HP Service Manager

Software Version: 9.41

For the supported Windows® and UNIX® operating systems

Smart Analytics Administrator and User Guide

Document Release Date: September 2015
Software Release Date: September 2015

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

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: https://softwaresupport.hp.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** 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 site at: https://softwaresupport.hp.com.

This website 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 website 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 to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: https://softwaresupport.hp.com/web/softwaresupport/access-levels.

HPSW Solutions Catalog accesses the HPSW Integrations and Solutions Catalog portal website. 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 website is https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710.

Contents

Chapter 1: Smart Analytics overview

Built on Service Manager (SM) and using an OEM-licensed version of HP IDOL, 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 extracting information from different types of data. Smart Analytics in the current release focuses on the following:

- 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
- Improving search experience across a variety of internal and external content

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

Smart Ticket

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

Hot Topic Analytics

Hot Topic Analytics intelligently displays an interactive diagram that indicates the hot topics among recent interactions, incidents, or problems. Hot Topic Analytics enables you to easily discover common issues, identify escalation candidates, and create new records for escalation based on the selected candidates.

Smart Search

Smart Search enables you to search across a variety of content, including Service Manager records (such as Incidents and Changes), SharePoint documents, static web pages, and KM documents. You can integrate multiple knowledge libraries by configuring different search connectors, so that Service Manager users can search all the information that they can access.

Chapter 2: Setting up Smart Analytics

To set up Service Manager 9.41 Smart Analytics, complete the following tasks:

- "Task 1: Install Smart Analytics" below
- "Task 2: Enable and configure Smart Analytics in Service Manager" on page 21

> **Note:** If you are upgrading your Smart Analytics from a previous version to SM 9.41 Smart Analytics, see "Upgrade to Service Manager 9.41 Smart Analytics" on page 22.

Task 1: Install Smart Analytics

To install Smart Analytics, follow the instructions in these sections:

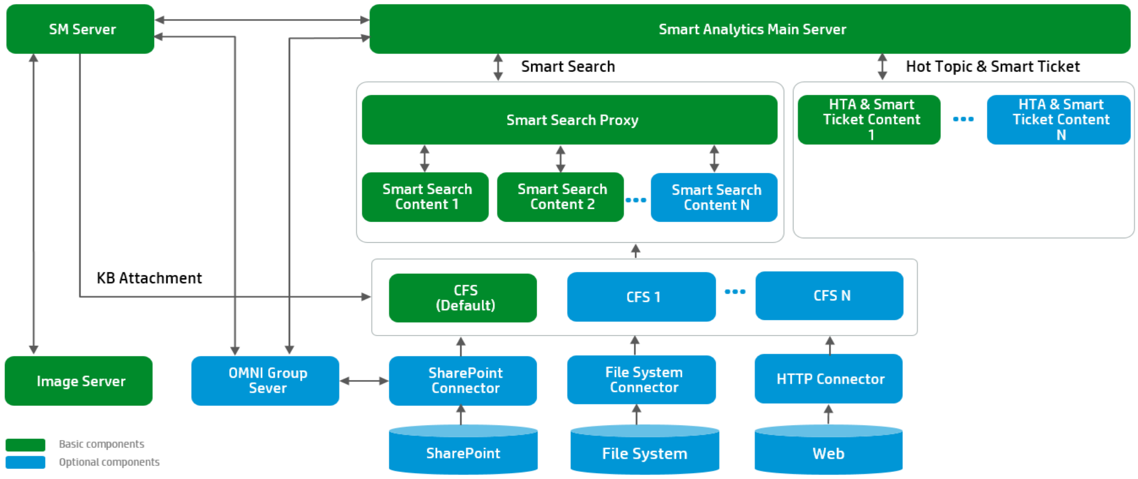
> **Note:** Before you install Service Manager 9.41 Smart Analytics, make sure that you have installed or upgraded to Service Manager 9.41 Applications.

> **Caution:** Before you turn off your computer, you must stop all Smart Analytics service to avoid any damage to the Smart Analytics data. To stop service for all Smart Analytics components, you can manually stop all the components, or run the stop.bat (for Windows) or the StopAll.sh (forLinux) script from the *<Smart Analytics Installation>*/scripts folder.

Installation overview

Smart Analytics is powered by HP IDOL. You need to prepare servers to deploy Smart Analytics. Check the information of Smart Analytics architecture as displayed in the following image before installation.

IDOL Deployment Diagram



Note: For more information, see the *Service Manager Smart Analytics Deployment Sizing Guide*, which is available on HP Software Support Online (https://softwaresupport.hp.com) as a white paper.

Quick installation	
Components included	• Smart Analytics Main Server • Smart Search Proxy server • One content server for Hot Topic Analytics and Smart Tickets • Two content servers for Smart Search • Default Connector Framework Server (for attachment index for Smart Search) • Image server for OCR
Default configuration	• Smart Analytics Main Server port: 9000 • Image server port: 18000 • CFS server port: 7000
Advanced installation	
Components included	• All components included in quick installation • Distributed Content Server

Quick installation	
	• Distributed Image Server • CFS server
Default configuration	• SharePoint connector port: 36000 • OMNI group server port: 5057 • HTTP connector port: 5678 • File system connector port: 1234 **Note:** After you install a connector, you must configure the parameters for this connector from the corresponding .cfg file before you start the service. For a configuration example, see "Configure an HTTP connector" on page 46.

Here is the description of the Smart Analytics connectors and protocol required for the installation.

Component	Description
OMNI Group Server	Communicates with SharePoint connector and LDAP to retrieve access permissions for your users. In this way, the access permissions can be applied to documents in the Smart Analytics main server. **Note:** LDAP - Lightweight Directory Access Protocol. A protocol that applications can use to retrieve information from a server. LDAP is used for directory services (such as corporate e-mail and telephone directories), and user authentication.
SharePoint Connector	Retrieves information from a Microsoft SharePoint repository, through the SharePoint web services. The connector can also retrieve information from an instance of SharePoint Online.
File system Connector	Retrieves various document types from file system so that the documents are available in global search.
HTTP Connector	A powerful tool for retrieving documents from a web site. The HTTP Connector uses spiders to find web pages and to process the web pages for content and links to other web sites. HTTP Connector can retrieve various document types, including Web documents, Word, Excel, and PDF files.

System requirements

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

Hardware requirements

Quick installation

- 64 GB RAM (8 GB minimum)
- 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above)
- 500 GB disk

Advanced installation

For the Smart Analytics proxy server (including DIH, DAH, community, category, agentstore, view, and one second-level DIH and DAH), one Hot Topic Analytics content, and two sets of Smart Search content:

- 64 GB RAM (8 GB minimum)
- 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above)
- 500 GB disk

Here is the description of the components for the Smart Analytics proxy server.

Component	Description
DIH (Distributed Index Handler)	Allows you to efficiently split and index extremely large quantities of data into multiple Smart Analytics servers, in order to create a completely scalable solution that delivers high performance and high availability. It provides a flexible way of transparently batching, routing, and categorizing the indexing of internal and external content into Smart Analytics main server.
DAH (Distributed Action Handler)	Distributes actions to multiple versions of Smart Analytics main server or a component. It allows you to use failover, load balancing, or distributed content.
Community	A Smart Analytics main server component that manages users and communities.

Component	Description
Agentstore	Smart Analytics main server stores agents and categories in the Agentstore component.
Category	A Smart Analytics main server component that manages categorization and clustering
View	A Smart Analytics main server component that converts files in a repository to HTML formats for viewing in a Web browser.

For each content or image server:

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

For each connector and CES and OMNI Group server:

- 2 GB RAM
- CPU - XEON 3 GHz or above
- 20 GB disk

Installation template	Hardware requirements
Basic	• 64 GB RAM (8 GB minimum) • 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above) • 500 GB disk
All in one	• 64 GB RAM (8 GB minimum) • 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above) • 600 GB disk
Distributed IDOL content server	• 4 GB RAM • A minimum of 2 dedicated CPU - XEON 3 GHz or above • 100 GB disk
Distributed image server	• 4 GB RAM • A minimum of 2 dedicated CPU - XEON 3 GHz or above • 100 GB disk

Supported operating systems

For the information about supported operating systems, see Service Manager 9.41 *Support Matrix*.

Install 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.

To perform Smart Analytics on a Windows-based system, follow these steps:

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

   > **Note:** If you are re-installing the same Smart Analytics component (except the content server and image server) on the same host in the same location, make sure that you shut down all Smart Analytics services, and then clear the installed Windows services and the target directory before re-installation.

2. Read the License Agreement. If you accept it, select the corresponding option, and then click **Next**.

3. Select the corresponding option for a new installation, and then click **Next**.

4. Choose an installation folder, and then click **Next**. The default installation folder is `C:\Program Files(x86)\HP\Service Manager 9.41\SmartAnalytics`.

5. Select your installation type and continue with the corresponding installation steps.

   > **Note:** If you cannot decide the correct host names or ports that you need to enter during the installation, or you want to change your settings after installation, you can modify the following configuration files after installation:
   >
   > - Smart Analytics main server: *<Smart Analytics Installation>*/IDOL/AutonomyIDOLServer.cfg
   > - Image server: *<Smart Analytics Installation>*/ImageServer#/ImageServer#.cfg
   > - Image proxy server: *<Smart Analytics Installation>*/ImageProxyServer/dah.cfg
   >
   >   This is only required if you have installed multiple image servers in the distributed mode.

- Content server: *<Smart Analytics Installation>*/Content#/Content#.cfg
- CFS server: *<Smart Analytics Installation>*/CFS/CFS.cfg
- SharePoint connector: *<Smart Analytics Installation>*/SharepointRemoteConnector/SharepointRemoteConnector.cfg
- OMNI group server: *<Smart Analytics Installation>*/OmniGroupServer/OmniGroupServer.cfg
- HTTP connector: *<Smart Analytics Installation>*/HTTPConnector/httpconnector.cfg
- File system connector: *<Smart Analytics Installation>*/FileSystemConnector/filesystemconnector.cfg

Restart the corresponding components after you modify the related configuration files.

Quick installation

Quick installation deploys the minimum required components to perform Smart Analytics on Service Manager internal data only. It sets default configurations, and no extra data source connectors are installed.

To perform quick installation for Smart Analytics on Windows, continue with these steps:

1. Select **Quick Install** as the installation type, and then click **Next**.
2. Enter the IP address of your Service Manager Server and select the IP address of your local machine from the drop-down list.

   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 (do not use a space before or after a comma).

   Note: Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

3. Enter the IP address, and the IPv6 address of the machines on which you have installed or will install any content server on a different machine. Use commas to separate multiple addresses (do not use a space before or after a comma).

> **Note:** IPv6 address is required here even if it is not used in Smart Analytics configuration. This is because internal components may communicate through IPv6 addresses.

> **Tip:** To get the IPv6 address of the local machine that the client server is installed on. Type **ipconfig** in the Windows command window and click **Enter**. Get the IPv6 address value of the working network for Smart Analytics.

4. Follow the configuration steps to configure the Smart Analytics server, Smart Search proxy server, the image server, and the CFS server. Click **Next** after each step of the configuration.

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

6. Wait for the installation to complete. If you want to start the services, select the corresponding option, and then click **Next**.

7. If you want to import the out-of-box data, select the corresponding option, and then click **Next**.

> **Note:** Importing the out-of-box data will erase the previous data for Hot Topic Analytics.
>
> You can also import the out-of-box data at any time after the installation, by running the *<Smart Analytics Installation>*/OOBData/oobdata.cmd file.

8. Wait for the service to start, and then click **Done**.

> **Note:** Wait for a few minutes until all the Smart Analytics components are started.

Advanced installation

To perform advanced installation for Smart Analytics on Windows, continue with these steps:

1. Select **Advanced Install** as the installation type, and then click **Next**. For the advanced installation, you can choose installation template from different scenarios.

2. Enter the IP address of your Service Manager Server and select the IP address of your local machine from the drop-down list.

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 (do not use a space before or after a comma).

> **Note:** Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

3. Choose an installation template, and then click **Next**. To customize your installation, select the **Customize** template to choose from the available components.

   Service Manager provides five out-of-box installation templates.

