HP Service Manager

Software Version: 9.34
For the supported Windows® and UNIX® operating systems

Smart Analytics Administrator's Guide

Document Release Date: September 2014
Software Release Date: September 2014

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

For a complete list of open source and third party acknowledgements, visit the HP Software Support Online web site and search for the product manual called HP Service Manager Open Source and Third Party License Agreements.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Introduction

Built on Service Manager 9.34 and using an OEM-licensed version of HP Autonomy IDOL, HP SM Smart Analytics heralds the debut of the “Big Data" edition of Service Manager. This powerful SM-IDOL integration drives automation further into ITSM processes by mining unstructured data and by translating that data into machine-accessible structured information. This first release focuses on:

- Improving the processes of Help Desk management
- Reducing the time and effort expended on interaction submittals by end users and IT professionals
- Accelerating the process of problem management

SM Smart Analytics enables your Service Manager to become a more intelligent and efficient system by extracting and understanding your content. SM Smart Analytics includes the following features in this release:

Smart Ticket

With Smart Ticket, you can quickly submit a Service Desk ticket by just entering a description or attaching a screenshot. SM Smart Analytics will intelligently populate other fields such as category or affected services by extracting and analyzing the content that you entered in the ticket.

Hot Topic Analytics

Hot Topic Analytics intelligently displays an interactive diagram indicating the hot topics among recent incidents so that you can easily discover incident trends and identify problem candidates.

Audiences

This document is intended for the audiences who are responsible for setting up, maintaining, or using SM Smart Analytics.

Setting up SM Smart Analytics

Note: You can obtain all the installation files described in this section from the HP Service Manager Smart Analytics (9.34) installation media (`T5001-15075.iso`).

To set up SM Smart Analytics, follow these steps:

Step 1: Install and configure Service Manager

To install and configure Service Manager, follow these steps:

1. Make sure that you have installed or upgraded to Service Manager to the following:
   - Server: SM 9.34 Patch 1
   - Web tier and Windows client: SM 9.34
   - Applications: SM 9.34

   Note: You can find these installation packages from the SM Smart Analytics installation media (`T5001-15075.iso`). For installation instructions, refer to Service Manager *Release Notes* on HP Software Support Online (SSO): http://support.openview.hp.com/selfsolve/document/KM00705452

2. (Optional) If you want to enable SM mobility ESS for end users, after you deploy or upgrade to SM 9.34, install the new Mobility client (`Mobility4SmartAnalytics-9.34.0040.war`), and then apply the `Mobility4SmartAnalyticsCP9.34.1.0040.unl` unload file.

   Note: If previously you have already enabled the mobile ESS feature by applying the mobile

ESS content pack for Service Manager 9.32, instead of applying the unload file, you need to manually resolve the conflicts after upgrading to Service Manager 9.34.

3. Apply the `SmartAnalyticsCP9.34.1.0042.unl` unload file on your Service Manager server by using Unload Manager:
   a. Go to **System Administration** > **Ongoing Maintenance** > **Unload Manager**.
   b. Double-click **Apply Unload**. A wizard opens.
   c. Select the unload file you want to apply, also specify a backup file, and then click **Next**. Details of the unload file appear.
   d. Double-click a conflicting object in the table to open the merge tool:
      i. Merge the object, and then select the Reconciled check box.
      ii. Click **Save** to go back to the wizard.
   e. Click **Next** after all the conflicting objects are reconciled.
   f. Click **Yes** on the confirmation window to apply the unload.
   g. Click **Finish**.

   Now, the unload has been applied and at the same time your old data backed up.
4. Install the language packs for SM Smart Analytics if needed.

Step 2: Install SM Smart Analytics

Follow the instructions in the following sections to install SM Smart Analytics:

Overview

SM Smart Analytics is powered by HP IDOL. You need to prepare IDOL servers to deploy SM Smart Analytics.

You can deploy SM Smart Analytics IDOL servers as a standalone or distributed system, depending on the amount of data to index and the number of actions to process.

Note: For more information, see the *Service Manager Smart Analytics 9.34 Deployment Sizing Guide*, which will be published on SSO (http://support.openview.hp.com/selfsolve/documents) as a white paper.

Standalone

Install all the IDOL server components on one host, including content, community, category, view, and agentstore components.

Distributed

1. Install multiple content servers (at least two) on different hosts. The content server indexes, collects, manipulates, and stores data.
2. Install the IDOL proxy server on a separate host, which includes the community, category, view, Distributed Index Handler (DIH), Distributed Action Handler (DAH), and agentstore components. The IDOL proxy server automatically routes tasks to the appropriate content servers.

Image server

The IDOL image server is required for both standalone and distributed setups to perform the Optical Character Recognition (OCR) tasks. You can install the image server on the same host as the IDOL server in the standalone setup or the IDOL proxy server in the distributed setup. However, we recommend that you install the image server on a dedicated host for better performance.

System Requirements

This section lists the hardware requirements and the supported operation systems for the SM Smart Analytics servers.

Hardware requirements

Standalone IDOL server

- A dedicated SCSI disk
- 32 GB RAM (4 GB minimum)

Note: If you want to install the image server on the same machine as the standalone IDOL server, 8 GB RAM is the minimum requirement.

- 200 GB Disk
- 8 cores CPU (a minimum of 2 dedicated CPU - XEON 3 GHz or above)

Distributed

For the IDOL proxy server:

- A dedicated SCSI disk
- 32 GB RAM (4 GB minimum)
- 100 GB Disk
- 8 cores CPU (a minimum of 2 dedicated CPU - XEON 3 GHz or above)

For each content server:

- A dedicated SCSI disk
- 4 GB RAM
- 100 GB Disk
- a minimum of 2 dedicated CPU - XEON 3 GHz or above

Image server

- A dedicated SCSI disk
- 4 GB RAM
- 100 GB Disk
- a minimum of 2 dedicated CPU - XEON 3 GHz or above

Supported operating systems

- Windows x86 64

  The following lists the most fully tested operating systems:

  - Windows Server 2012 x86 64
  - Windows Server 2008 R2 x86 64

- Linux x86 64

  The following lists the minimum recommended versions:

- Red Hat Enterprise Linux (RHEL) 5
- SuSE Linux Enterprise Server (SLES) 10

Install SM Smart Analytics servers on Windows

Note: Before you install the SM Smart Analytics servers, make sure that your servers meet the system requirements as specified in "System Requirements" on page 10.

Standalone

To install SM Smart Analytics servers on Windows in the standalone setup, follow these steps:

1. Run the Smart Analytics installer for Windows (`setupSmartAnalyticsWindowsX64.exe`).

   Note: If you are re-installing Smart Analytics server on the same host, be sure to clear the target directory before re-installation.

2. View the introduction of the installer, and then click **Next**.
3. Read and accept the license agreement, and then click **Next**.
4. Select **Standalone**, and then click **Next**.
5. Select the servers that you want to install:
   - **IDOL Server**: The IDOL server includes the content, community, category, view, and agentstore components.
   - **Image Server**: The image server performs the Optical Character Recognition (OCR) tasks.
6. Choose an installation folder, and then click **Next**. The default installation folder is: `C:\Program Files\HP SM SmartAnalytics`
7. Choose where you want to create a shortcut for Smart Analytics, and then click **Next**
8. If you are installing the IDOL server, specify the following ports, and then click **Next**.
   - IDOL Server Port: The action (ACI) port number. Default: 9000
   - IDOL Index Port: The port number for index actions. Default: 9001
   - IDOL Service Port: The port on the host server on which the service listens for service status and control requests. Default: 9002

9. Specify the Service Manager server, and the click **Next**.

   You need to specify the IP addresses (or host names) of the Service Manager servers that are permitted to send administrative and query actions to the Smart Analytics servers. Use commas to separate multiple addresses (no space before or after a comma).

10. If you are installing the image server, specify the following ports, and then click **Next**.

    - Image Server Port: The port for sending actions to the image server. Default: 18000
    - Image Service Port: The port on the host server on which the service listens for service status and control requests. Default: 18001

11. View the pre-installation summary, and then click **Install**. If you want to change your configuration, click **Previous**.

12. Wait for the installation to complete, and then click **Done**.

13. Make sure that the Smart Analytics services are started according to your installation.

Server name	Service name
Standalone IDOL server	`HP SM Smart Analytics Server`
Image server	`HP SM Smart Analytics Image Server`

Tip: If you want to uninstall SM Smart Analytics from Windows, select "HP SM Smart Analytics" in **Programs and Features** from the control panel, and then click **Uninstall**.

