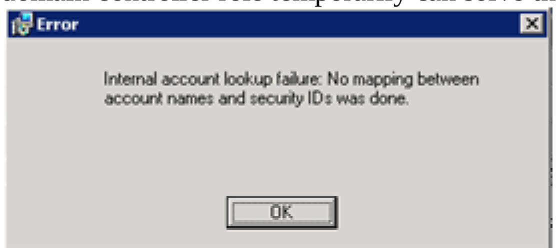
APPENDIX B

TROUBLESHOOTING TIPS

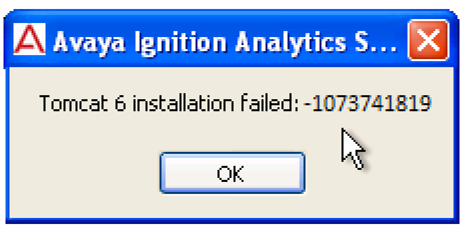
DURING APPLICATION INSTALLATION

The application installation was not successful – Error "Internal account lookup failure"
Verify that you are logged into the Windows system as a user with full administrative rights on the system as the installation process includes the addition of files, will write applicable registry entries, and create a new service account.

Verify if the machine is a domain controller (user active directory). Suppressing the domain controller role temporarily can solve the issue.



Installation failed: -1073741819
Verify if the machine is installed with Symantec Endpoint Protection. Suppressing the service temporarily can resolve the issue. Please uninstall application from control panel, and re-install application to further proceed.

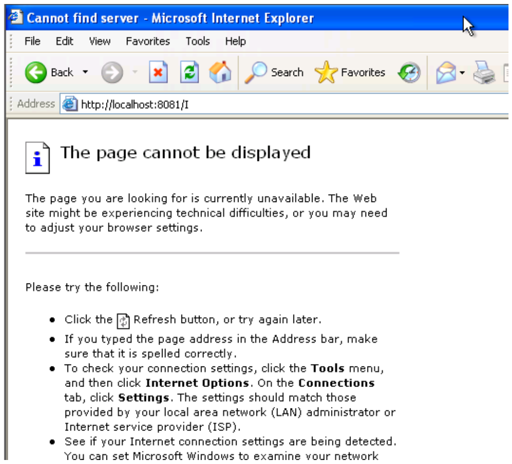


Installation failed with return value other than -1073741819
Verify if the machine is a client machine that is member of domain. Disconnect the machine from the domain temporarily during installation may solve the problem. Please uninstall application from control panel, and re-install application to further proceed.

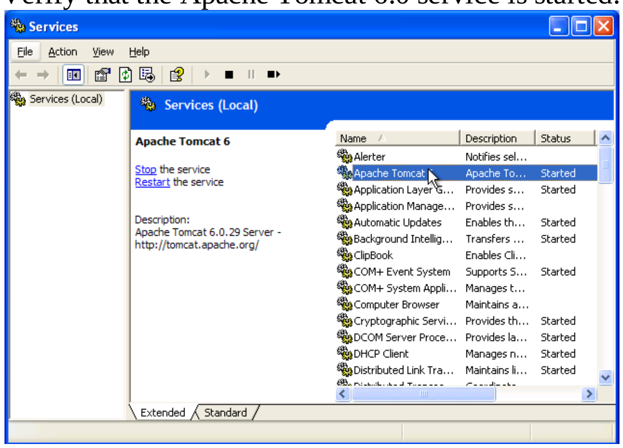
If the issue persists, mark down the pop up message and return value, and contact your system administrator.

DURING APPLICATION ACCESS

I cannot access my application via the URL – Error "Cannot find server"
Verify that the correct URL was entered.