Installation template	Components included	Description
Basic	○ Proxy server components (including DIH, DAH, community, category, agentstore, view, and one second-level DIH and DAH) ○ Image server ○ CFS server	Deploys the minimum required components to perform Smart Alalytics on Service Manager internal data only. No extra data source connectors are installed.
All in one	○ Proxy server components (including DIH, DAH, community, category, agentstore, view, and one second-level DIH and DAH) ○ Image server ○ CFS server ○ OMNI group server ○ SharePoint connector ○ HTTP connector ○ File system connector	Deploys all components in one physical machine. In this way, you can use the full Smart Analytics functionality without a large volume of data.
Distributed IDOL content	Content server	Add more content stores to handle

Installation template	Components included	Description
server		more data
Distributed image server	○ Image server ○ Image proxy server	By default, one image server is included in the basic installation to handle OCR process. If there are too many image processing requests, you can deploy a distributed image server.
Customize	No pre-set component	Install any component based on your customized requirements.

4. **When you install the Smart Analytics main server:**

   Enter the IP address, and the IPv6 address of the machines on which you have installed or will install any content servers. Use commas to separate multiple addresses (do not use a space before or after a comma).

   Note: IPv6 address is required here even if it is not used in Smart Analytics configuration. This is because internal components may communicate through IPv6 addresses.

   Tip: To get the IPv6 address of the local machine that the client server is installed on. Type **ipconfig** in the Windows command window and click **Enter**. Get the IPv6 address value of the working network for Smart Analytics.

   When you install a Smart Analytics content server:

   Enter the IP address, and the IPv6 address of the machine on which you have installed or will install Smart Analytics main server.

5. Follow the configuration steps to configure the servers and connectors you selected. Click **Next** after each configuration step.

   Some useful information for configuration:

   - **Configure Smart Search Proxy Server** > **Replicas** : Specifies the number of identical copies of each document to index. This is configured in the level2proxy\AutonomyIDOLServer.cfg file.

     The default value is set to **0**, which means that there is only one copy of each document for Smart Search. If you set the number as 1, it means that there will be two mirrored copies of the document in your Smart Search content servers.

In consistent hashing mode, content is distributed between virtual nodes, which the DIH assigns to its child servers. When you configure replicas, DIH copies the documents in a particular virtual node to two or more child servers. This method ensures there are two mirrored copies of the document in your system without you having to set up specifically mirrored child servers

> **Note:** The number of copies (that is, the value of Replicas plus one) must be no more than the number of child servers. If you create more copies than there are child servers, DIH does not start.

- **Configure SharePoint Connector** > **SharePoint URL Type**:
  - To retrieve all content databases and site collections, set the value of this parameter to **WebApplication**. Set the value of the SharepointUrl parameter to the URL of the web application. You cannot use this value with SharePoint Online.
  - To retrieve only one site collection, set the value of this parameter to **SiteCollection**. Set the value of the SharepointUrl parameter as the URL of the site collection.
- **Configure LDAP Repository** (for OMNI Group server):
  - LDAP User Base: the base DN or top level of the directory tree you want to search for users. This indicates where in the LDAP directory tree you want to begin the search.
  - LDAPGroupBase: the base DN or top level of the directory tree you want to search for groups. This indicates where in the LDAP directory tree you want to begin the search.
  - (Optional) UserFilter: the query you want to use to retrieve the set of users you want to store in the group server. For example, `UserFilter=(objectClass=user)`.
  - (Optional) GroupFilter: you can use GroupFilter to set the filter that is passed to the LDAP server to request a list of groups. For example, `GroupFilter=(objectClass=hpGroup)`.

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

7. Wait for the installation to complete. If you want to start the services, select the corresponding option, and then click **Next**.

   > **Note:** HP recommends you to start the services manually after you configure the .cfg files for each connector.

8. If you want to import the out-of-box data, select the corresponding option, and then click **Next**.

   - Importing the out-of-box data will erase the previous data for Hot Topic Analytics.
   - You can also import the out-of-box data at any time after the installation, by running the *<Smart Analytics Installation>*/OOBData/oobdata.cmd file.

9. Wait for the service to start, and then click **Done**.

   - Wait for a few minutes until all the Smart Analytics components are started.
   - Make sure that all the required components are started. If not, you must start the corresponding component manually.

Tip: If you want to uninstall SM Smart Analytics, see "Uninstall Smart Analytics" on page 75.

Install 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 a Linux-based system, 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.

   To get the Hostname of the local machine that the client server is installed on, type **hostname -A** in the command line.

> To get the IPv6 address of the local machine that Smart Analytics main server is installed on, type **ifconfig** in the command line to get the **inet6** value.

3. Run the following command to import the out-of-box data before you start any component of Smart Analytics:

   ```
   [INSTALL_DIR]/OOBData/ImportOOBData.sh
   ```

4. Run the corresponding commands to start the SM Smart Analytics servers that you installed:

   - To start the main components of SM Smart Analytics servers, run the following command:

     ```
     [INSTALL_DIR]/scripts/StartALL.sh
     ```

     This script starts three content servers, a Smart Search proxy server, a main proxy server, a Connector Framework Server (CFS), and an image server one by one.

     > **Note:** By running this script, you also start the other components, such as connectors, if they are installed.

     > **Tip:** If you want to stop all these components, run the following command:
     >
     > ```
     > [INSTALL_DIR]/scripts/StopALL.sh
     > ```

5. Run the corresponding commands to start each component that you installed:

   - To start a content server, run the following command:

     ```
     [INSTALL_DIR]/scripts/StartContent[x].sh
     ```

     > **Note:** Replace [x] with the number of your content server, for example, `StartContent1`.

     > **Tip:** If you want to stop a content server, run the following command:
     >
     > ```
     > [INSTALL_DIR]/scripts/StopContent[x].sh
     > ```

   - To start both the main proxy server and the Smart Search proxy server, run the following command:

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

> **Note:** Before you start the main proxy server, make sure all the content servers have started.

> **Tip:** If you want to stop the main proxy server, run the following command:
>
> ```
> [INSTALL_DIR]/scripts/StopIDOL.sh
> ```

- To start a Connector Framework Server (CFS), run the following command:

  ```
  [INSTALL_DIR]/scripts/StartCFS.sh
  ```

  > **Tip:** If you want to stop a Connector Framework Server (CFS), run the following command:
  >
  > ```
  > [INSTALL_DIR]/scripts/StopCFS.sh
  > ```

- To start an image server, run the following command:

  ```
  [INSTALL_DIR]/scripts/StartImageServer[x].sh
  ```

  > **Note:** Replace [x] with the number of your image server, for example, `StartImageServer1`.

  > **Tip:** If you want to stop an image server, run the following command:
  >
  > ```
  > [INSTALL_DIR]/scripts/StopImageServer[x].sh
  > ```

- To start an image proxy server, run the following command:

  ```
  [INSTALL_DIR]/scripts/StartImageDAH.sh
  ```

  > **Tip:** If you want to stop an image proxy server, run the following command:
  >
  > ```
  > [INSTALL_DIR]/scripts/StopImageDAH.sh
  > ```

- To start an HTTP connector, run the following command:

```
[INSTALL_DIR]/scripts/StartHTTPConnector.sh
```

> **Tip:** If you want to stop an HTTP connector, run the following command:
>
> ```
> [INSTALL_DIR]/scripts/StopHTTPConnector.sh
> ```

- To start a file system connector, run the following command:

  ```
  [INSTALL_DIR]/scripts/StartFileSystemConnector.sh
  ```

  > **Tip:** If you want to stop a file system connector, run the following command:
  >
  > ```
  > [INSTALL_DIR]/scripts/StopFileSystemConnector.sh
  > ```

> **Tip:** If you want to uninstall SM Smart Analytics, see "Uninstall Smart Analytics" on page 75.

Task 2: Enable and configure Smart Analytics in Service Manager

To enable and configure Smart Analytics, follow these steps:

1. In Service Manager, set up the connection to the Smart Analytics servers and enable Smart Analytics. See "Enable Smart Analytics in Service Manager" on page 30.

   > **Note:** If you want to set up an SSL connection, see "Configure TSL/SSL for two-way authentication " on page 55.

2. Set up data cleansing configuration. See "Configure data cleansing" on page 30.

3. Configure Smart Ticket. See "Configure Smart Ticket" on page 35.

4. Configure Hot Topic Analytics. See "Configure Hot Topic Analytics" on page 40.

5. Set up smart search connectors. See "Configure and monitor connectors" on page 44.

6. Configure Smart Search. See "Configure Smart Search" on page 42.

7. Add the "idol.assistant" capability word to the operator records. See "Add Smart Analytics capability word for power users" on page 54.

Upgrade to Service Manager 9.41 Smart Analytics

Note: You can skip this section if you have not installed any previous version of Smart Analytics. Otherwise, follow the instructions in this section to upgrade your Smart Analytics to SM 9.41 Smart Analytics.

Before you upgrade your Smart Analytics, make sure all index tasks are finished, and then stop all the Smart Analytics services and back up all the Smart Analytics files.

- For Windows system, you must delete all the Smart Analytics services except the Image Server service.
- After you upgrade your Smart Analytics, you have to re-index the Hot Topic Analytics data. However, do not start a training for Smart Ticket.

The following instructions are for upgrading the Smart Analytics proxy server only. You need to install other components in the advanced installation mode by using the Smart Analytics installation tool. For detailed information, see "Advanced installation" on page 14.

Note: If you cannot decide the correct host names or ports that you need to enter during the installation, or you want to change your settings after installation, you can modify the following configuration files after installation:

- Smart Analytics main server: *<Smart Analytics Installation>*/IDOL/AutonomyIDOLServer.cfg
- Image server: *<Smart Analytics Installation>*/ImageServer#/ImageServer#.cfg
- Image proxy server: *<Smart Analytics Installation>*/ImageProxyServer/dah.cfg

  This is only required if you have installed multiple image servers in the distributed mode.
- Content server: *<Smart Analytics Installation>*/Content#/Content#.cfg
- CFS server: *<Smart Analytics Installation>*/CFS/CFS.cfg

- SharePoint connector: *<Smart Analytics Installation>*/SharepointRemoteConnector/SharepointRemoteConnector.cfg
- OMNI group server: *<Smart Analytics Installation>*/OmniGroupServer/OmniGroupServer.cfg
- HTTP connector: *<Smart Analytics Installation>*/HTTPConnector/httpconnector.cfg
- File system connector: *<Smart Analytics Installation>*/FileSystemConnector/filesystemconnector.cfg

Restart the corresponding components after you modify the related configuration files.

To upgrade your Smart Analytics, follow these steps:

1. Run the Smart Analytics installer for Windows (`setupSmartAnalyticsWindowsX64.exe`).
2. Check the introduction of the installer, and then click **Next**.
3. Read the License Agreement. If you accept it, select the corresponding option, and then click **Next**.
4. Select the upgrade option, and then click **Next**.

   Caution: Before you continue with the next step, make sure you have backed up all your existing files and deleted the services except the Image Server service.

5. Choose your previous installation folder for Smart Analytics, and then click **Next**.

   Note: If you are upgrading the Smart Analytics proxy server, the folder should include the IDOL folder. If you are upgrading a distributed content server, the folder should be the parent of the content folder.

Check your previous deployment type and continue with the selected upgrade steps.

Upgrade a standalone deployment

To upgrade a standalone version of Smart Analytics, continue with these steps:

1. Select **Standalone** as your previous deployment type, and then click **Next**.
2. Enter the IP address of your Service Manager Server and select the IP address of your local

machine from the drop-down list.

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 (do not use a space before or after a comma).

> **Note:** Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

3. Enter the IP address, and the IPv6 address of the machines on which you have installed or will install any content servers. Use commas to separate multiple addresses (do not use a space before or after a comma).

> **Tip:** To get the IPv6 address of the local machine that the client server is installed on. Type **ipconfig** in the Windows command window and click **Enter**. Get the IPv6 address value of the working network for Smart Analytics.

4. Follow the configuration steps to configure your smart search content servers and the CFS server. Click **Next** after each step of configuration.

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

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

> **Note:** During the Smart Analytics upgrade process, the existing configuration file will be renamed to <component name>-old.cfg. After you finish the upgrade, compare it with the new configuration file. If there is any customized change made in the previous .cfg file and it is still valid, manually add it back to the new .cfg file.