Distributed

To install SM Smart Analytics on Windows in the distributed setup, follow these steps:

Note: For the distributed installation, you must install at least two content servers in different destinations to connect to an IDOL proxy server.

1. Install the first content server on one host:

   a. Run Smart Analytics installer for Windows (`setupSmartAnalyticsWindowsX64.exe`).

   b. View the introduction of the installer, and then click **Next**.

   c. Read and accept the license agreement, and then click **Next**.

d. Select **Distributed**, and then click **Next**.

e. Select **Content Server** to install the first content server.

f. Choose an installation folder, and then click **Next**.

g. Choose where you want to create a shortcut, and then click **Next**.

h. Specify the following ports for the content server, and then click **Next**.

- Content Server Port: The port number for the content server. Default: 21000
- Content Index Port: The port number for content index. Default: 21001
- Content Service Port: The port on the server on which the service listens for service status and control requests. Default: 21002

i. Specify the IDOL proxy server to which the content server connects, and then click **Next**.

> **Note:** This is the host name or IP address of the IDOL proxy server that you need to install after installing two content servers.

j. View the pre-installation summary, and then click **Install**.

k. Wait for the installation to complete, and then click **Done**.

2. Register the service for the content server on Windows:

a. Open the command-line window.

b. Type the following command, and then press Enter.

```
cd CONTENT_SERVER_INSTALL_DIR
```

> **Note:** CONTENT_SERVER_INSTALL_DIR is the directory that contains content.exe

c. Type the following command, and then press Enter.

```
content.exe -install
```

The content service is registered successfully without any prompt.

> **Tip:** If you want to remove the content service, run the following command:
> `content.exe -uninstall`

3. Repeat the previous two steps to install the second content server on a different host and register

the service.

Tip: We recommend that you install the second content server on a different host for the distributed setup. However, if you want to install the second content server on the same host as the first content server, follow these step:

a. Create a directory at the same level of the first content server. For example, you can name it as content2.

b. Copy the following files from installation directory of the first content server to the directory that you created in the previous step:

- langfiles
- modules
- content.cfg
- content.exe
- licensekey.dat

c. Rename content.exe to a different name such as content2.exe.

d. Rename content.cfg to the same name as the .exe file in the previous step such as content2.cfg. Make sure that the new file name (without extension) for .cfg matches the new file name for .exe, otherwise the content server cannot start.

e. Edit the .cfg file as needed. For example, at least you need to modify the ports to avoid port conflict.

f. Register the new content service by following the same instruction in step 2.

4. Install the IDOL proxy server:

a. From the installer, select **Distributed**, and then select **IDOL Proxy Server**. The IDOL proxy server includes the community, category, view, DIH, DAH, and agentstore components.

b. Choose an installation folder, and then click **Next**.

c. Choose where you want to create a shortcut, and then click **Next**.

d. Specify the following ports for the proxy server, and then click **Next**.

- IDOL Server Port: The action (ACI) port number. Default: 9000
- IDOL Index Port: The port number for index actions. Default: 9001

- IDOL Service Port: The port on the host server on which the service listens for service status and control requests. Default: 9002

e. Specify the Service Manager server, and then click **Next**.

You need to specify the IP addresses (or host names) of the Service Manager servers that are permitted to send administrative and query actions to the Smart Analytics servers. Use commas to separate multiple addresses (no space before or after a comma).

f. Specify the IP addresses and the ports of the two content servers that you created in the previous steps, and then click **Next**.

g. View the pre-installation summary, and then click **Install**.

h. Wait for the installation to complete, and then click **Done**.

5. Install the image server:

a. From the installer, select **Distributed**, and then select **Image Server**. The image server performs image analysis, including Optical Character Recognition (OCR).

b. Choose an installation folder, and then click **Next**.

c. Choose where you want to create a shortcut, and then click **Next**.

d. Specify the Service Manager server, and the click **Next**.

You can specify the IP addresses (or host names) of the Service Manager servers that are permitted to send administrative and query actions to the Smart Analytics servers. You can use commas to separate multiple addresses (no space before or after a comma).

e. Specify the following ports for the image server, and then click **Next**.

- Image Server Port: The port for sending actions to the image server. Default: 18000
- Image Service Port: The port on the host server on which the service listens for service status and control requests. Default: 18001

f. View the pre-installation summary, and then click **Install**.

g. Wait for the installation to complete, and then click **Done**.

6. Make sure that the SM Smart Analytics services are started on the servers according to your installation.

Server name	Service name on Windows
Distributed IDOL server	`HP SM Smart Analytics Proxy Server`
Image server	`HP SM Smart Analytics Image Server`
Content servers	`content` **Note:** The service name is the same as the file name of "content.exe" without the .exe extension. If you change content.exe to content1.exe, the service name will be content1.

Tip: If you want to uninstall SM Smart Analytics from Windows, select "HP SM Smart Analytics" in **Programs and Features** from the control panel, and then click **Uninstall**.

Install SM Smart Analytics on Linux

Note: Before you install the SM Smart Analytics servers, make sure that your servers meet the system requirements as specified in "System Requirements" on page 10.

To install the SM Smart Analytics servers on Linux, follow these steps:

1. Obtain the SM Smart Analytics installer (`setupSmartAnalyticsLinuxX64.bin`) for Linux from the SM Smart Analytics installation media.
2. Run the installer from the command line or by using the GUI interface on the Linux server, and then follow the on-screen instructions to install SM Smart Analytics.

   Tip: For more information on the configuration items during installation, refer to the installation section for Windows.

3. Run the corresponding commands to start the SM Smart Analytics servers that you installed:
   - IDOL server (standalone or distributed)

     ```
     [INSTALL_DIR]/IDOLServer/scripts/StartIDOL.sh
     ```

     Tip: If you want to stop the IDOL server, run the following command:

```
[INSTALL_DIR]/IDOLServer/scripts/StopIDOL.sh
```

- Content server

  ```
  INSTALL_DIR]/IDOLServer/content/startContent.sh
  ```

  Tip: If you want to stop the content server, run the following command:

  ```
  [INSTALL_DIR]/IDOLServer/content/stopContent.sh
  ```

- Image server

  ```
  [INSTALL_DIR]/ImageServer/scripts/StartImageserver.sh
  ```

  Tip: If you want to stop the image server, run the following command:

  ```
  [INSTALL_DIR]/ImageServer/scripts/StopImageserver.sh
  ```

Tip: If you want to uninstall the Smart Analytics servers from Linux system, remove the installation directory directly.

Step 3: Enable and configure SM Smart Analytics in Service Manager

To enable and configure SM Smart Analytics, follow these steps:

1. In Service Manager, set up the connection to the SM Smart Analytics servers and enable SM Smart Analytics. See "Enable Smart Analytics in Service Manager" on page 19.

   Note: If you want to set up SSL connection, see "Configure SSL between Service Manager and Smart Analytics " on page 28.

2. Set up data cleansing configuration. See "Configure data cleansing" on page 20
3. Configure Smart Ticket. See "Configure Smart Ticket" on page 22.
4. Configure Hot Topic Analytics. See "Configure Hot Topic Analytics" on page 26.
5. Add the "idol.assistant" capability word to operator records. See "Add Smart Analytics capability word for power users" on page 27.

Administrator tasks

This section includes the following topics to help you configure or trouble shoot SM Smart Analytics as administrators:

Enable Smart Analytics in Service Manager

User Role: Administrator

To enable Smart Analytics in Service Manager and set up connections, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Configuration**.
2. Make sure that the **Smart Analytics Server Enabled** check box is selected to enable Smart Analytics. You can clear the selection if you want to disable the Smart Analytics feature or if you need to disconnect Service Manager from the Smart Analytics IDOL servers.
3. Enter the address and port for the IDOL server (for standalone) or the IDOL proxy server (for distributed setup), and then click **Test Connection**.
4. Make sure that **Image Server Enabled** check box is selected to enable the Optical Character

Recognition (OCR) feature for the Smart Ticket.

Note: This OCR feature for Smart Ticket only functions when **Smart Analytics Server Enabled** is checked in step 2.