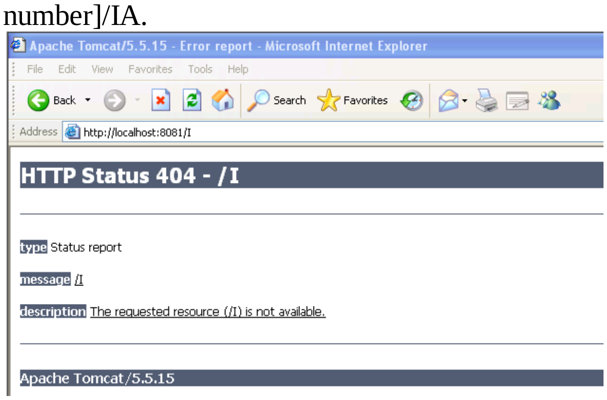


Verify that the Apache Tomcat 6.0 service is started.



I cannot access my application via the URL – Error "Error Report: HTTP Status 404 - "

Verify that the correct URL was entered, including case sensitivity. If the issue persists, contact your system administrator. The URL should be http://[hostname]:[port number]/IA.

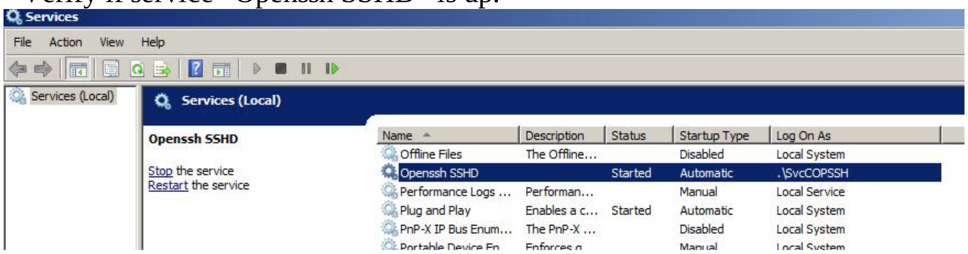


Please uninstall application from control panel, and re-install application to further proceed.

If the issue persists, contact your system administrator.

COPSSH SETUP

- Verify if service “Openssh SSHD” is up.



- Verify if port 22 is blocked by firewall.

- Windows User on Ignition Analytics server should have a password configured for SFTP to work. After setting a password, in some cases, restarting windows is needed to make it into effect.

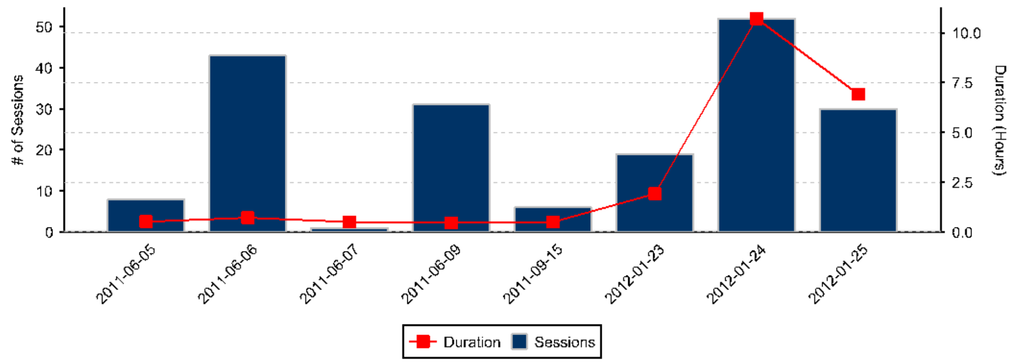
APPENDIX C

SAMPLE REPORTS

Usage Summary
by Date

AVAYA idEngines

for period 02/20/2002 - 02/20/2012



Date	Sessions #	Sessions %	Duration (Hours) #	Duration (Hours) %
Total	190		22.24	
2011-06-05	8	4 %	0.52	2 %
2011-06-06	43	23 %	0.72	3 %
2011-06-07	1	1 %	0.50	2 %
2011-06-09	31	16 %	0.45	2 %
2011-09-15	6	3 %	0.50	2 %
2012-01-23	19	10 %	1.92	9 %
2012-01-24	52	27 %	10.72	48 %
2012-01-25	30	16 %	6.91	31 %

AVAYA idEngines Identity Engines Ignition Analytics Page 1

RADIUS Audit Top 5 Users by Usage

Report Date Range 04/01/2009 - 05/16/2009