Upgrade a distributed deployment - Smart Analytics proxy server

To upgrade a distributed version with the Smart Analytics proxy server installed, continue with these steps:

1. Select **Distributed** as your previous deployment type, and then click **Next**.

2. Select **HP SM Smart Analytics Proxy**, and then click **Next**.

3. Enter the IP address of your Service Manager Server and select the IP address of your local machine from the drop-down list.

   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 (do not use a space before or after a comma).

   > **Note:** Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

4. Enter the IP address, and the IPv6 address of the machine on which you have installed or will install the content server.

   > **Tip:** To get the IPv6 address of the local machine that the client server is installed on. Type **ipconfig** in the Windows command window and click **Enter**. Get the IPv6 address value of the working network for Smart Analytics.

5. Follow the configuration steps to configure your smart search content servers and the CFS server. Click **Next** after each step of configuration.

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

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

   After you upgrade your Smart Analytics, you need to manually modify the following configurations in the *<SmartAnalytics>*/IDOL/AutonomyIDOLServer.cfg file.

Configurations after upgrade	Configurations in your previous file	You need to modify the value to
VirtualDatabases=1	VirtualDatabases=<x>	VirtualDatabases=<x>

[vdb0]
dbname=Users
type=combinator
mapsto=0:Users
	[VDB0]
	DbName=News
	Type=Combinator
	MapsTo=0:News
		Do not change

Configurations after upgrade	Configurations in your previous file	You need to modify the value to

	[VDB<x>]
	DbName=my_database
	Type=Combinator
	MapsTo=<y>:my_database
	Note: The number of x starts from 1.
		[VDB<x>]
		DbName=my_database
		Type=Combinator
		MapsTo=<y+1>:my_database
		○ You must add the VDB configurations by their number sequence.
		○ There may be other content between two VDB configuration sections.
		○ Make sure the total number of the VDB configuration sections equals to the number specified in the VirtualDatabases parameter.
		○ There is no difference if you use the upper or lower case for the section name of [VDB<x>].

[DistributionIDOLServers] Number=2	[DistributionIDOLServers] Number=<x>	[DistributionIDOLServers] Number=<x+1>

[IDOLServer0]
Name=SmartSearch
Host=12.3.4.56
Port=20010
DistributeByFieldsValues=GlobalSearch
		Do not change

Configurations after upgrade	Configurations in your previous file	You need to modify the value to

[IDOLServer1]
Name=Content1
Host=
Port=
DistributeByFieldsValues=CONTENT1
	[IDOLServer<x>]
	Host=12.3.4.56
	Port=20010
	DistributeByFieldsValues=CONTENT<x>
	Note: The number of x starts from 0.
		[IDOLServer<x+1>]
		Name=Content<x+1>
		Host=12.3.4.56
		Port=20010
		DistributeByFieldsValues=CONTENT<x+1>
		○ You must add the IDOL server configurations by their number sequence.
		○ Make sure the total number of the IDOL server configuration sections equals to the number specified in the [DistributionIDOLServers] Number parameter.

Note: During the process that you upgrade the Smart Analytics, the existing configuration file will be renamed to <component name>-old.cfg. After you finish the upgrade, compare it with the new configuration file. If there is any customized change made in the previous .cfg file and it is still valid, manually add it back to the new .cfg file.

Upgrade a distributed deployment - Smart Analytics content server

To upgrade a distributed version with the Smart Analytics content server installed, continue with these steps:

1. Select **Distributed** as your previous deployment type, and then click **Next**.
2. Select **Content**, and then click **Next**.
3. Specify the content folder for your content server, and then click **Next**.

Use commas to separate multiple content folders (do not use a space before or after a comma).

> **Note:** Make sure the content folder is directly under the install folder you have specified.

4. Enter the IP address of your Service Manager Server and select the IP address of your local machine from the drop-down list, and then click **Next**.

> **Note:** Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

5. Enter the IP address, and the IPv6 address of the machine on which you have installed Smart Analytics.

> **Tip:** To get the IPv6 address of the local machine that the client server is installed on. Type **ipconfig** in the Windows command window and click **Enter**. Get the IPv6 address value of the working network for Smart Analytics.

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

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

> **Note:** During the process that you upgrade the Smart Analytics, the existing configuration file will be renamed to <component name>-old.cfg. After you finish the upgrade, compare it with the new configuration file. If there is any customized change made in the previous .cfg file and it is still valid, manually add it back to the new .cfg file.

Chapter 3: Administrator tasks

This section includes the following topics to help you configure or troubleshoot 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:

> **Note:** When Smart Analytics communicates with Service Manager, only IPv4 is supported and IPv6 is not supported.

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Configuration**.
2. Click the **Enable Smart Analytics** button to enable Smart Analytics.

   After you click this button, a message is displayed to state that once you migrate to IDOL, you cannot use SOLR as the search engine any more and you have to log out and re-log in to Service Manager before Smart Analytics is applied.
3. Click **Yes** to migrate to IDOL. Your account logs out automatically and you need to re-log in to Service Manager.
4. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Configuration**.
5. Enter the address and port for Smart Analytics server, and then click **Test Connection**.
6. Enter the address and port for the default CFS server, and then click **Test Connection**. This default CFS server is used for Service Manager attachment index.
7. Enter the address and port for the Image Server, and then click **Test Connection**.
8. Click **Save**.

   Once you click **Save**, all the Service Manager Integration Suite tasks for the Smart Analytics integration are automatically started.

Configure data cleansing

User Role: Administrator

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

- For Smart Ticket and Hot Topic Analytics features, data cleansing is only applied to the "Title Field" or "Content Fields" that are defined in configurations.
- For Smart Search, data cleansing can be applied to any field individually which you can configure. For detailed information, see the data cleansing description from "Managing Smart Search Knowledgebases" on page 48.
- All modification for data cleansing will take effect from next round of indexing.

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. For example, Interaction.

   Note: In the module drop-down list there is a Global option. This means that it's a global data cleansing record for all modules which are using Hot Topic Analytics and Smart Ticket.

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.
   - **ExtractFromTemplate**: Extract the content from template that is configured as regular expressions. The capturing groups that are matched by the Regular Expressions are extracted and returned.
4. Enter the text or pattern for the action that you selected. For the **Remove** action, you only need to type the text string to be removed. For the **Include** and **Exclude** actions, the start pattern is the text string that you need to specify while the end pattern can be one of these options: a text string that you specify, end of line, or end of document.

The processing of the **ExtractFromTemplate** action is of first priority. The Data cleansing actions are processes in the following order:

a. **ExtractFromTemplate**

If there are matched texts found, then return. Otherwise, perform the **Include** action.

b. **Include**

If there are matched texts found, then perform the **Remove** action. Otherwise, perform the **Exclude** action..

c. **Exclude**

If there are matched texts found, then perform the **Remove** action.

d. **Remove**

To learn how the text or pattern takes effect, see the following examples.

- Example of the **Remove** action:

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

- Examples of the **Include** action:

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`

Start pattern	`description of the issue:`
End pattern	`actions suggested by help desk agent:`
After cleansing	`Sent items are not being sent by Outlook.`

Original content	Description of the issue: Items are not sent by Outlook. Actions suggested by help desk agent: asked customer to check network connection status, shows connection is OK
Start pattern	description of the issue:
End pattern	**End of line**
After cleansing	Items are not sent by Outlook.

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
Start pattern	description of the issue:
End pattern	**End of document**
After cleansing	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

- Examples of the **Exclude** action:

Original content	SQL Server is down and cannot be restarted. [appendix: error log] Details: Xxxxxxxxxxxxxxxx [end of appendix]
Start pattern	[appendix: error log]
End pattern	[end of appendix]
After cleansing	SQL Server is down and cannot be restarted.

Original content	SQL Server is down and cannot be restarted.

	[appendix: error log] Details: Xxxxxxxxxxxxxxxx [end of appendix]
Start pattern	[appendix: error log]
End pattern	**End of line**
After cleansing	SQL Server is down and cannot be restarted. Xxxxxxxxxxxxxxxx [end of appendix]

Original content	SQL Server is down and cannot be restarted. [appendix: error log] Details: Xxxxxxxxxxxxxxxx [end of appendix]
Start pattern	[appendix: error log]
End pattern	**End of document**
After cleansing	SQL Server is down and cannot be restarted.

- Example of the **ExtractFromTemplate** action:

Example configuration	Brief description of the problem: ([^]*)FirstName:([^]*)LastName:([^]*)Phone:([^]*)
Data before cleansing	**Brief description of the problem**: The user called because he could not access to eDocs. The user was able to find the eDocs administrator but that person does not work for the company anymore First Name : Herr Maximo Christian Last Name : Graf Phone : 01 234 567
Data after cleansing	The user called because he could not access to eDocs. The user was able to find the eDocs administrator but that person does not work for the company anymore Herr Maximo Christian Graf

	01 234 567

Note: Regular expression is supported only for the **ExtractFromTemplate** action.

5. Select the **Match Case** check box if you only want to find the texts that match the case of the text or pattern that you entered.

6. Select the **Active** check box to activate this configuration.

7. Click **Add**. The new data cleansing configuration is now added.

Configure Smart Ticket

User Role: Administrator

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

- Standard category field

- Service category field

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 Smart Ticket task

In the out-of-box system, two Smart Ticket configuration tasks ("Standard category field" and "Service category field") are used for Smart Ticket by default. You can choose to use these out-of-box Smart Ticket tasks, or you can create new Smart Ticket tasks.

To add a new Smart Ticket task, 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: You can also select one of the out-of-box templates ("Category" or "Affected Service")

> from the drop-down list, and then click **Add** to create a new Smart Ticket task based on the template.

3. Type the task name for the new Smart Ticket configuration.

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 `category~="service catalog"`, which means the data that is not in the "service catalog" category can be selected as the training samples.

7. Select the target fields to be automatically filled by SM Smart Analytics. You can select up to three levels. For example, Category, Subcategory, and Area.

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 91.

Setting	**Description**
Training Samples Per Category	The maximum records to be used as the training samples for each category. Default: 200
Test Data Coverage	The percentage of records out of the total source data that are used to test the trained system. Default: 5
Source Data Coverage	The percentage of records out of the total source data that are used to train the system. Default: 90
Training Method	○ Choose "use best terms" for a faster training process if you have huge data volume.

Setting	Description
	◦ Choose "use training documents" for a higher accuracy with a slower training process. Default: use training documents
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 removed when the system removes the low weight training documents.

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

11. Modify the Smart Ticket form (idol.quick.new.interaction) to use the new Smart Ticket task that you just created.

    Note: This step is only required for operators to create Smart Interaction from index.do. The new auto-classification task will take effect directly on the user requests from SRC and ESS after a training is performed.

Perform training and testing

To perform a training for a Smart Ticket task, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Click the 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 91.

Tip: If you disable or enable the Multi-Company mode for Service Manager, you need to delete the existing Smart Ticket configuration tasks and re-create them before you perform training.

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 record 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 record is from the San Diego office, the record 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 **Rule Base** tab.
4. In the **Rule Field Name** field, specify the field name based on which you define the rule.
5. Click **Apply Rule**, and then click **Search**. A list containing all the categories appears, where you can choose the target category and set the value for the rule that you want to apply.
6. Click a category.
7. In the **Rule Field Value** field, set the value for the rule that you want to apply.
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 task 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 a Smart Ticket configuration, 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 from this configuration.

> **Tip:** If you are unable to see the **Multiple Company** tab, see the related topic in "Troubleshooting: Smart Analytics setup" on page 114.

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. Select and open a Hot Topic Analytics configuration record from the configuration list. For example, Incident.

   > **Note:** In the out-of-box system, three Hot Topic Analytics configuration records are provided (for the Interaction, Problem, and Incident modules). If you want to add a new Hot Topic Analytics configuration for another module, select a file from the **Add Configuration** drop-down list, and then click **Add**. For more information, refer to "Enable Hot Topic Analytics for other modules" on page 103.

3. 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 an individual record in Hot Topic Analytics. The title field is also an important data source for hot topic hunting.