5. Enter the address and port for the IDOL image server, and then click **Test Connection**.
6. Click **Save**.

Configure data cleansing

User Role: Administrator

The purpose of data cleansing is to remove unwanted data from the data set that is used to train and index into Smart Analytics as well as runtime processing.

Note: The data cleansing configurations will be applied to all the fields that are defined as "Content" or "Category based on following fields" in the configuration GUI.

To add a data cleansing configuration, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Data Cleansing**.
2. Select a module.
3. Select one of the following actions:
   - **Remove**: Remove the matched texts and index the rest to SM Smart Analytics.
   - **Include**: Extract and index the texts between the start pattern and the end pattern exclusively.
   - **Exclude**: Exclude the texts that match the pattern (including start, end, and all the words between them) and index the rest to SM Smart Analytics.
4. Select the **Active** check box to activate this configuration.
5. Type the text or pattern for the action that you selected. To learn how the text or pattern takes effect, see the following examples.

- Example o fthe **Remove** action:

Configured text to be removed	`[telephone communication history with customer]:`
Original content	`[telephone communication history with customer]: Microsoft Office keeps asking for installation of additional components / language packs.`
After cleansing	`Microsoft Office keeps asking for installation of additional components / language packs`

- Example of the **Include** action:

Start pattern	`description of the issue:`
End pattern	`actions suggested by help desk agent:`

Original content	`Description of the issue:`
	`Sent items are not being sent by Outlook.`
	`Actions suggested by help desk agent:`
	`asked customer to check network connection status, shows connection is OK`

After cleansing	`Sent items are not being sent by Outlook.`

- Example of the **Exclude** action:

Start pattern	`[appendix: error log]`
End pattern	`[end of appendix]`

Original content	`SQL Server is down and cannot be restarted.`
	`[appendix: error log]`
	`Xxxxxxxxxxxxxxx`
	`[end of appendix]`

After cleansing	`SQL Server is down and cannot be restarted.`

Note: Regular expressions are not supported.

6. Select the **Match Case** checkbox if you only want to find the texts that match the case of the text or pattern that you entered.
7. Click **Add**.

Configure Smart Ticket

User Role: Administrator

Smart Ticket provides the following two out-of-box auto-classification configurations:

- Category
- Affected Service

These out-of-box configurations are best practices based on the out-of-box data. You can use or modify these configurations, or you can add new configurations that best reflect your business needs.

Add a new auto-classification

To add a new auto-classification, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Select **Blank** from the drop-down list, and then click **Add**.

   Note: Alternatively, you can choose an out-of-box template, and then modify it.

3. Type the task name for the new classification.
4. Go to the **Configurations** tab.
5. Select a module for auto-classification. For example, Interaction.
6. In the **Training Sample query** field, define a query to refine the sample data. The default value is true, which means all the data will be used as the source data.
7. Select the target fields to be automatically filled by SM Smart Analytics. You can select up to three levels. For example, category.
8. Select the source fields that the auto classification is based on. For example, title and description.
9. In the **Training Optimization** tab, modify the settings for training optimization.

   Note: We recommend that you keep the default settings. For more information on improving

accuracy for Smart Ticket, see "Improving accuracy for Smart Ticket" on page 40.

Setting	Description
Training Samples Per Category	The maximum records to be used as the training samples for each category.
Test Data Coverage	The percentage of records out of the total source data that are used to test the trained system.
Source Data Coverage	The percentage of records out of the total source data that are used to train the system.
Training Method	■ Choose "best term" for a faster training process if you have huge data volume. ■ Choose "training documents" for a higher accuracy with a slower training process.
Adjust Term Weight From Test Result	Select this option to automatically adjust the term weight for some terms in some categories based on testing result. Default: Disabled
Remove Low Weight Document	After the training is finished by using the "training documents" method, check the weight of every training document, and then remove the low-weight training documents from the training sample pool. Default: Disabled **Weight Threshold** The threshold to remove the low weight training documents, after finish training by using the "training documents" training method. **Min Number of Training Samples** The minimum number of the training documents in a category. Use this parameter to ensure that a certain number of training samples will not be remove when the system removes the low weight training documents.

10. Click **Add**. The new classification is now added to the **Current Configuration List**.

Perform training and testing

To perform a training for an auto-classification, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Click a task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
3. Click the **Training** button to start training this auto-classification.

   Tip: You can click **Refresh Status** to view the latest training status.

4. When the training is done, click **Testing**. When the testing is finished, you can view an estimated result of the accuracy for this auto-classification in the **Testing Result** field.

   Tip: The quality of the sample data is critical to the accuracy of the auto-classification. To refine your sample data, you can define a query in **Training Sample query** field under the **Configurations** tab. For more best practices to improve accuracy, see "Improving accuracy for Smart Ticket" on page 40

Apply a rule-based training

You can append the rule-based analysis on top of the meaning based analysis. The typical scenario is that if one particular ticket has the same relevancy within several categories, you can append a rule to one specific category to improve the categorization accuracy.

"Rule Field Name" is where you can specify the field based on which you define the rule,

"Apply Rule" lists all the categories, where you can choose the target category and set the value for the rule you want to append.

For example, suppose there are two affected services, "printer_San Diego" and "printer_Shanghai". You can define the rule field as "Primary Contact Location City". Then, set value "San Diego" to the "printer_San Diego", and set value "Shanghai" to the "printer_Shanghai". With this rule, if the contact person for the new coming ticket is from San Diego office, the ticket will be automatically filled with "printer_San Diego" as the affected service.

To apply a rule-based training for an auto-classification, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Click a task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
3. Go to the **Configurations** tab.
4. In the **Rule Field Name** field, specify the field name based on which you define the rule.

5. Click **Apply Rule**. A list containing all the categories appears, where you can choose the target category and set the value for the rule you want to append.
6. Click a category.
7. In the **Rule Field Value** field, set the value for the rule that you want to append.
8. Click the **Apply Rule** button.

Perform tuning in the Smart Ticket definition

Another way to improve the accuracy of Smart Ticket is to perform tuning continually for the Smart Ticket definition.

To perform tuning in the Smart Ticket definition, follow these steps:

1. Service Desk agents select tuning candidates during their daily work:
   a. In an interaction record, update the fields suggested by Smart Ticket if the suggested values are incorrect, such as category or affected service.
   b. After the interaction is closed, from the interaction record, click **More** > **Add to Tuning Records** to add this record as a tuning candidate for Smart Ticket.

   Note: The **Add to Tuning Records** option is only available when an interaction is in the "Closed" status.
2. A system administrator tunes Smart Ticket after a period of time to increase the accuracy:
   a. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
   b. Click a task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
   c. Go to the **Tuning** tab.
   d. Click **Manage Tuning Records** to open **Tuning Records** where you can find all the tuning candidates.
   e. Delete the meaningless or inappropriate records. The rest of records will be used in tuning Smart Ticket.
   f. Click the **Tuning** button to start the tuning process.

Configure Smart Ticket for multi-company

SM Smart Analytics supports multi-tenancy. When multi-company mode is enabled in Service Manager, you can configure specific Smart Ticket definition to apply to multiple companies when applicable. The Smart Ticket configuration takes effect on these companies individually by segregating their data in Smart Analytics database.

To specify the companies in the Smart Ticket definition, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Click a task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
3. Click the **Multiple Company** tab, and then do one of the following:
   - Click **Add Company** to add companies to this configuration.

     Note: A training is needed if you add a new company.

   - Click **Remove Company** to remove companies to this configuration.

Configure Hot Topic Analytics

User Role: Administrator

To configure Hot Topic Analytics, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**.
2. From the **Analytic Corpus** tab, modify the following settings as needed:
   - **Index Condition**: Define a query to specify the records that you want to include in Hot Topic Analytics.
   - **Title Field**: Select a field to define the title when viewing individual incident in Hot Topic Analytics. The title field is also an important data source for hunting.
   - **Contents Fields**: Select the data source for Hot Topic Analytics. Be sure to only use text fields such as description and solution.
3. From the **Filter Fields** tab, modify the following settings as needed:

- **Timestamp Field**: Select a field to indicate the time stamp for filtering.
- **Properties Fields**: Select fields that can be used for advanced filtering in Hot Topic Analytics. For example, you can define Category or Priority as filter.

4. From the **Advanced** tab, modify the following settings as needed:
   - **Expiry Time**: Hot Topic Analytics removes the data that was indexed longer than the setting in this field from its analysis.
   - **Max Return Results**: The maximum records returned from Hot Topic Analytics.
5. Click **Save** to save your modification.
6. Click the **Start Index** to start indexing.

   Tip: You can click **Refresh Status** to refresh the index status.

Add Smart Analytics capability word for power users

User Role: Administrator

To enable power users such as Service Desk Agent or Problem Coordinator to use the Smart Analytics features, you need to add the "idol.assistant" capability word to the their operator records. The operators with this capability word can see the **Service Desk** > **Open Smart Interaction** and **Problem Management** > **Hot Topic Analytics** menus and use these features.

Note: ESS self-service users are able to submit Smart Request tickets after you enable SM Smart Analytics. No additional capability word is needed.

To add the "idol.assistant" capability word to an operator record, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Operators**.
2. Enter or select your search criteria, and then click **Search**.
3. Select an operator from the record list to view the operator record.
4. Click the **Startup** tab.
5. Add `idol.assistant` in the **Execute Capabilities** section.

Configure SSL between Service Manager and Smart Analytics

User Role: Administrator

If you want to set up SSL connection between Service Manager and Smart Analytics, follow these steps as an example:

Note: The following steps are just to create the self-signed certificate, which is used for internal use and testing only.

1. Use OpenSSL to generate the SSL certificate files for the Smart Analytics server:
   a. Generate a private key:

      ```
      openssl genrsa -out idolserver.key 2048
      ```

   b. Generate a Certificate Signing Request (CSR):

      ```
      openssl req -new -key idolserver.key -out idolserver.csr
      ```

   c. Generating a self-signed certificate:

      ```
      openssl x509 -req -days 365 -in idolserver.csr -signkey
      idolserver.key -out idolserver.crt
      ```

2. Configure the certificate in the Smart Analytics server:
   a. Update the `AutonomyIDOLServer.cfg` file as the following:

      ```
      [server]
      SSLConfig=SSLOption1
      SSLIDOLComponents=TRUE

      [SSLOption1]
      SSLMethod=SSLV23
      SSLCertificate=<absolute path to the idolserver.crt file>
      SSLPrivateKey=<absolute path to the idolserver.key file>

      [IndexServer]
      SSLConfig=SSLOption1

      [DataDRE]
      SSLConfig=SSLOption1

      [CatDRE]
      SSLConfig=SSLOption1
      ```

```
[AgentDRE]
SSLConfig=SSLOption1

[Agent]
SSLConfig=SSLOption1
```

b. Update the `AgentStore.cfg` file as the following:

```
[server]
SSLConfig=SSLOption1
SSLIDOLComponents=TRUE

[IndexServer]
SSLConfig=SSLOption1

[SSLOption1]
SSLMethod=SSLV23
SSLCertificate=<absolute path to the idolserver.crt file>
SSLPrivateKey=<absolute path to the idolserver.key file>
```

3. Restart the Smart Analytics server, and then verify that SSL is in use:

   - Check the log (*<Smart Analytics server>*`\IDOL\logs\application.log`). The following example confirms that SSL is in use.

     ```
     17/07/2014 18:27:23 [0] 00-Always: Engine [content] state : RUNNING
     17/07/2014 18:27:23 [0] 00-Always: Engine [community] state : RUNNING
     17/07/2014 18:27:23 [0] 00-Always: Engine [category] state : RUNNING
     17/07/2014 18:27:23 [0] 00-Always: Engine [agentstore] state : RUNNING
     17/07/2014 18:27:23 [0] 00-Always: Engine [view] state : RUNNING
     17/07/2014 18:27:23 [0] 00-Always: All 5 components started successfully.
     17/07/2014 18:27:23 [0] 30-Normal: ACI Server validated operations key.
     17/07/2014 18:27:23 [0] 30-Normal: ACI Server has no QPS limit.
     17/07/2014 18:27:23 [0] 30-Normal: ACI Server is licensed for SSL encryption.
     17/07/2014 18:27:23 [0] 30-Normal: This ACI Server will not accept
     unencrypted communications from ACI clients.
     17/07/2014 18:27:23 [0] 30-Normal: Running with FIPS mode inactive
     17/07/2014 18:27:23 [0] 30-Normal: ACI Servers runs in SSL mode.
     ```

   - If viewing from a web browser by entering comments (such as `https://<SmartAnalyticsServer>:9000/`), a warning is displayed. If you continue, the response in the browser indicates that unencrypted communications are disallowed, which confirms that SSL is working.

4. In the Service Manager server, add the certificate (`idolserver.crt`) to keystore by running the following commands:

   ```
   keytool -import -v -alias sm -keystore smtrust -storepass password -
   file idolserver.crt
   ```

5. Update the `sm.ini` file by adding the following lines:

   ```
   truststoreFile:smtrust
   truststorePass:password
   ```

6. Restart the Service Manager server.

Use Smart Analytics Assistant

User Role: Administrator

Smart Analytics Assistant is a build-in tool for you to perform some administrative actions in Smart Analytics. For example, you can use this tool for troubleshooting.

To use Smart Analytics Assistant, follow these steps:

1. In the command line, type `saa`, and then press Enter.
2. Select one of the actions for Smart Analytics from the drop-down list.

   Note: Replace <*variable_value*> in the query examples with the corresponding value such as database name and file name.

   - **Backup Category**

     Export a category including its descendants, training documents and terms and weights to XML format. The file is stored in the *<Smart Analytics server>*`\IDOL\category\Imex` directory.

     Query:

     ```
     http://<SmartAnalyticsServer>:<port>/action=CategoryExportToXML&cat
     egory=<variable_
     value>&includeCatID=true&ExportFileName=MyCategory.xml
     ```

   - **Backup Index**

     Export all the index documents of a database from Smart Analytics server to a series of compressed files in the following current working directory of the Smart Analytics server: *<Smart Analytics Server>*`\IDOL\content`. If no DatabaseMatch specified, export all documents.

     Query:

     ```
     http://<SmartAnalyticsServer>:<indexPort>/DREEXPORTIDX?DatabaseMatc
     h=<variable_value>
     ```

- **Restore Category**

  Import category information contained in an XML file to a specified category, and build the category immediately.

  Query:

  ```
  http://<SmartAnalyticsServer>:<port>/action=CategoryImportFromXML&I
  mportFilename=c:\\path\to\MyCategory.xml&BuildNow=true
  ```

- **Restore Index**

  Restore IDX: Index IDX or XML files located on a machine that Smart Analytics can access directly into the Smart Analytics. If no DREDbName specified, use dbname of the indexed file.

  Query:

  ```
  http://<SmartAnalyticsServer>:<indexPort>/DREADD?c:\\path\to\xxx.id
  x&DREDbName=<variable_value>& CreateDatabase=True
  ```

- **View Index Status**

  Check the status of index actions in the Smart Analytics index queue.

  Query:

  ```
  http://<SmartAnalyticsServer>:<port>/action=indexerGetStatus
  ```

- **View Log** (Action History)

  Display a log of requests, including the date and time that a request was made, the client IP address that made the request, and the internal thread that handled the action.

  Query:

  ```
  http://<SmartAnalyticsServer>:<port>/action=GRL&format=xml
  ```

- **View Status**

  Request details about all components. Check whether all components are up and running; check how many documents are in each database.

  Query:

  ```
  http://<SmartAnalyticsServer>:<port>/action=GetStatus
  ```

Note: By default, the Smart Analytics server port is 9000 and the index port is 9001.

3. Click **Run**. The result of the action is displayed.

Transfer Smart Analytics intelligence between systems

User Role: Administrator

As an administrator, you may want to transfer the intelligence in Smart Analytics from one system to another system. For example, when you finish testing Smart Analytics in your testing environment, you may want to migrate the configured Smart Analytics to your production environment.

To transfer Smart Analytics from one environment (source) to another environment (target), follow these steps:

1. Prepare an unload file from your source SM.

File name	Condition
cate2idol2	True
Idoladapter	True
Idolpbmhunter	True
Idolindex	True
idolDataFilter	True
Number	name="cate2idolid" or name="idoladapterid" or name="idolpbmhunter" or name="idolindexid" or name="idoldatafilter"

2. Back up index and category data of the original Smart Analytics server. To do this, run the following commands in the SM Smart Analytics Assistant (SAA) utility:

   `http://<idolhost>:<indexport>/DREEXPORTIDX?FileName=c:/backup_index`

   `http://<idolhost>:<categoryport>/action=BackupServer&path=c:\backup_category`

   Tip: *<idolhost>* is the address of the Smart Analytics server. By default, the index port is 9001 and the category port is 9020.