   - **Contents Fields**: Select the data source for Hot Topic Analytics. Be sure to only use text fields such as description and solution.

4. 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 a filter.

5. From the **Advanced** tab, modify the following settings as needed:

   - **Expiry Day**: Hot Topic Analytics removes the data that was indexed earlier than the setting in this field from its analysis.

   - **Max Return Results**: Define the maximum number of records returned from Hot Topic Analytics.

   - **Group By**: Specify the field that is used to group the records as the last level in the hot topic map.

- **Analytics Action**: Specify the query condition for the analytics action.

  > **Note:** In the out-of-box system, the **Analytics Action** setting is only available in the Hot Topic Analytics configuration record for incidents with the following three action queries: Set Parent, Create Problem, and Create Change/Article. If you want to add more custom action queries in the **Analytics Action** section, see "Add more "Analytics Action" queries in the Hot Topic Analytics for Incidents" on page 107

6. Click **Save** to save your modification.
7. Click the **Start Index** button to start indexing.

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

Configure Smart Search

User Role: Administrator

To configure Smart Search, follow these steps:

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

   The **Smart Search Configuration** page opens.

2. From the **Add Knowledgebase** section, modify the following settings as needed:
   - **Knowledgebase name**: Specifies the name of the library you want to add.
   - **Knowledgebase type**: Specifies the type of the library you want to add. For detailed information about different types of knowledgebase, see "Managing Smart Search Knowledgebases" on page 48.
   - **Add**: Adds the library you specified as a new knowledgebase.
3. From the **Environment Configuration** section, modify the following settings as needed:
   - **Expiry days**: Smart Search removes the data that was indexed longer than the setting in this field from search.

- **Assign the default knowledge view group to all operators**: If this option is selected, the default knowledge view group is assigned to all operators.

- **Connector configuration**: Click to configure and monitor the status of the connectors and servers. For detailed information, see "Configure and monitor connectors" on the next page.

4. From the **Current Knowledgebase List** section, you can check the following information.

Field	Description
Knowledgebase Name	Specifies the name of the Smart Search knowledgebase. **Note:** When the administrator adds a new library, users can only see this library available on the list after next login.
Type	Specifies the type of the Smart Search knowledgebase.
Display Name	Specifies the display name for the Smart Search knowledgebase. You can change this value from a knowledgebase details page.
Interval	Displays the current interval used to update the selected knowledgebase index. Each interval unit is 5 minutes (default). You can change this value from a knowledgebase details page.
Index Status	Displays the current index status of the library. A library has the following four index status: ○ Offline: the library is newly added or the Smart Search server is shut down. ○ Not started: the **Full Reindex** button is clicked for the library and the indexing is in the queue. ○ Indexing: the indexing for the library is ongoing. ○ Finished: the indexing for the library is finished.
Doc count	Displays the number of records in the library. The number of the records is affected by the replica settings. When a content server is disabled, the number may be incorrect before you redistribute the server data.
Last Index time	Displays the time when the libary is last indexed.
Full Reindex:	When selected, the search engine performs a full re-index of a knowledgebase. If the index does not exist, it will be created. If it does exist, it will be deleted and re-created. A full re-index will remove all changes for this knowledgebase from the change cache since they will no longer be relevant.

Field	Description
Refresh Status	When selected, the search engine refreshes the status of the library to show how many documents are indexed and searchable at that time in the process.

- **Full Reindex**: When you click the **Full Reindex** button, the IDOL search engine performs a full re-index of the selected library. However, because indexing runs as a background process, the search engine does not begin indexing until the specified refresh interval is reached. Performing a full re-index on a large knowledgebase may have a significant impact on system resources.

- **Refresh Status**: Refreshes the index status of the knowledgebases.

5. When you first install the IDOL search engine after having used the Solr search engine, you will need to re-index all of your knowledgebases, as the old indexes will not work. Once the new index has been created, you can re-index all of your knowledgebases. Read about the indexing process in "Indexing the Knowledgebases" on page 1, and also see "Perform a Full Re-Index on a Knowledgebase" on page 1.

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

Configure and monitor connectors

User Role: Administrator

To enable search actions among different data sources, you need to configure different connectors and servers, and monitor their working status. You can get the URL information from the respective .cfg file of the connectors after you have configured them on your servers.

To configure and monitor connectors and servers, follow these steps:

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

2. Click the **Connector Configuration and Monitor** link to open the configuration page.

3. From the **CFS Server** tab, a list of all CFS server URLs is provided. You can click the **Refresh Status** button to refresh the URL list. Connectors need CFS servers to transfer data, so after you add a new connector, the corresponding CFS server information is added to this list.

> **Note:** If there two or more connectors that are installed on the same machine and share one CFS server, there is no new URLs added to the list.

4. From the **SharePoint Connector** tab, a list of all connector URLs and their status is provided. You can perform the following actions:

    - **Add a SharePoint connector**: Type a configured SharePoint connector URL here. You can click **Test connection** to test the URL connection status, and click **Add** to add this URL to the current list. To get the URL information for the SharePoint connector you have configured, check the following configuration file:

      <Smart Analytics Installation>/SharepointRemoteConnector/SharepointRemoteConnector.cfg

    - **sAMAccountName Field**: Choose the field type from the drop-down list. This field is the mapping field of SharePoint and SM users.

        - If SharePoint on premise is used, configure this field to the domain account field of the SM operator table.

        - If SharePoint Online is used only, there is no need to set this field as operator email field is used for user mapping.

    - **Delete**: Select a SharePoint connector URL and then click this button to delete it from the list.

    - **Refresh Status**: Click to refresh the status of the URL list.

5. From the **OMNI Group Server** tab, a Repository list of all OMNI group servers is provided. OMNI Group Server provides the LDAP configuration information which may be required for SharePoint login. You can also check the target task of a repository and its working status. You can click the **Refresh Status** button to refresh the URL list.

6. From the **HTTP Connector** tab, a list of all connector URLs and their status is provided. You can perform the following actions:

    - **Add an HTTP connector**: Type a new HTTP connector URL here. You can click **Test connection** to test the URL connection status, and click **Add** to add this URL to the current list. To get the URL information for the HTTP connector you have configured, check the following configuration file:

      <Smart Analytics Installation>/HTTPConnector/httpconnector.cfg

- **Delete**: Select an HTTP connector URL, and then click this button to delete it from the list.
- **Refresh Status**: Click to refresh the status of the URL list.

7. From the **File System Connector** tab, a list of all connector URLs and their status is provided. You can perform the following actions:

   - **Add a File system connector**: Type a new file system connector URL here. You can click **Test connection** to test the URL connection status, and click **Add** to add this URL to the current list. To get the URL information for the HTTP connector you have configured, check the following configuration file:

     <Smart Analytics Installation>/FileSystemConnector/filesystemconnector.cfg

   - **Delete**: Select a file system connector URL and then click this button to delete it from the list.
   - **Refresh Status**: Click to refresh the status of the URL list.

   > **Note:** When the fileserver connectors (including CFS server) and the fileserver share folders are on the same machine, Service Manager supports the UNC path (DirectoryPathCSVs=\\path\to\shared\folder) by using the IE browser.

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

Configure an HTTP connector

User Role: Administrator

After you install a connector, you must configure the parameters for this connector from the corresponding .cfg file before you start the service. In this example, the parameters for an HTTP connector is configured from the *<Smart Analytics Installation>*/HTTPConnector/httpconnector.cfg file.

The following table describes the parameters of the `[MYSITE]` section in the httpconnector.cfg file. If you want to configure multiple tasks for one connector, you just need to copy the content in the `[MYSITE]` section and rename the section.

> **Note:** Remember to restart the service of this HTTP connector after you configure and save the parameters.

Parameter	Description
`URL=http://MYSITE.COM`	Use this parameter to specify the root URL of the website for web crawling.
`DIRECTORY=MYSITE`	Specify the file location to save the crawling pages.
`CantHaveCSVs=*.css,*.js`	Specify the file types which are excluded from search resources. In this example, the .css and .js files are excluded.
`CantHaveCheck=1`	Specify that the value specified in the `CantHaveCSVs` parameter must be excluded from the URL.
`//StayOnSite=False`	The web crawling does not stay on the current site and will follow the links that leave the current page.
`//Depth=99`	Specify the maximum depth to which the connector can follow links during web crawling. In this example, this parameter is commented, which means it uses the default value (3).
`//ProxyHost=PROXY.COM`	Specify the proxy URL.
`//ProxyPort=80`	Specify the proxy port.
`//FOLLOWROBOTPROTOCOL=FALSE`	Specify whether the HTTP connector follows the protocol of the website. Most websites have a robot protocol to claim which page can be fetched by the spider. If you enable this parameter, the HTTP connector will not follow the protocol.
`//----Login with form----`	Uncomment the content under this section if you use a login form to log in to your websites.
`//LOGINMETHOD=FORMPOST`	Specify that the website requires you to enter information such as the user name and password, and the form uses the POST method to send this information to the site's server.
`//LOGINURL=https://login.com/`	Specify the login URL.
`//LOGINUSERFIELD=os_username`	Specify the ID of the field in which you enter your username. You can get the ID by viewing the source of the web page.
`//LOGINUSERVALUE=USERNAME@COMPANY.COM`	Specify the user name.
`//LOGINPASSFIELD=os_password`	Specify the ID of the field in which you enter your password.
`//LOGINPASSVALUE=PASSWORD_ENCRYPTED`	Specify your password.

Parameter	Description
`//LoginSubmitField=ButtonID`	Specify the ID of the button you click to log in to your website
`//----HTTP digest authentication----`	Uncomment the content under this section if you use an HTTP digest authentication to log in to your website.
`//DigestUsername=USERNAME`	Specify the user name for HTTP digest authentication.
`//DigestPassword=PASSWORD_ENCRYPTED`	Specify the password for HTTP digest authentication.
`//----NTLM authentication----`	Uncomment the content under this section if you use NTLM authentication to log in to your web page.
`//NTLMUsername=USERNAME`	Specify the user name for NTLM authentication.
`//NTLMPassword=PASSWORD`	Specify the password for NTLM authentication.

Managing Smart Search Knowledgebases

User Role: Administrator

You can add four types of Smart Search knowledgebases to Smart Analytics: an sclib knowledgebase, an fsyslib knowledgebase, a weblib knowledgebase, and an splib knowledgebase. An sclib knowledgebase is created from a table in Service Manager. For example, the out-of-the-box Incident_Library uses the probsummary table. A weblib knowledgebase is created by using web crawling to browse and index an external web site. The system creates an fsyslib knowledgebase when it crawls a file system. An splib knowledgebase is created to browse and index a SharePoint connector.

Add a new Smart Search knowledgebase

To add a new Smart Search knowledgebase, follow these steps:

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

   The **Smart Search Configuration** page opens.

2. From the **Add Knowledgebase** section, type a unique name for the new Smart Search knowledgebase in the Knowledgebase name field (required).

3. Select the knowledgebase type from the Type field drop-down list.

4. Click **Add**. The new IDOL knowledgebase record is added and a new knowledgebase maintenance page is displayed.
5. Configure the required knowledgebase information. The field availability varies for different knowledgebase types.