   Note: For how to use the SM SAA utility, see "Use Smart Analytics Assistant" on page 30.

3. Copy the generated index and category backup files to the file system of the target Smart Analytics server.

4. Import the unload file that you generated in step 1 into the target SM server.
5. In the target SM server, configure the Smart Analytics server to connect to the address of the new Smart Analytics server.
6. [Optional] Clean the target Smart Analytics server if it is not clean:
   - Clean index

     To do this, run the following command from the web browser on the Smart Analytics server:

     `http://localhost:<indexport>/DREINITIAL`

     Note: You must run this command locally on the Smart Analytics server instead of using SM SAA utility due to security restriction.

   - Clean category

     To do this, run the following command by using the SM SAA utility:

     `http://<idolhost>:<aciport>/action=CategoryDelete&Category=0`

     Tip: By default, the ACI port is 9000. You can find all the port numbers by performing the following action in SM SAA:

     `http://<idolhost>:<aciport>/action=GetStatus`

7. Restore the index and category data into the new Smart Analytics server by running the following commands from the SM SAA utility on the target SM server:
   - `http://<idolhost>:<indexport> /DREADD?c:\path\to\<xxx>.idx&CreateDatabase=True`
   - `http://<idolhost>:<categoryport> /action=RestoreServer&filename=c:\backup_category\<xxx>.zip`
   - `http://<idolhost>:<categoryport>/action=CategorySyncCatDRE`

   Now, the target SM server works for both Smart Ticket and Hot Topic Analytics as the source SM server does.

User tasks

This section includes some typical user tasks after implementing the SM Smart Analytics:

Create a Smart Ticket in ESS

User Role: Self-service Users

If you have installed and enabled Smart Analytics, a new menu, **Submit a Smart Request**, is automatically added to leverage the power of the Smart Ticket feature. Clicking it opens a new, simplified request form that only requires “description” or “attachment” to submit a request, which simplifies the process of submitting the ESS support requests.

To submit a self-service request using Smart Ticket in self-service user view (ess.do), follow these steps:

1. Log on to Service Manager.
2. Click **Submit a Smart Request**.
3. Type the description for your request.
4. Click **Add Files** to attach an image file. For example, a screenshot of the error message.
5. Click **Submit**.

   An interaction is now created. The fields defined in Smart Ticket configuration are automatically filled by SM Smart Analytics.

Create a Smart Ticket in SRC

User Role: Self-service Users

To submit a support request in SRC, follow these steps:

1. Log on to Service Manager from the SRC portal.
2. Click **Support**, and then click **Create**.
3. Type a description for your request.
4. Add an attachment. For example, a screenshot of the error message.
5. Fill in other required information.
6. Click **Submit**.

   An interaction is now created. The fields defined in Smart Ticket configuration are automatically filled by SM Smart Analytics.

Create a Smart Ticket in Mobility client

User Role: Self-service Users

To submit a self-service request in Mobility client, follow these steps:

1. Log on to Service Manager on your mobile device.
2. Click **Open Ticket**.
3. Type a description for your request.
4. Add an attachment. For example, a screenshot of the error message.
5. Click **Submit**.

   An interaction is now created. The fields defined in Smart Ticket configuration are automatically filled by SM Smart Analytics.

Create a Smart Ticket in power user view

User Role: Service Desk Agent

To submit a request on behalf of a user in power user view (index.do), follow these steps:

1. Log on to Service Manager.
2. Click **Service Desk** > **Open Smart Interaction**.
3. Fill in the name of the contact.
4. Type a description of the issue.

5. Click **Smart Classification**.

   The **Category**, **Area**, **Subarea**, and **Affected Service** fields are intelligently populated with the most likely values based on the analysis by SM Smart Analytics. Meanwhile, SM Smart Analytics also suggests some other possible values for you to choose from.

   Note: If you are not satisfied with the values suggested by SM Smart Analytics, you can click the **Fill Field** icon to manually choose a value for each field.

6. Click **Continue**. The full interaction form is displayed, and the corresponding fields are populated with the values that you specified in the previous step.

7. Complete the interaction with additional information if needed, and then proceed your ticket accordingly.

Create a problem by using Hot Topic Analytics

User Role: Problem Coordinator

You can easily identify problem candidates based on the hot areas automatically suggested by Hot Topic Analytics.

Note: You must use the web client to view the dynamic topic map in Hot Topic Analytics.

To find problem candidates by using Hot Topic Analytics, follow these steps:

1. Log on to Service Manager from the web client.

2. Click **Problem Management** > **Hot Topic Analytics**.

3. View the hot topics suggested by Hot Topic Analytics.

   - The size of a topic indicates the heat of the topic. The background color of a topic is just to identify the topic.

   - You can click a hot topic to drill down to the sub-topics.

   - The incidents that belong to a topic are displayed in the list on the right. You can click the incident ID to view the incident record.

4. If you want to run a custom analysis, enter your keywords, and then click **Find Hot Topics**.

5. To further refine the result, click Advanced Filters, specify your filters, and then click **Search** again. The graphic is refreshed with the filtered results.

6. After you identify the problem candidates, select the check boxes before the incident IDs, and

then click **Create problem** to create a problem based on incidents.

A new problem is now created based on the incidents that you selected.

SM Smart Analytics best practices

This section provides you some best practices on how you can configure and use SM Smart Analytics so that it brings more values to your business.

Tailoring

This section provides some best practices on tailoring Service Manager for SM Smart Analytics.

Extend auto-classification to modules with Process Designer enabled

Service Manager provides several Process Designer rule sets for applying Smart Ticket in the Service Desk module. Follow the out-of-box rule sets, you can create new rule sets to extend the Smart Ticket feature to other modules.

Rule Set	Description
sd.idol.ocr	This rule triggers Optical Character Recognition (OCR) and auto-classification to fill the fields defined in the Smart Ticket definitions.
sd.idol.tuning.action	This rule sends the record to the tuning list.

For example, if you want to automatically classify change category with Process Designer enabled, follow these steps:

1. Define Smart Ticket task for Change module:

    a. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Configuration** > **Smart Tickets**.

    b. Select **Blank**, and the click the **Add** button

    c. In the **Add Smart Ticket Task** form, fill in the task name with any words meaningful to you.

d. In the **Configuration** tab, choose **Change** for **Module Name**.

e. With the help of "Query Builder", provide a query condition clause in **Training Sample Query**. This query decides which change records will be sent to Smart Analytics server for Smart Ticket training.

f. Enter the fields in Change that you want to be automatically filled by Smart Ticket, for example, "category."

g. Enter the fields in Change that you want to use as the inputs for Smart Analytics to provide suggestions,for example, "description."

2. Create Smart Ticket rule sets for Change workflow by referring to the OOB Smart Ticket rule sets.

> **Tip:** For how the design workflows and rule actions, see Process Designer documents that were release together with Process Designer content packs.

3. Add Smart Ticket rule sets to Change workflow:

a. From **Change Management** > **Configuration** > **Change Workflows**, select the workflow that you want to apply Smart Ticket, for example, "standard change."

b. Select the **Registration and Categorization** phase.

c. Click the **Rule Sets** tab in the property section.

d. Select the **On Exit** event.

e. Select the Smart Ticket rule that you created.

Add filters to the Hot Topic Analytics form

The out-of-box Hot Topic Analytics form contains some filter fields, if you want to add more filter fields, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**.

2. Go to the **Filter Fields** tab.

3. In the **Properties Fields** section, select fields that can be used for advanced filtering in Hot Topic Analytics. For example, you can define Category or Priority as filter.

4. Click **Save** to save your modification.

5. Add the new filter fields into the "Hot Topic Analytics" form using the form designer

Improving accuracy for Smart Ticket

SM Smart Analytics provides several methods to help you to increase Smart Ticket accuracy according to different data sets.This section include some best practices you can follow to improve your accuracy for Smart Ticket.

- **Set up data cleansing rules**

  Data cleansing can help you prepare sample data that you want to send to Smart Analytics for indexing and training. By setting up proper data cleansing rules, you can have better quality of sample data, which is critical to the best accuracy of auto-suggestion.To set up data cleansing rules, see "Configure data cleansing" on page 20.

- **Choose best sample data**

  In the definition for Smart Ticket or Hot Topic Analytics,you can specify a sample data query, through which you can decide what kind of data that you want to use as sample data to teach Smart Analytics server to build the intelligence out of your large data volume.

- **Apply rule based training for Smart Ticket**

  The basic training of Smart Ticket is meaning based training, which means Smart Analytics builds intelligence based on the text information of your data. On top of meaning based intelligence, SM Smart Analytics also supports you to add rule based training to the Smart Ticket. Those rules will further increase the suggestion accuracy, especially in the case that multiple suggestion results have the same relevancy with the new ticket. The typical scenario is that if one particular ticket has the same relevancy within several categories, you can append a rule to one specific category to improve the categorization accuracy.

  For how to apply a rule to the Smart Ticket task definition, see "Apply a rule-based training" on page 24.

- **Optimize your training for Smart Ticket**

  Several advanced parameters are defined in Smart Ticket task definition which are used to optimize your accuracy of auto suggestion. But please be noted, the settings here are tradeoffs between training time and accuracy. It means higher accuracy is achieved at the cost of longer training time. Listed below are some best practices for these optimization configurations.

  - Training by documents vs. training by terms

    Choose “best term” for a faster training process if you have huge data volume; choose "training documents" for a higher accuracy with a slower training process.

  - Training sample per category

The maximum records for each category, normally more training sample per category leads to higher accuracy but longer training time.

- Source data coverage

  The percentage of records out of the total source data that are used to create categories. Normally the higher percentage means higher accuracy, but there is a threshold point, when training source data percentage exceed it the margin contribution will be lowered remarkably. The out of the box value for this configuration is "90%", it is a best number tested in the lab. You can use the "source data coverage calculator" tool to find the best number for your data set.

- Document weight and term weight

  Enable"Adjust term weight from test result" to automatically adjust the term weight for some terms in some categories based on testing result, which may help improve accuracy.

  Enable "Remove low weight document" to help reduce the disturbance of low relevance training samples and improve accuracy.

  By default, these two parameters are disabled in the out-of-box environment.

  These advanced features need your experiment to get best results. You may enable either one or both.

- **Perform tuning periodically**

  Tuning the training result is a mechanism to continuously improve the accuracy of auto suggestion. For how to tune the training result, see "Perform tuning in the Smart Ticket definition" on page 25.

Set stop phrases for Hot Topic Analytics

User Role: Administrator

If you want to add stop phrases for Hot Topic Analytics, follow these steps:

1. Make sure the following configuration is defined in the `AutonomyIDOLServer.cfg` file:

   ```
   QuerySummaryStopPhraseMode=9
   ```

2. Run Hot Topic Analytics, and then find the topics that you want to remove from the topic map.
3. Stop the Smart Analytics server.
4. Add those words as stop phrases in the `./content/main/qssp.db` file.
5. Start the Smart Analytics server.
6. Run Hot Topic Analytics again. Now, those stop phrases are no longer displayed in the topic map.

Troubleshooting

This section contains the following topics to help administrators to troubleshoot SM Smart Analytics:

Troubleshooting: Checking Smart Analytics log files

You can check the following log files to help you troubleshoot Smart Analytics issues:

Service Manager server log

This Service Manager server log file (`sm.log`) tracks all interactions between Service Manager and Smart Analytics. By default, the `sm.log` file is in the following directory: `<Service Manager>\Server\logs\sm.log`.

Smart Analytics log files

The log files from the Smart Analytics IDOL server provide details to help you identify possible problems or invalid configurations. By default, you can find these log files in the following directory on the Smart Analytics IDOL server:

- Linux: `/opt/HP/SM/SmartAnalytics/IDOLServer/IDOL/logs`
- Windows: `C:\HP SM SmartAnalytics\IDOL10.6Server\IDOL\logs`

Check the following table for details about the log files in IDOL server.

File name	Description
action.log	Logs all the actions on IDOL server.
agentstore_ application.log	Logs general application errors, warnings and information relating to the agent index.
agentstore_ index.log	Logs messages relating to the indexing, deletion and updating of agents.
agentstore_ query.log	Logs messages relating to the querying of agents.
application.log	Logs general application errors, warnings and information relating to indexes.
category_ application.log	Logs general application errors, warnings and information relating to the category index.
category_ category.log	Logs messages relating to category actions that read or manipulate the categories, including errors, warnings and progress information.
category_ cluster.log	Logs messages relating to cluster actions, including errors, warnings and progress information.
category_ schedule.log	Logs messages relating to the running of the Analysis Schedules that are specified in the configuration file.
category_ taxonomy.log	Logs messages relating to the TaxonomyGenerate action, including errors, warnings and progress information.
content_ application.log	Logs general application errors, warnings and information relating to the data index.
content_ index.log	Logs messages relating to the indexing, deletion and updating of documents.
content_ query.log	Logs messages relating to query processes.

File name	Description
content_ queryterms.log	Logs the query terms. DiSH collects this log stream using the service port to produce statistics based on query terms.
index.log	Logs the index actions that the Smart Analytics server receives.
query.log	Logs all the requests that the Smart Analytics server receives.
stats_index.log	Logs the statistics of the Smart Analytics server.

The default logging behavior of the IDOL server is keeping the log files the in the `./logs` folder and compressing log files into zip files when the size reaches 20480 KBs. You can customize the settings according to your requirements.

For example, if you want to delete history log files automatically whenever the number of log files is more than 100, you can add `LogOldAction=Delete` and `LogMaxOldFiles=100` into the configuration file.

The following are the default configuration items for the logging behavior in the IDOL server:

```
LogArchiveDirectory=./logs/archive
LogDirectory=./logs
LogTime=TRUE
LogEcho=FALSE
LogLevel=normal
LogExpireAction=compress
LogOldAction=move
LogMaxSizeKBs=20480
```

You can find these configuration items in the [Logging] section of the IDOL configuration file, which is located in the following path by default:

```
C:\Program Files\HP SM SmartAnalytics\IDOL10.6Server\IDOL\AutonomyIDOLServer.cfg
```

The following table lists the description for these configuration items:

Parameter	Description
LogArchiveDirectory	Path to log archive directory. Type the directory in which you want the application to archive old log files when *LogOldAction* is set to `Move`.
LogDirectory	Path to log directory.
LogTime	Displays time with each log entry. Enable this parameter to display the current time next to each log entry in the log file. Possible values: `TRUE` or `FALSE`
LogEcho	Displays logging messages on the console. Possible values: `TRUE` or `FALSE`

Parameter	Description
LogLevel	The log levels are hierarchical from least logging to most logging. You can use the *LogLevelMatch* parameter to specify which messages are reported relative to the specified *LogLevel*. For example, if `LogLevelMatch=LessThan` and `LogLevel=Warning`, "Normal" and "Full" message types are reported. The following are the possible values for this parameter: • `Always` Basic processes are logged. **Note:** This produces only minimal logging and no errors are logged. • `Error` Errors are logged. • `Warning` Errors and warnings are logged. • `Normal` Errors, warnings, and basic processes are logged. • `Full` Every occurrence is logged. **Note:** This produces a large log file and can affect performance.

Parameter	Description
LogExpireAction	Determines how log files are handled when they exceed the maximum size. Type one of the following to determine how log files are handled when they exceed the *MaxLogSizeKBs* size: • `Compress` The log file's name is appended with a timestamp, compressed and saved in the log directory. By default, this is a ZIP file. Use the *LogCompressionMode* parameter to specify another compression format. • `Consecutive` The log file's name is appended with a number and saved in the log directory. When the next log file reaches its *LogMaxSizeKBs* size, it is appended with the next consecutive number. • `Datestamp` The log file's name is appended with a timestamp and saved in the log directory. • `Previous` The log file's name is appended with .previous and saved in the log directory. Every time a log file reaches its *LogMaxSizeKBs* size, it is given the same postfix so that it overwrites the old log file. • `Day` Only one log file is created for each day and is appended with the current timestamp. Log files are archived after they reach the *LogMaxSizeKBs* size. **Note:** The *LogMaxSizeKBs* parameter takes precedence over the *LogExpireAction* parameter. Therefore, if you set *LogExpireAction* to Day, and the value for *LogMaxSizeKBs* results in more than one log file, multiple log files are generated for each day.