Field	Description
Display Name	Types a display name for the IDOL knowledgebase.
Refresh Interval	Displays the current interval used to update the selected knowledgebase index. Each interval unit is 5 minutes (default). You may increase the interval, which slows down time between updates, by increasing this number. Setting this number to 0 (zero) disables updates to the index. To re-start indexing, reset the interval to a value greater than zero.
Connector	Selects the specified connector from the configured connectors. This field is not required for an sclib type.
Table Name (only for sclib)	The table that will be indexed. A valid Service Manager table is required.
Skip These Extensions (only for sclib)	A semicolon-separated list of file extensions that should not be indexed or extracted. Certain file types either cannot be indexed, or provide no relevance. By providing these extensions, you can increase index performance. **Note:** Sample gif;jpg without any spaces.
Document ID Field (only for sclib)	Every table in Service Manager has a unique ID field and this field identifies the field name of the ID field. The indexer uses this field to uniquely identify each document in the index. This is a required field for indexing a knowledgebase.
Index Attachments (only for sclib)	If the table being indexed has attachments, select this check box to have the attachments indexed.
Table Query (only for sclib)	Specifies a Service Manager style query to limit what records in the table are indexed. For example, a query to return only documents that are neither draft nor retired in the kmdocument table: status ~= "draft" and status ~="retired". A blank query indicates that all records will be indexed.
Status	
Full Reindex:	When clicked, the search engine performs a full re-index of a knowledgebase. If the index does not exist, it will be created. If it does exist, it will be deleted

Field	Description
	and re-created. A full re-index will remove all changes for this knowledgebase from the change cache since they will no longer be relevant.
Refresh Statistics	When clicked, the search engine refreshes the statistics for this library.
Filed Definitions (only for sclib)	
Field Name	Specifies the field name in the Service Manager table to be included in the index.
Alias	Specifies the name that the field is to be indexed as. You can make use of the Alias field to have a single common field name for searching and for the hitlist. For example, you may wish to alias different fields from different tables as "Title" so that they can be searched by using Advanced Search. Fields can have more than one alias. Separate these fields with a semicolon. An alias can be the same name as the field name. If the alias name includes ".", the system converts the period to an underscore when indexed.
Type	Indicates whether the field is a plain text string, a rich text string, or a date type. The indexer ignores HTML markup in rich text strings and indexes plain text strings completely. Rich text: This value is for the legacy Solr search. Reference: some entity has the reference relationship. It applies the reference field to display the information that is meaningful to the user.
Hitlist	Defines what fields are available on the search hitlist. Fields marked as "true" in the hitlist column are available to be included on a search hitlist. The information for these field is displayed at the bottom of the search result.
Index weight	Defines the sequence of the search results which are displayed on the search hitlist. You can assign different index weight to adjust the display sequence. If the sort value of a field is assigned as level 4, the search results of this field is displayed at the top of the list. No index means that this field is not used for search. **Note:** HP recommends you to tune this field according to your own business use cases.
Match	By setting the field in this column to "true," the system indexes the field's content as an advanced search filter for Smart Search in this knowledgebase. The search engine searches this individual field with the Advanced Search filter. For example, if you set the Category field as true, this field is used as an advanced search filter. If you leave this value as empty, it applies the false

Field	Description
	value.
Sort	Defines the sequence of the search results which are displayed on the search hitlist. If you set multiple fields as hitlist, you can decide the display sequence by assigning different sort values for these fields. If the sort value of a field is assigned as 1, the search results of this field is displayed at the top of the list.
Data cleasing	Used to remove a field from the table before indexing.
Script	
Knowledgebase access script:	This script specifies the script the system uses to determine if a particular user has rights to access the knowledgebase. See the default script for detailed information.
Category index script:	This script processes the document category so that the indexer can translate the document's category into a string that the search engine can use later to find the document based on the user's category access.
Advanced Search script:	This script is used to build and return a string of library-specific query values that were entered by the user under the tabs in the Advanced Search screen. Tailor this script when a knowledgebase has a tab in the Advanced Search screen and you wish to modify the fields available for Advanced Search.
Default Locale	Specifies the default language used by the search engine when searching and indexing. By default, the language code is English.

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

Modify a current Smart Search knowledgebase

To modify a current Smart Search knowledgebase, follow these steps:

1. Click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. The **Smart Search Configuration** page opens. The current knowledgebase list is displayed on the **Smart Search Configuration** page.

2. Click a Smart Search knowledgebase to open the knowledgebase maintenance page.

3. Configure the required knowledgebase information. The field availability varies for different knowledgebase types.

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

Customize context-aware search

User Role: Administrator

Context-aware search enables users to view records and search results in the same window. User can copy a solution from the search results to the working record or trigger automated tasks. To enable the context-aware search icon inside a record, you can add the 9527 display option to a specific display screen.

Service Manager provides out-of-box pre-defined filters and actions for different libraries. The information of pre-defined filters and actions is saved in the smartsearchpreconditions and smartsearchaction tables. To perform Smart Search for a record, you can customize the Smart Search pre-defined filters to narrow down the library scope, and you can customize the Smart Search actions to pre-define the possible actions based on your search conditions and results.

Customize Smart Search pre-defined filters

To customize Smart Search pre-defined filters, follow these steps:

1. Click **Smart Analytics** > **Smart Search** > **More** > **Predefined Filters**.

   The **Smart Search Predefined Filters** page opens.

2. Click **Search** to open all the available pre-defined filter records.

3. Double-click a record to view or change it. Service Manager displays each record in its appropriate form.

4. Update any field within the record.

5. If you make changes, click **Save**.

Note: Make sure that the filename record is already defined as a Knowledge Management Mapping Record. Otherwise, you must define the file name from **Knowledge Management** > **Configuration** > **Integration Mapping**.

Customize Smart Search actions

To customize Smart Search actions, follow these steps:

1. Click **Smart Analytics** > **Smart Search** > **More** > **Smart Search Action**.

   The **Smart Search Predefined Filters** page opens.

2. Click **Search** to open all the available action records.
3. Double-click a record to view or change it. Service Manager displays each record in its appropriate form.
4. Update any field within the record.

   > **Note:** The integration with Operations Orchestration Flow in context-aware search is supported in Incident only.

5. If you make changes, click **Save**.

Modify Stop Words for IDOL search engine

User role: System Administrator

A stop-word list is a list of terms that can be ignored when the search engine is searching or indexing. Typically, stop-word lists include short and common words or prepositions, such as "a," "the," or "with" in English. However, they may also include longer words, such as long number strings, or words that are too common to be useful as search targets, such as the term "internet." Stop words are removed from words entered in the "Search for" box unless they are enclosed in double quotes (phrase search). They are not removed during indexing to allow for phrase searching.

Smart Search applies both the Smart Analytics stop words and the Service Manager stop words. However, some stop words used in Service Manager conflict with the stop words logic used in Smart Search. For example, "before" is a stop word defined in Service Manager, which means that "before" in a search string is ignored. However, in Smart Search, it supports the search string as "A BEFORE B", which means that Smart Search returns the results in which A comes before B. If "before" is not removed from the Service Manager stop words list, the returned results are not as expected. To avoid this problem, when you enable Smart Analytics, some of the English stop words used by the Solr search engine are removed. Here is a list of the removed stop words.

If you want to keep all the Service Manager stop words when you upgrade your Smart Analytics server, back up the stop words list before upgrade and import it after the

When you search by the IDOL search engine:

- If the search word is a stop word defined in the Solr search engine, no result is returned.
- If the search word is a stop word defined in IDOL search engine only, a warning message is displayed.

Stop words are stored in Service Manager in lists by specific language. Not all languages support stop words (for example, Japanese and Chinese). Adjust the list of stop words by either adding or removing words from this list.

The stop-word list for your log-in language is used by default, and is loaded once when you first log in. Changing the query language parameter on the advanced search screen changes the stop-word list used. The new stop-word list is loaded each time you search in a language other than your log-in language. This may cause a delay in your search being submitted as the stop-word list is loaded. If you need to perform extensive searches in a language other than your log-in language, HP recommends that you log out and then log back in with the other language to reduce this delay.

To modify Service Manager stop words:

1. Click **Smart Analytics** > **Smart Search** > **More** > **Stop Words**.
2. Click **Search**.
3. Select the record for the language code you wish to change.
4. Add a new word or modify an existing word.
5. Click **Save**.

To modify Smart Analytics stop words:

1. Open the *<Smart Analytics Installation>*/lanfiles folder.

   The stop words lists are saved as the <language name>.dat file in this folder.
2. Open the language file that you wish to change.
3. Add a new word or modify an existing word.
4. Click **Save**.

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 their operator records. The operators with this capability word can see Smart Analytics menus and use these features.

> **Note:** ESS self-service users are able to submit Smart Request records 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 TSL/SSL for two-way authentication

User Role: Administrator

TLS/SSL creates encrypted connections that allow private and sensitive information to be transmitted without the risk of eavesdropping, data tampering, or message forgery. HP recommends setting up a TLS/SSL connection between Service Manager and Smart Analytics, Connector Framework Server (CFS), or connectors. To do this, see the following steps for different scenarios.

For details about how to create two-way authentication certificates, see How to setup SingleSignOn (SSO) in a Horizontally scaled environment.

Configure TSL/SSL for two-way authentication between Service Manager and Smart Analytics

To Configure TSL/SSL for two-way authentication between Service Manager and Smart Analytics, follow these steps as an example:

1. Create a signed Service Manager server certificate and Smart Analytics certificate using the OpenSSL toolkit as a private certificate authority.

   ```
   CA Certificate keystore file: cacerts

   CA Certificate keystore password: "changeit"

   CA Certificate file: mycacert.pem

   SM Server keystore file: server.keystore
   ```

```
SM Server serverkeystore password: "serverkeystore"

Client public certificate file: clientpubkey.cert

Client certificate private key file: exported_rsa.key

Trusted clients keystore file: trustedclients.keystore (Import Client public
certificate into Trustedclients keystore)

Trusted clients keystore password: "trustedclients"
```

2. Configure the Service Manager server to use the server certificate and to trust the client certificate.

   a. Copy the following files to server host and put them under the RUN directory:

      - certs\cacerts
      - certs\trustedclients.keystore
      - key\server.keystore

   b. Set the following parameter values in the `sm.ini` file.

Parameter	Value
ssl	1
sslConnector	1
ssl_reqClientAuth	2
trustedsignon	1
keystoreFile	server.keystore
keystorePass	serverkeystore
ssl_trustedClientsJKS	trustedclients.keystore
ssl_trustedClientsPwd	trustedclients
truststoreFile	cacerts
truststorePass	changeit

3. Configure the Smart Analytics components to use the client certificate and to trust the server

certificate.

a. Copy the following files to the <*Smart Analytics Installation*>\ssl Certificate folder on your Smart Analytics local machine:

   - certs\clientpubkey.cert
   - certs\ mycacert.pem
   - exported_rsa.key

b. Configure all content components to use the certificates by setting the content.cfg file.

   ```
   [SSLOption1]

   SSLMethod=SSLV23

   SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

   SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

   SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

   [IndexServer]

   SSLConfig=SSLOption1

   [Server]

   SSLConfig=SSLOption1
   ```

c. Configure all content components to use the certificates by setting the content.cfg file.

   ```
   [SSLOption1]

   SSLMethod=SSLV23

   SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

   SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

   SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem
   ```

```
[IndexServer]

SSLConfig=SSLOption1

[Server]

SSLConfig=SSLOption1

SSLIDOLComponents=TRUE

[IDOLServerN]

SSLConfig=SSLOption1
```

d. Configure the Smart Analytics main server to use the certificates by setting the autonomyIDOLServer.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics
Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[IndexServer]

SSLConfig=SSLOption1

[DataDRE]

SSLConfig=SSLOption1

[CatDRE]

SSLConfig=SSLOption1

[AgentDRE]

SSLConfig=SSLOption1
```

```
[Server]

SSLConfig=SSLOption1

SSLIDOLComponents=TRUE

[IDOLServerN]

SSLConfig=SSLOption1

[Agent]

SSLConfig=SSLOption1
```

e. Change the <*Smart Analytics Installation*>\IDOL\agentstore.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[IndexServer]

SSLConfig=SSLOption1

[Server]

SSLConfig=SSLOption1

SSLIDOLComponents=true
```

4. Configure the CFS to index into IDOL which is configured with SSL.

   a. Configure Smart Analytics main server to use the certificates by setting the autonomyIDOLServer.cfg file.

```
[SSLOption1]
```

```
SSLMethod=SSLV23

SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[IndexServer]

SSLConfig=SSLOption1

[DataDRE]

SSLConfig=SSLOption1

[CatDRE]

SSLConfig=SSLOption1

[AgentDRE]

SSLConfig=SSLOption1

[Server]

SSLConfig=SSLOption1

SSLIDOLComponents=TRUE

[IDOLServerN]

SSLConfig=SSLOption1

[Agent]

SSLConfig=SSLOption1
```

b. Configure Smart Analytics main server to use the certificates by setting the autonomyIDOLServer.cfg file.

```
[SSLOption1]
```

```
SSLMethod=SSLV23

SSLCertificate=<Smart Analytics
Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[Indexing]

IndexerSections=IdolServer

IndexBatchSize=1000

IndexTimeInterval=60

[IDOLServerN]

Host=idolserver

Port=20010

DefaultDatabaseName=News

//need to configure if idol index port is ssl encrypted

SSLConfig=SSLOption1
```

5. Restart the Service Manager server.

Configure TSL/SSL for two-way authentication between Service Manager and CFS/connectors

To Configure TSL/SSL for two-way authentication between Service Manager and CFS/connectors, follow these steps as an example:

1. Create a signed Service Manager server certificate and Connector Framework Server (CFS) or connectors certificate using the OpenSSL toolkit as a private certificate authority.