Parameter	Description
LogOldAction	Determines how log files are handled when the maximum number of log files is exceeded. Type one of the following to determine how log files are handled when the *LogDirectory* has reached the maximum number of log files, as determined by the *LogMaxOldFiles* parameter: • `Delete` The log files are deleted. • `Move` The log files are moved to the specified *LogArchiveDirectory*.
LogMaxSizeKBs	Maximum log file size (in kilobytes). If you do not want to restrict the log file size, type `-1`. The *LogExpireAction* parameter determines how a log file is handled after it has reached its maximum size.
LogMaxOldFiles	Maximum number of log files in the log directory. The maximum number of log files the specified *LogDirectory* can store before the application runs the specified *LogOldAction*. If you do not want to restrict how many log files the *LogDirectory* can store, type `-1`. (default: -1, unlimited)

Troubleshooting: Smart Analytics setup

Unable to install Smart Analytics with an error message "Windows error 216 occurred while loading the Java VM"

If you encounter the error message "Windows error 216 occurred while loading the Java VM" when installing Smart Analytics, it indicates that you are running the installer on a 32-bit Windows, which Smart Analytics does not support. For more information, see "System Requirements" on page 10.

Failed to start Smart Analytics IDOL server with error message

If you see an error message that indicates the msvcr100.dll file is missing from your computer, install .Net Framework 3.5 (or a higher version) and Visual C++ Redistributable X64 package. You can download these two packages from Microsoft website.

Failed to connect Smart Analytics IDOL server or image server

If your Service Manager failed to connect the Smart Analytics server, check the `application.log` file in the *<SM Smart Analytics>*`\ IDOL10.6Server\IDOL\logs\` directory to make sure that the Smart Analytics server is started. You also need to make sure that following five components are started: agent store, content, community, category, and view. If any component is not running normally, restart the Smart Analytics server.

The following is a sample message in the log file indicating your Smart Analytics server and the five components are started successfully:

```
30/06/2014 14:40:30 [0] 00-Always: Determining child engine status...
30/06/2014 14:40:30 [0] 00-Always: Engine [content] state : RUNNING
30/06/2014 14:40:30 [0] 00-Always: Engine [community] state : RUNNING
30/06/2014 14:40:30 [0] 00-Always: Engine [category] state : RUNNING
30/06/2014 14:40:30 [0] 00-Always: Engine [agentstore] state : RUNNING
30/06/2014 14:40:30 [0] 00-Always: Engine [view] state : RUNNING
30/06/2014 14:40:30 [0] 00-Always: All 5 components started successfully.
30/06/2014 14:40:30 [0] 30-Normal: ACI Server validated operations key.
30/06/2014 14:40:30 [0] 30-Normal: ACI Server has no QPS limit.
30/06/2014 14:40:30 [0] 30-Normal: ACI Server is licensed for SSL encryption.
30/06/2014 14:40:30 [0] 30-Normal: Performed hostname lookup and converted
USERCLIENTS from [*,127.0.0.1] -> [*,127.0.0.1,::1].
30/06/2014 14:40:30 [0] 30-Normal: Performed hostname lookup and converted
ADMINCLIENTS from [*,127.0.0.1] -> [*,127.0.0.1,::1].
30/06/2014 14:40:30 [0] 30-Normal: This ACI Server will not accept unencrypted
communications from ACI clients.
30/06/2014 14:40:30 [0] 30-Normal: ACI Server setting MaxInputString to 64000.
30/06/2014 14:40:30 [0] 30-Normal: ACI Server successfully loaded online help.
30/06/2014 14:40:30 [0] 30-Normal: ACI Server successfully loaded admin UI.
30/06/2014 14:40:30 [100] 30-Normal: ACI thread 100 attached to port 9000
30/06/2014 14:40:30 [101] 30-Normal: ACI thread 101 attached to port 9000
30/06/2014 14:40:30 [102] 30-Normal: ACI thread 102 attached to port 9000
30/06/2014 14:40:30 [103] 30-Normal: ACI thread 103 attached to port 9000
30/06/2014 14:40:30 [104] 30-Normal: ACI thread 104 attached to port 9000
```

If your Service Manager failed to connect the image server, check the `application.log` file in the *<SM Smart Analytics>*`\IDOL10.6ImageServer\Imageserver\logs`directory to make sure that the image server is started.

The following is a sample message in the log file indicating your image server is started successfully:

```
19/06/2014 10:55:43 [1] 00-Always: ACI Server starting at xxx.xxx.xxx.xxx:18000
19/06/2014 10:55:43 [54] 00-Always: ACI Server thread 1 initialized
19/06/2014 10:55:43 [55] 00-Always: ACI Server thread 2 initialized
19/06/2014 10:55:43 [57] 00-Always: ACI Server thread 3 initialized
19/06/2014 10:55:43 [58] 00-Always: ACI Server thread 4 initialized
```

Unable to see the Multiple Company tab in the Smart Ticket configuration form

1. Make sure that the multi-company mode is enabled in Service Manager. To enable the multi-company mode, follow these steps:
   a. Click System **Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
   b. On the **General** tab, select the **Run in Multi-Company Mode** option.
   c. Click **Save**.
2. Log out and log back in Service Manage for the change to take effect.

Troubleshooting: Smart Analytics operation

Train, Index, and Test buttons are disabled

If the **Train**, **Index**, and **Test** buttons are disabled in the configuration pages for Smart and Hot Topic Analytics, follow these steps:

1. Make sure that in the Smart Analytics Configuration form, the **Smart Analytics Server Enabled** option is enabled and be sure to click the **Save** button to save this configuration.
2. If the issue still exists, make sure that the upgrade to SM 9.34 is successful. Check that all of the libraries are the SM 9.34 version. The default folder is `C:\Program Files (x86)\HP\Service Manager 9.30\Server\RUN\lib`.
3. If the issue still exists, you might use an old license. In this case, launch the SM server with the new license file, which includes the Smart Analytics module license.

   For Service Manager trial version installation, follow these steps:

   a. Move your old license file out of the folder. The default folder is `C:\Program Files (x86)\HP\Service Manager 9.30\Server\RUN\`.

   b. Run "sm -instanton" to generate the instant on license.

   c. Restart the Service Manager server to load the instant on license.

Indexing or training failure

Check the SMIS task log first, and then check the information in `sm.log`. For more information, see "Check task logs in SMIS" on page 53.

Hot Topic Analytics has no result after indexing

You may need to wait for a while (by default, 120 seconds) for Smart Analytics to commit the results from cache to disk.

Unable to launch Hot Topic Analytics in the multi-company mode

The following error message is displayed and you are unable to launch Hot Topic Analytics in the multi-company mode:

```
ERROR uncaught exception: Error: "company" table doesn't have mandanten field defined
```

In this case, you need to configure the company information in Mandanten correctly.

To set up company in Mandanten, as following steps.

1. Click **System Administration** > **Ongoing Maintenance** > **Mandanten** > **Mandanten Field Restrictions**.

2. Add a new definition with "probsummary" as **Field Name** and "company" as **Mandant Field Name**.

Smart Analytics Assistant

Smart Analytics Assistant is a build-in tool that can help administrator to troubleshoot Smart Analytics. To use this tool, see "Use Smart Analytics Assistant" on page 30.

Troubleshooting: Smart Analytics background schedule in SMIS

In Smart Analytics, some background processes are managed by Integration Manager, which is a plug-in based platform called Service Manager Integration Suite (SMIS). In the out-of-box system, the following two instances:

- **SMIDOL**

  SMIDOL instance is for the training, testing, index, and tuning processes, which are triggered in **Smart Analytics Configuration**. Normally, one only has one SMIDOL instance named SMIDOL* (* is the sequence number, usually 0).

- **SMIDOLOCR**

  SMIDOLOCR instance is for the image analyzing process, which is triggered when users submit requests from the ESS portal, including SRC and Mobility. For performance consideration, you can have multiple SMIDOLOCR instances for one Service Manager server. The number of instances equals to the thread number of the image servers. If the image servers cannot be connected, only one instance is created. The instance name is SMIDOLOCR* (* is the sequence number). The OCR task is added to one of these instances after an interaction is created in ESS, depending on which instance has the least tasks in queue.