   ```
   CA Certificate keystore file: cacerts

   CA Certificate keystore password: "changeit"

   CA Certificate file: mycacert.pem
   ```

```
SM Server keystore file: server.keystore

SM Server serverkeystore password: "serverkeystore"

Client public certificate file: clientpubkey.cert

Client certificate private key file: exported_rsa.key

Trusted clients keystore file: trustedclients.keystore (Import Client public
certificate into Trustedclients keystore)

Trusted clients keystore password: "trustedclients"
```

2. Configure the Service Manager server to use the server certificate and to trust the client certificate.

   a. Copy the following files to server host and put them under the RUN directory:

      - certs\cacerts
      - certs\trustedclients.keystore
      - key\server.keystore

   b. Set the following parameter values in the `sm.ini` file.

Parameter	Value
`ssl`	`1`
`sslConnector`	`1`
`ssl_reqClientAuth`	`2`
`trustedsignon`	`1`
`keystoreFile`	`server.keystore`
`keystorePass`	`serverkeystore`
`ssl_trustedClientsJKS`	`trustedclients.keystore`
`ssl_trustedClientsPwd`	`trustedclients`
`truststoreFile`	`cacerts`
`truststorePass`	`changeit`

3. Configure the Smart Analytics Connector Framework Server (CFS) or connectors to use the client certificate and to trust the server certificate.

   a. Copy the following files to the <*Smart Analytics Installation*>\ssl Certificate folder on your Smart Analytics local machine:

      - certs\clientpubkey.cert
      - certs\ mycacert.pem
      - exported_rsa.key

   b. Configure the Connector Framework Server (CFS) to use the certificates by setting the CFS.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics
Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

//Use this parameter to specify the path to a directory containing multiple
CA certificates in PEM format to check against. Each file must contain one
CA certificate.

//SSLCACertificatesPath=C:\Autonomy\HTTPConnector\CACERTS\

[Server]

//to make CFS ACI port ssl encrypted.

SSLConfig=SSLOption1
```

   c. Configure the connectors to use the certificates by setting the <*connector*>.cfg file.

```
[Ingestion]
```

```
    //If CFS ACI port is ssl encrypted

    IngestSSLConfig=SSLOption1
```

4. Restart the Service Manager server.

Use Smart Analytics Assistant

User Role: Administrator

Smart Analytics Assistant is a build-in tool that enable administrators to interactively perform IDOL administrative actions in Smart Analytics. For example, you can use this tool for content server maintenance, system status checking, and troubleshooting.

In the interface, there is a command line to enable the administrator to send IDOL actions to IDOL components. The most frequently used actions have been included in the drop-down list. You can get more actions and information from IDOL reference guides.

Service Manager provides five blocks to fulfill different functionality. For each component in all blocks, you can click the underlined name to get detail status.

Block	**Description**
Main Proxy	Top level proxy status that shows component name, host, port, and status. If any component is down, you need further investigation.
Smart Ticket and Hot Topic content	By default, one content store is used for Smart Ticket and Hot Topic Analytics. It must always be online. If you need more content store to host more databases, you can click the “Add” link. The content store to be added to the system has to be installed and running in another machine.
Smart Search Proxy	The second level proxy that is dedicated to Smart Search. Only DAH and DIH are included in this proxy.
Smart Search Content	By default, two content stores are used for Smart Search. You can add more content stores by clicking the “Add” link. The content store to be added to the system has to be installed and running in another machine.
Image Server	By default, one image server is installed for OCR purpose. If you want to improve performance, you can add more image servers. The content store to be added to the system has to be installed and running in another machine.

To use Smart Analytics Assistant, follow these steps:

1. Type `saa` in the command line, and then press Enter. The Smart Analytics Assistant interface is launched.

2. Select one of the actions for Smart Analytics from the drop-down list, or typing an action.

   > **Note:** Replace *<Host>*, *<port>*, *<variable_value>* in the following action examples with the corresponding values that you can find from the corresponding status blocks.

   - **Backup Component**

     Creates a backup that can be used to restore the component's state. You can use this action for the Content, Category, Agent and Community components, but you must send the action to the component ACI port, rather than to the IDOL Proxy port. The backup file is stored in the path that you specified.

     For example, to backup category,

     ```
     http://<Host>:<CategoryPort>/action=BackupServer&path=c:\backup_
     category
     ```

     > **Note:** By default, the Smart Analytics server CategoryPort is 9020.

   - **Backup Database**

     Exports all the index documents of a database from the Smart Analytics content server to a series of compressed files in the defined backup directory. This action is suitable to backup an individual database. If you want to backup all databases in a content server, use the action Backup Component as mentioned above.

     Action example:

     ```
     http://<Host>:<indexPort>/DREEXPORTIDX?filename=c:/BackupFolderName
     /FilePrefix&DatabaseMatch=<Database_name>&HostDetails=true
     ```

     > **Note:** In this example, the filename is a combination of path and basic file name. Please make sure you specify `parameter DatabaseMatch=DatabaseName`.

   - **Restore Component or Category step 1**

Imports backup files of component that was backed up by using the action Backup Component. It could be Content, Category, and Community component. For the Category component, you need an extra step to synchronize it.

Action example:

```
http://<Host>:<CategoryPort>/action=RestoreServer&filename=c:\backu
p_category\***.zip
```

- **Restore Category step 2 - Synchronize**

  After restore category component, you need to synchronize and build the category.

  Action example:

  ```
  http://<Host>:<MainProxyACIPort>/action=CategorySyncCatDRE
  ```

  > **Note:** By default, the port number is 9000.

- **Restore Database**

  Restores the index IDX exported before. If no DREDbName is specified, use the dbname of the indexed file.

  Action example:

  ```
  http://<MainProxyHost>:<IndexPort>/DREADD?c:\\path\to\<xxx.idx>&DRE
  DbName=<variable_value>&CreateDatabase=True
  ```

  > **Note:** By default, the port number is 9001.

- **View Index Status**

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

  Action:

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

- **View Action History**

Displays 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.

Action example:

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

- **View Root Category Detail**

  Displays the root categories after training.

  Action example:

  ```
  http://<Host>:<port>/action=CategoryGetHierDetails
  ```

- **View Status**

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

  Action example:

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

  > **Note:** If any component is offline, check the corresponding log file and fix it to bring it online. During indexing, the DIH periodically checks whether all the connected content servers are available. If a content is unavailable, the DIH queues the data that this content server normally receives, and when the content server starts operating again, the DIH indexes the queued data into it.

- **Show Smart Search content server status**

  Displays the status of the Smart Search content server.

  Action example:

  ```
  http://SmartSearchProxyHost:DIHPort(20080)
  /action=EngineManagement&EngineAction=showstatus
  ```

- **Add Smart Search Content servers dynamically**

  To add a Smart Search content server dynamically, follow these steps:

i. Run the following action:

```
http://SmartSearchProxyHost:DIHPort(20080)
/action=EngineManagement&EngineAction=Add&Host=ContentServerHos
t&Port=ContentServerPort&weight=1
```

ii. Run the following action:

```
http://SmartSearchProxyHost:DAHPort(20070)
/action=EngineManagement&EngineAction=EngineAdd&EngineHost=Cont
entServerHost&EnginePort=ContentServerPort
```

iii. Repeat previous steps until all content servers are added.

iv. Click the **Redistribute** link in **saa** to redistribute data among all Smart Search Content servers after you add the new content servers.

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

Add a new content server

User Role: Administrator

As an initial setting, HP deployed one content server at main level, and two content servers at Smart Search level. If you need add more content server(s) to process more data, follow these steps.

- **Add a content server for Smart Ticket and Hot Topic Analytics**

  You may need to add content server(s) if the data size is huge for Smart Ticket and Hot Topic Analytics, it is suggested to store no more than 3 million records for each content server

  To add a content server for Smart Ticket and Hot Topic Analytics, follow these steps:

  a. Install a content server by using Smart Analytics installer. For details about installing a content server, see "Install Smart Analytics servers on Windows" on page 12.

  b. After you start the new content server, add it to Smart Analytics main server by editing the <*Smart Analytics Installation*>/IDOL/AutonomyIDOLServer.cfg file as the followings:

  i. Increase the value of **Number** by 1 in the **DistributionIDOLServers** section:

```
[DistributionIDOLServers]
```

```
Number=3
```

ii. Add a new section of **[IDOLServer*N*]**, where N should be replaced by the number of your server:

```
[IDOLServerN]

Name=ContentN

Host=ContentHostAddress

Port=ContentPort

DistributeByFieldsValues=CONTENTN
```

c. Restart the **HP SM Smart Analytics Main Server** service.

- **Add a content server for Smart Search**

  If the default or existing smart search content servers are not enough for the indexed data, you may need to add additional content server(s).

  To add a content server for Smart Search, follow these steps:

  a. Install a content server by using Smart Analytics installer. For details about installing a content server, see "Install Smart Analytics servers on Windows" on page 12.

  > **Note:** Make sure the content server configured the Service Manager server and Smart Search proxy server as its client. These configuration are set in content's configuration file.
  >
  > Make sure Smart Search proxy also configured the new content server as its client (in the level2proxy\AutonomyIDOLServer.cfg file)
  >
  > The following are configuration items about clients:
  >
  > ```
  > [Service]
  >
  > ServiceStatusClients=127.0.0.1, SmarSearchProxyAddress,
  > SMServerAddress,123.45.67.*
  >
  > ServiceControlClients=127.0.0.1, SmarSearchProxyAddress,
  > SMServerAddress,123.45.67.*
  > ```

```
[Server]

QueryClients=127.0.0.1, SmarSearchProxyAddress,
SMServerAddress,123.45.67.*

AdminClients=127.0.0.1, SmarSearchProxyAddress,
SMServerAddress,123.45.67.*

IndexClients=127.0.0.1, SmarSearchProxyAddress,
SMServerAddress,123.45.67.*
```

b. Make sure the Smart Search proxy server has configured the new content servers as its clients. You need to configure the IPv4 and IPv6 addresses for the new content serverin the level2proxy\AutonomyIDOLServer.cfg file for the following items.

- ServiceStatusClients
- ServiceControlClients
- QueryClients
- AdminClients
- IndexClients

You may need to restart the Smart Search proxy server after you update the configuration file.

c. After you start a new content server, go to the Smart Analytics Assistant page to add it to the Smart Search Content by clicking the **Add** link in the **Smart Search Content** section. For details about using Smart Analytics Assistant, see "Use Smart Analytics Assistant" on page 64.

d. Repeat the above steps if you want to add more content servers.

e. Click the **Redistribute** link to balance data distribution. This step is **mandatory** to mark the new content server active.

> **Note:** HP recommends that you back up your existing content servers before you run the Redistribute action. It may take a long time to redistribute your data among all Smart Search content servers.

Modify Smart Search contents and weight for data distribution

User Role: Administrator

Smart Search uses **consistent hashing** for distribution of data. In consistent hashing mode, you can add, remove, or change the weight of child servers in your DIH without having to reindex all your content.

In this mode, DIH distributes documents among a large, fixed number of virtual nodes (4096), and then assigns these nodes to one or more child servers. When you change the number or weight of the child servers, you can use the **DREREDISTRIBUTE** index action to redistribute the virtual nodes between the new set of servers without reindexing all the data.

In consistent hashing mode, all content is distributed in virtual nodes, which the DIH assigns to one or more child servers. When you run the **DREREDISTRIBUTE** index action, DIH checks whether the child server architecture has changed. If there is a change, DIH automatically exports and indexes the content in virtual nodes to redistribute your data evenly between the available child servers.

You can check current Smart Search contents and their ratio of data (including the information of data weight and vnode) by sending an action to the Smart Search proxy DIH server (20080 by default):

Action example:

```
http://<Smart Search Host>:<dih
port>/action=enginemanagement&engineaction=showstatus
```

To modify the Smart Search content servers and the weight for data distribution, use the **EngineMangement&EngineAction=Edit** action.

- Change the weight of data distribution.

  Action example:

  ```
  http://<Smart Search Host>:<dih
  port>/action=EngineManagement&EngineAction=Edit&ID=2&Weight=2
  ```

- Update only this content server (receives document updates but does not receive new documents):

  Action example:

  ```
  http://<Smart Search Host>:<dih
  port>/action=EngineManagement&EngineAction=Edit&ID=2&UpdateOnly=true
  ```

- Disable this content server (mark it as offline):

  > **Note:** When a child server is disabled, the DIH continues to assign documents to it, and queue up index actions, but it does not attempt to send them until the child server is enabled again.

  Action example:

  ```
  http://<Smart Search Host>:<dih
  port>/action=EngineManagement&EngineAction=Edit&ID=2&Disabled=true
  ```

Remove a content server for Smart Search

User Role: Administrator

To remove a content server for Smart Search, follow these steps:

1. Update the data weight of the content server that you want to remove to 0.

   Action example:

   ```
   http://<Smart Search Host>:<dih
   port>/action=EngineManagement&EngineAction=Edit&ID=2&Weight=0
   ```

2. Redistribute data among the remaining contents servers.

   Action example:

   ```
   http://<Smart Search Host>:<dih port>/DREREDISTRIBUTE
   ```

3. Remove the content server.

   Action example:

   ```
   action=EngineManagement&EngineAction=Remove&ID=2
   ```

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	Query
Idolcategorytest	true
Idolserverinfo	true
Number	name="cate2idolid" or name="cate2idoltestid" or name#"idol"
cate2idol2	true
counters	table.name#"idol"
idolDataFilter	true
idoladapter	true
idolindex	true
idolpbmhunter	true
idolsecgroup	true
idoltestresult	true
idoltestsample	true
idoltuning	true

2. Backup all contents, agent, community and category components. To do this, run the following actions in the SM Smart Analytics Assistant (SAA) utility:

```
http://<idolhost>:<ACIPort>/action=BackupServer&path=backup_dir
```

Tip: *<idolhost>* is the address of the Smart Analytics server. The default port numbers are:

- content0: 10010
- content1: 30010

- content2: 30020
- category: 9020
- community: 9030
- agent: 9050

Note: For how to use the SM SAA utility, see "Use Smart Analytics Assistant" on page 64.

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. Restore all components that you back up in step 2. To do this, run the following actions in the SM Smart Analytics Assistant (SAA) utility:

```
http://<idolhost>:<ACIPort>/action=RestoreServer&filename=c:\backupdir\subfolde
r
```

7. Synchronize category. To do this, run the following commands in the SM Smart Analytics Assistant (SAA) utility:

```
http://<idolhost>:<MainProxyPort>/action=CategorySyncCatDRE
```

   Now, the target Service Manager server works for Smart Search, Smart Ticket, and Hot Topic Analytics as the source Service Manager server does.

Back up indexed data

User Role: Administrator

To ensure that you always have current copies of the data that the IDOL Server stores, we recommends that you back up the IDOL Server in regular intervals. By default, scheduled data backup is not configured. If you want to enable it, you need to insert the following lines in the [schedule] section of the default configuration file for content store, modify it accordingly, and then restart the IDOL Server.