You can check the following topics for troubleshooting Smart Analytics background schedule in SMIS:

Manually create and enable the SMIDOL or SMIDOLOCR instance

The SMIDOL instance is created and enabled automatically when you enable Smart Analytics in the **Smart Analytics Configuration** menu or when the training, testing, tuning, or index process is triggered. The SMIDOLOCR is created and enabled automatically when you enable the image server in the **Smart Analytics Configuration** menu or when the image process is triggered.

If the instance is not created automatically or you want do some troubleshooting, you can manually start up the SMIS instance for Smart Analytics.

To create and enable an SMIS instance for Smart Analytics manually, follow these steps:

1. Do one of the following to access Integration Manager:
   - Click **Tailoring** > **Integration Manager**.
   - Type `smis` in the command line, and then press Enter.
2. Click **Add**.
3. Select the **SMIDOL** or **SMIDOLOCR** template, and then click **Next**. The Integration Instance Information screen is displayed.
4. Change the configuration as needed, and then click **Next**. The Parameters screen is displayed.
5. Do not change anything and click **Next**. The Fields screen is displayed.
6. Do not change anything and click **Next**. The Mapping screen is displayed.
7. Click **Finish**. The main SMIS configuration screen is displayed.
8. Click **Enable** to enable the instance.

Manually disable and remove the SMIDOL or SMIDOLOCR instance

The SMIDOL instance is removed when you disable Smart Analytics and the SMIDOLOCR instances are removed when you disable image server in the **Smart Analytics Configuration** menu.

If you want to manually disable or delete an SMIDOL or SMIDOLOCR instance, follow these steps:

1. Do one of the following to access Integration Manager:
   - Click **Tailoring** > **Integration Manager**.
   - Type `smis` in the command line, and then press Enter.
2. Select an instance, and then click **Disable** or **Remove**.

Configure the SMIDOL or SMIDOLOCR instance

If the SMISIDOL or SMISIDOLOCR instance are created automatically, the default configuration is as following:

Name:	SMIDOL* or SMIDOLOCR* (* is the sequence number)
Interval Times:	30s
Max Retry Times:	5
Log Level:	INFO
Log File Directory:	N/A
Run as system startup:	true

To change the settings for performance tuning or troubleshooting, follow these steps:

1. Do one of the following to access Integration Manager:
   - Click **Tailoring** > **Integration Manager**.
   - Type `smis` in the command line, and then press Enter.
2. Select an instance, and then click **Disable**.
3. Select the disabled instance, and then click **Edit**.
4. Change the configuration, and then click **Finish**.

Check task logs in SMIS

To view all the task logs, click **Tailoring** > **Integration Manager**, and then click **Log**.

For training, testing, tuning, and index operations, check the log for the SMIDOL* instance to identify the corresponding task.

For image operation, you have to check all SMIDOLOCR* instances to identify the corresponding task.

Tip:

- Besides the task log, the program executed by SMIS prints log to `sm.log` by default. You can define another file to print all SMIS logs by specifying the log file directory in the SMIS instance.
- By default, if SMIS fails to execute a task after five retries, the task is set as expired and will never be triggered automatically. However, you can retry the task manually.
- If a SMIS instance is always running and obviously no background process of this instance is running, this instance may be dead due to some exception that cannot be caught. In this case, you cannot disable or delete the instance from the SMIS configuration page. The workaround is to kill the corresponding SMIS process from the SM System Status page.

Limitations

SM Smart Analytics contains the following limitations in the current release:

- **Security**

  SM Smart Analytics supports the multi-company mode in this release. However, "append query" for individual users is not supported.

- **Smart Ticket**

  In this release, IT agents are unable to use the Optical Character Recognition (OCR) feature when creating interactions for users in the out-of-box environment. However, when PD is enabled, IT agents can use the "Image2Text" feature to copy and paste messages to the interaction records.

Appendix A: SM Smart Analytics API

SM Smart Analytics provides two types of APIs (RESTful API and Javascript API) for the Smart Ticket (auto-classification) feature:

Note: This release only provides APIs for Smart Ticket. For Hot Topic Analytics, you must use the Service Manager web client to view the dynamic hot topic information.

Auto-classification RESTful API

Note: You must add the capability word "RESTful API" to an user's operator record for a user to be able to execute a RESTful API request. To do this, see "Add RESTful API to operator's capabilities" on page 58.

To perform auto-classification, you need to use two RESTful APIs.

Use the first API to query all the categorization configurations, and then use your desired configuration (adapter id) to call the second API, which will return the category values.

Normally, you only need to use the first API once to get the configuration while you can use the second API to do categorization jobs as many times as you need.

API-1: Get all the configurations/adapters definitions

Request:

```
GET http://<SM Server Address>:13930/SM/9/rest/idoladapters?view=expand
```

Response example:

```
{
  "@count": 2,
  "@start": 1,
  "@totalcount": 2,
  "Messages": [],
  "ResourceName": "idoladapter",
  "ReturnCode": 0,
  "content": [
    {"idoladapter": {
      "adapter.id": 5,
      "level1.field": "affected.item",
      "source": [
```

```
        "title",
        "description"
      ]
    }},
    {"idoladapter": {
      "adapter.id": 7,
      "level1.field": "category",
      "level2.field": "subcategory",
      "level3.field": "product.type",
      "source": [
        "title",
        "description"
      ]
    }}
  ]
}
```

API-2: Get the categorization result based on adapter id. (For example: id=137, company=HP, text="my laptop is broken", return top 2 suggestions)

Request:

```
POST http://<SM Server Address>:13080/sm/9/rest/idoladapters/{adapter.id}
```

An example of request body:

```
{
  "idoladapter":{
  "source":["Critical CPU temp. BIOS error message", Maybe I work too hard, but the
temperature of my computers CPU is critical according to the error message it
displays in the message"],
  "company" :"HP",
  "top":2
  }
}
```

Response example:

```
{
  "Messages": [],
  "ReturnCode": 0,
  "idoladapter": {
    "level1.field": "category",
    "level2.field": "subcategory",
    "level3.field": "product.type",
    "suggest.candidates": [
      {
         "level1.value": "request for service",
```

```
         "level2.value": "app. infrastructure",
         "level3.value": "shared web hosting"
      },
      {
         "level1.value": "request for service",
         "level2.value": "infrastructure",
         "level3.value": "server"
      }
     ]
     }
}
```

Add RESTful API to operator's capabilities

To use the RESTful API, you must add RESTful API to operator's capabilities:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Operators**.
2. Enter or select your search criteria, and then click **Search**.
3. Select an operator from the record list to view the operator record.
4. Click the **Startup** tab.
5. Add `RESTful API` in the **Execute Capabilities** section.

Auto-classification Javascript API

This Javascript API returns an array of arrays that contains the suggested categories.

Syntax

```
lib.acicategory.getCategoryByContent(file,adapterid,numresult,company)
```

Arguments

Name	Data type	Required	Description
file	Datum object	Yes	This argument contains the object that holds the input source data. For example, an "incidents" file with title and description.
adapterid	Integer	Yes	This argument contains the id you use to call createAndTrainingOneCategory, or adapter.id in idoladapter.

numresult	Integer	Yes	This argument controls the number of suggested categories to return.
company	String	No	The company that the categories belong to. **Note:** If you use an *adapterid* with the multi-company setting configured, you must specify this parameter in your request.

Return values

An array of arrays that contains the suggested categories. For example:

```
[["incident","hardware","hardware failure"],
["incident","performance","performance degradation"],["incident","failure","job
failed"]]
```

Example

This example assumes that you configure a category group for interactions is configured as the following:

id: 201
Source fields: title and description
Category fields: category, subcategory, product_type

Then, the Javascript API can be used as in the following example:

```
var f = new SCFile("incidents");
f.title = "my pc is broken";
f.description=["Starting from yesterday, my pc cannot be started. Both battery
and power adapter looks good. The pc itself was very hot before it is broken."]
f.category="incident";
print(lib.JSON.json().stringify(lib.acicategory.getCategoryByContent
(f,201,3,"es")))
```

If the input parameter (file) includes value of level 1 and level 2 fields that are configured in the idoladapter, this function will use the their values as the parent schema to suggest child category to get better accuracy. In this example, the level 1 field is specified as `f.category="incident"`, which means the returned suggestion will all belong to the "incident" category.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Smart Analytics Administrator's Guide (Service Manager 9.34)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-ITSM@hp.com.

We appreciate your feedback!


Java™
COMPATIBLE