```
[Schedule]
Backup=true
BackupCheckIndexUpdates=TRUE
BackupCompression=true
BackupTime=00:00
BackupInterval=24
BackupMaintainStructure=true
BackupRetryAttempts=3
BackupRetryPause=5
NumberOfBackups=3
BackupDir0=E:\DataIndex_Backup0
BackupDir1=E:\DataIndex_Backup1
BackupDir2=E:\DataIndex_Backup2
```

For agent and category, you can manually run the backup action in SAA after each training.

Uninstall Smart Analytics

User Role: Administrator

If you want to uninstall Smart Analytics, follow the instructions in this section.

- Before you uninstall Smart Analytics, we recommend that you back up your index and category data if you want to restore it in the future. For backup and restore instructions, see *step 2* and *step 7* respectively in "Transfer Smart Analytics intelligence between systems" on page 72.
- Restart the system after you uninstall Smart Analytics. Otherwise, the services and files cannot be totally removed. Besides, the data and configurations remain after uninstall, and you must delete then manually for safety concerns.

Windows

To uninstall Service Manager Smart Analytics from Windows, follow these steps:

1. Go to **Control Panel** > **Programs** > **Uninstall a program**.
2. Select **HP SM 9.41 Smart Analytics**, and then click **Uninstall/Change**. The Unistall HP SM 9.41 Smart Analytics wizard is displayed.
3. Click **Next**.
4. If you want to completely remove Smart Analytics, select **Complete Uninstall**. If you want uninstall

specific Smart Analytics features, select **Uninstall Specific Features**.

> **Note:** If your Smart Analytics is upgraded from a former version, and there is an image server installed, you have to delete the files and service manually when you are uninstalling.

5. Click **Next**, and then follow the on-screen instructions to uninstall Smart Analytics.

Linux

To uninstall Service Manager Smart Analytics from Linux, follow these steps:

1. Go to the _uninstall folder under the Smart Analytics installation directory.
2. Type `./uninstaller -?` from the command line interface to view the uninstallation options and instructions.

   > **Note:** As the Maintenance Mode is not enabled in the SM Smart Analytics uninstaller, the parameters under the Maintenance Mode are not applicable.

3. Use the available commands, and then follow the on-screen instructions to uninstall Smart Analytics.

   For example, you can use `uninstaller -i console` to launch a command line based interactive uninstall process. If you log on to the system through X-Window, you can launch the graphical uninstaller by using the `uninstaller -i swing` command.

   You can specify the features that you want to uninstall, or you can uninstall Service Manager Smart Analytics completely.

Chapter 4: User tasks

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

Use Smart Search as a general search tool

Smart Search supports cross-module search from selectable sources inside and outside of Service Manager. It can also perform fuzzy search, and use advanced filters. Smart Search used as a general search tool is supported for self-service users, mobility users, and Service Request Catalog users.

Search capabilities

	Scenario	**Sample or explanation**

Input - search key words	None of these words	NOT email
	Any of these words	email OR access
	All of these words	Email AND ACCESS
	Location between these words	email BEFORE access email AFTER access email NEAR*N* access **Note:** This means that the term **access** is within *N* words from the term **email**. For example, **email NEAR1 access** returns the results in which the term **email** and the term **access** are adjacent.
	This exact phrase	"email access"
	Wildcard	*email*, email?
	Punctuation	\\, \?, *
	Free-text search/exact match search	Email/status = "true"
Output - Search accuracy	Configurable weight to determine the ranking of search result.	Relevance scores for matches in certain fields over matches in other less important fields
	Adaptive learning if use as solution	
	Configurable Predefined condition for suggested solution based on context-aware search	
Output - search list	Summary of search result plus the Customizable hitlist fields will be showed in search main page	

Search Utility	Fuzzy Search	Search Emal, return result for correct typing: Email
	Support language-specific word stemming	Search break, return broken and breaks as well
	Attachment search	Separately search attachment
	Global filter for all libraries	Last modify time, status, assignment, affected services
	Facet oriented search per library	Configurable, all of matched field can be treated as facet to narrow down the search result
	Store last search condition for next usage per user	
	Check all libraries in one click	
	Clear all conditions in one click	
	Show count per each value for search result.	
	Language detection	Auto detect language according to the search key words
	Allow index duplicated fields for different search purpose, "Multivalue=true"	

To use Smart Search, follow these steps:

1. Click the **Search** button on the top-right corner of the Service Manager UI. The Smart Search window opens.

2. Type the key words or phrases you want to search for. HP Service Manager displays a list of documents matching your search request when you are typing. If no result is displayed, type a new search string for your search or use Advanced Search to specify additional search criteria.

   > **Note:** You need to set up and verify the server connectivity for multiple servers and connectors. For detailed information to configure and monitor the connectors and servers, see "Configure and monitor connectors" on page 44.

3. Configure the following search conditions for your Smart Search.

Field	Description
Search within results	This option is only activated when there are results returned. Click this option button to add it as a filter to the filter panel on the right. You can click the remove button on the filter to remove it. For example, type **Service** in the search box and then click **Enter**. After the results are returned, you click this option and a filter of **Previous Search: Service** is added to the search results panel. Then type **Server** in the search box and then click **Enter**. The results are returned as the same as you search for **Service AND Server**.
General filter	Click the **Filter** button to cascade the general filter to filter the content by the last modified time. The option you selected is added to the filter panel on the right. You can click **Clear All** to remove all the filters.
Library	Specifies the knowledgebases for your search repository.
All	Click the check box to select all the knowledgebases as your search repository.
<Knowledgebase name>	Click the check box to include this knowledgebase to your search repository. **Note:** Your library options in smart search is remembered for your next login.

4. Click **Search**.

> **Note:** If you do not type any content in the search box, no result is returned when you click the **Search** button.

5. Click the document title or identifier to open it.

In the search results, if you click the button to vote up or vote down an article, this will affect the ranking of the search result next time. This is not configurable in this release. Also, if the document is re-used for a solution, the ranking for this document is also affected. For detailed information, see "Use adaptive learning in Smart Search" on the next page.

Actionable context aware search

At any time while you create or update an Interaction or Problem record or update an Incident record, you can perform a smart search to find solutions. When you find a solution, you can add the solution to the resolution or workaround field of the record you are processing.

- The context aware search is disabled from the self-service user view (ess.do).
- To remove the legacy search icon, you need to edit the form to remove the legacy icon manually.

To use Smart Search for a solution, follow these steps:

1. While you are submitting a record, click the quick search button to open the quick Smart Search window on the right panel. Smart search uses the content in the **Description** field of this record as the search string.
2. In the Smart Search results, click the hyperlink to view a solution document.
3. When there is a document with the correct solution or workaround, the **Use Solution** button appears, and you can click **Use Solution** to add the solution to the resolution or workaround field of the record.
4. After you select **Use Solution**, the system displays the record with the resolution or workaround field updated. You can continue processing the Interaction, Incident, or Problem record that prompted your quick Smart Search.

Use adaptive learning in Smart Search

Smart Search adaptive learning is enabled by default to collect words or specific phrases used to search a knowledgebase for those documents that are considered useful or can be performed with actions.

Smart Search maintains a count which specifies the number of times search words or phrases resulted in finding a useful document (whether marked as useful or used as a solution). Each time a user performs a search using the same words or phrases, the count is incremented or a new entry is created when the search returns useful results. Also, each time an operator clicks the **Use Solution** button, the phrase used by the operator to search for the solution is saved or the count is incremented for the phrase for the adaptive learning record associated with the solution.

Note: For a working copy of a document that has no published version, the system collects the words and phrases for adaptive learning. For a working copy of a document that already has a published version, the system does not collect the words and phrases for adaptive learning.

Example: If **monitor** or **blue monitor** is used in a document that resolves an incident and is used as a solution or performed with other actions, the phrase **blue monitor** or the word **monitor** is appended to the adaptive learning terms for that document and the count is incremented. For additional searches, a document with one **blue monitor** in it will come up with a reasonable relevancy. You can also change the count of **monitor** to 15, for example, to make this document appear higher on the search results list than another document with the word **monitor** in it.

At the same time when an operator clicks the **Use Solution** button, the system creates or increments the associated AuTNRANK value of this record. When an operator performs a search by using advanced search and then clicks the **Vote** button to mark a document as useful, the system also creates or increments the associated AuTNRANK value of this record as follows:

- When the search results are filtered by "Any of these words," the system adds separate entries for each word in the search phrase.
- When the search results are filtered by "All of these words" or "This exact phrase," the system creates a single entry for all the words in the search phrase.

The AuTNRANK value becomes a weighted value so that when another user performs a different search using the same words or phrase, documents containing the same words or phrase are returned higher on the hit list in the next set of search results.

Note: If you perform a full re-index of a knowledgebase, all the AuTNRANK values are removed from the library.

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 you to add attachments or comments to submit a request, which simplifies the process of submitting the ESS support requests.

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

1. Log on to Service Manager from the ESS portal.
2. Click **Submit a Smart Request**.
3. Click **Add Files** to attach an image file. For example, a screenshot of the error message.

> **Note:** For image files containing multiple languages, Service Manager provides a language list according to the language priorities. The following restrictions apply to the language list:
>
> - Arabic cannot be combined with any other alphabets or languages.
> - Hebrew cannot be combined with either Japanese, Simplified Chinese, or Traditional Chinese.

4. Type comments for your request.
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 the Mobility client, follow these steps:

1. Log on to Service Manager on your mobile device.
2. Click **Submit a Smart Request** on the main menu.
3. Add an attachment. For example, a screenshot of the error message.
4. Type comments for your request.
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 the power user view (index.do), follow these steps:

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

   The fields such as **Category** and **Affected Service** 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 with your record accordingly.

Use Hot Topic Analytics to create an incident, problem, or change

User Role: Incident Manager, Problem Manager, Change Manager

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

> **Note:** You must use the web client instead of the Windows client to view the dynamic topic map in Hot Topic Analytics.

To use Hot Topic Analytics to find incident, problem, or change candidates, follow these steps:

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

2. Do one of the followings to access Hot Topic Analytics for your module:

   - Click **Service Desk** > **Hot Topic Analytics**. On the Hot Topic Analytics for Interactions screen, you can analyze the interactions that are categorized for the suggested hot topics, and then create new incidents based on your selected interactions.

     > **Note:** If Process Designer and the streamlined interaction solution are enabled for the Service Desk module, we recommend that you remove the **Create Incident** action from the Hot Topic Analytics for Interactions screen to accommodate the streamlined interaction solution. For information on tailoring the actions, see "Customize actions in hot topic map" on page 105.

   - Click **Incident Management** > **Hot Topic Analytics**. On the Hot Topic Analytics for Incidents screen, you can analyze the incidents that are categorized for the suggested hot topics, and then create new problems or changes based on your selected incidents.

   - Click **Problem Management** > **Hot Topic Analytics**. On the Hot Topic Analytics for Problems screen, you can analyze the problems that are categorized for the suggested hot topics, and then create new changes based on your selected problems.

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

  > **Note:** In the out-of-box system, for the Hot Topic Analytics for incidents, the last level of the topic map is the affected service.

- The records that belong to a topic are displayed in the list on the right.

4. If you want to run a custom analysis, enter your keywords, and then click **Find Hot Topics**.
5. If you want to further refine the results, click **Advanced Filter**, specify your filters, and then click **Find Hot Topics** again. The graphic is refreshed with the filtered results.

   > **Tip:** If you want to build complex queries based on your specific needs, you can click **Edit Query** to use Query Editor to define your queries. When you define your queries, be sure to use only the fields that are specified in the **Properties Fields** section of the Hot Topic Analytics configuration. Otherwise, your queries will not take effect because the fields that you use are not included in the analysis of Hot Topic Analytics.

6. Review the filtered records that are listed to the right of the graphic to identify the candidates for escalation. You can click the record ID to view the record detail.
7. After you identify the candidates, select the check boxes before the record IDs, and then click the corresponding button (such as **Create Problem**). A form to create the new record is displayed, and some fields are populated based on the selected candidates.

   > **Note:** For the Hot Topic Analytics for Incidents, you need to select **Create Problem** or **Create Change/Article** from the **Analytics Action** drop-down list so that the **Create Problem** or **Create Change** button can be displayed when you select the candidates.

8. Update the form as needed, and then click **Save** to create the new record.

   When the new record is created, the selected candidates are listed in the **Related Records** section of the new record.

Use Hot Topic Analytics to create a KM article

User Role: Service Desk agents, Incident Manager, Problem Manager

You can create KM articles for interactions, incidents, or problems based on the hot topics automatically suggested by Hot Topic Analytics.

> **Note:** You must use the web client instead of the Windows client to view the dynamic topic map in Hot Topic Analytics.

To use Hot Topic Analytics to create a KM article, follow these steps:

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

2. Do one of the following to access Hot Topic Analytics:

   - Click **Service Desk** > **Hot Topic Analytics**.

   - Click **Incident Management** > **Hot Topic Analytics**.

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

   The Hot Topic Analytics for the specific module is displayed.

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 serves to identify the topic.

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

     > **Note:** In the out-of-box system, for the Hot Topic Analytics for incidents, the last level of the topic map is the affected service.

   - The records that belong to a topic are displayed in the list on the right.

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

5. If you want to further refine the results, click **Advanced Filters**, specify your filters, and then click **Find Hot Topics** again. The graphic is refreshed with the filtered results.

6. Review the categorized records as listed to the right of the graphic to identify the candidates for creating the new KM article. You can click the record ID to view the record detail.

7. After you identify the candidates, select the check boxes before the record IDs, and then click the **Create Article** button.

   > **Note:** For the Hot Topic Analytics for Incidents, make sure that you select **Create Change/Article** in the **Analytics Action** drop-down list so that the **Create Article** button can be displayed above the record list.

8. Select a document type. The New Knowledge Document form is displayed and the information in your selected records is copied to the new KM record.

9. Enter information in the mandatory fields (such as **Title**) and other optional fields if necessary.

10. Click **Submit**. The new KM record is created.

Use Hot Topic Analytics to set incident parent

User Role: Incident Analyst

By using Hot Topic Analytics, you can easily identify similar incidents, and then group them by setting the parent incident.

To use Hot Topic Analytics to set the incident parent, follow these steps:

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

   > **Note:** You must use the web client instead of the Windows client to view the dynamic topic map in Hot Topic Analytics.

2. Click **Incident Management** > **Hot Topic Analytics**. The Hot Topic Analytics for Incidents screen is displayed.

3. From the **Analytics Action** drop-down list, select **Set Parent**. The hot topic map is refreshed.

   > **Note:** In the out-of-box system, only the incidents that have not been set as the parent or child incidents are included in the hot topic analysis. The administrator can set particular

> queries for different actions in **Analytics Action** from the **Advanced** tab in the Hot Topic Analytics configuration. For more information, see "Configure Hot Topic Analytics" on page 40.

4. 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 serves to identify the topic.
    - You can click a hot topic to drill down to the sub-topics.
    - The records that belong to a topic are displayed in the list on the right. You can click the record ID to view the record detail.
5. If you want to run a custom analysis, enter your keywords, and then click **Find Hot Topics**.
6. If you want to further refine the results, click **Advanced Filters**, specify your filters, and then click **Find Hot Topics** again. The graphic is refreshed with the filtered results.

> **Tip:** If you want to build complex queries based on your specific needs, you can click **Edit Query** to use Query Editor to define your queries. When you define your queries, be sure to use only the fields that are specified in the **Properties Fields** section of the Hot Topic Analytics configuration. Otherwise, your queries will not take effect because the fields that you use are not included in the analysis of Hot Topic Analytics.

7. After you identify a group of incidents for which you want to set the parent/child relationship, select the check boxes before the record IDs, and then click the **Set Parent** button. The Set Parent screen is displayed.
8. From the **Link to Parent Incident** drop-down list, select the parent incident. The system will suggest the parent incident (the status of the incident is not closed) based on the similarity among incidents.
9. From the Child Incidents list, select at least one child incident.
10. Click the **Proceed** button. The Parent/Child relationship is set for the selected incidents.

> **Note:** If you want to create a new incident as the parent instead of selecting one from the list, you can click the **New Parent Incident** button create a new parent incident.

Access Hot Topic Analytics from SM reports

User Role: Service Desk Agent, Incident Manager, Problem Manager

When viewing SM reports for interactions, incidents, and problems, you can click a section in the report to drill down to the detailed record list, and then access Hot Topic Analytics for further analysis. Your selected filter condition in the report is automatically used in Hot Topic Analytics if the fields are indexed by Smart Analytics.

> **Note:** The fields and queries that are used to generate reports may not be supported by the Hot Topic Analytics configuration. In this case, Hot Topic Analytics does not take effect and cannot provide hot topic suggestions.

To access Hot Topic Analytics from SM reports, follow these steps:

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

   > **Note:** You must use the web client instead of the Windows client to view the dynamic topic map in Hot Topic Analytics.

2. Do one of the following to open the report dashboard for the Service Desk, Incident Management, or Problem Management module:

   - Click **Service Desk** > **Service Desk Overview**. The Service Desk Overview dashboard is displayed.
   - Click **Incident Management** > **Incident Overview**. The Incident Overview dashboard is displayed.
   - Click **Problem Management** > **Problem Overview**. The Problem Overview dashboard is displayed.

3. Click a section in a report where you can drill down the report and view the detailed record list. For example, if you click the section indicating "High" priority from the "Incident Backlog by Priority" report, the incidents with high priority are listed in the record list. The record list is displayed.

4. From the record list, click the **Hot Topic Analytics** button or **More** > **Hot Topic Analytics**. The Hot Topic Analytics is displayed and the hot areas are suggested based on the specific filter that is used to drill down the report. For example, the high priority incidents.

5. Review the hot topics suggested by Hot Topic Analytics, and then decide your further actions.

Chapter 5: Smart Analytics best practices

This section provides the following best practices on how you can configure and use Smart Analytics so that it brings more value to your business:

Improving accuracy for Smart Ticket

Smart Analytics provides several methods to help you to increase Smart Ticket accuracy according to different data sets. This section provides some best practices for you to improve the accuracy of Smart Ticket.

- **Set up data cleansing rules**

  Data cleansing can help you prepare the data that you want to send to Smart Analytics for indexing, training, and analyzing. By setting up proper data cleansing rules, you can have better data quality, which is critical to the best accuracy of auto-suggestion. To set up data cleansing rules, see "Configure data cleansing" on page 30.

- **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 to build the intelligence out of your large data volume.

  For example, you may have an "Other" category in your Service Manager implementation to accommodate the interactions for which the Service Desk agents cannot find a better, more accurate category. Normally, the interactions in this "Other" category are not considered as good sample data for Smart Ticket. We recommend that you add a filtering clause such as `category~="Other"` into the **Training Sample Query** field to exclude those records.

  Another example is that you can choose the records logged by Subject Matter Experts (SME) as the training samples for Smart Tickets. In this way, you can have sample data with better quality for categorization.

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

The basic training of Smart Ticket is meaning based training, which means Smart Analytics builds its intelligence based on the text information of your data. On top of meaning based intelligence, 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 record. The typical scenario is that if one particular record 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 38.

- **Optimize your training for Smart Ticket**

  Several advanced parameters defined in the Smart Ticket task definition are used to optimize the accuracy of auto suggestion. Note that these settings are tradeoffs between training time and accuracy, which 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 or 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 higher percentage means higher accuracy, but there is a threshold point. When the training source data percentage exceeds the threshold, the margin contribution will be lowered remarkably. The out-of-box value for this configuration is 90%, which 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 the 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 information about how to tune the training result, see "Perform tuning in the Smart Ticket definition" on page 39.

Set stop phrases for Hot Topic Analytics

User Role: Administrator

Adding stop phrases in the qssp.db file is a way to hide particular words or phrases from appearing in the Hot Topic Analytics topic map. The stop phrases are still retained in the Smart Analytics data set.

To add stop phrases for Hot Topic Analytics, follow these steps:

1. Make sure the following configuration is defined in the `IDOL/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 following Smart Analytics services:

   - HP SM Smart Analytics Main Server

   - HP SM Smart Analytics Content1

4. Add the words that you identified as stop phrases to the `./Content1/main/qssp.db` file.

5. Restart the following Smart Analytics services:

   - HP SM Smart Analytics Main Server

  - HP SM Smart Analytics Content1

6. Run Hot Topic Analytics again. Now, those stop phrases are no longer displayed in the topic map.

Chapter 6: Smart Analytics tailoring

This section provides the following tailoring best practices for Smart Analytics:

Extend Smart Ticket to other modules

User Role: Administrator

In the out-of-box system, Smart Ticket (auto-classification) is only enabled for the Service Desk module. If you want to use this feature in other modules, you can tailor your Service Manager system.

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

1. Define the Smart Ticket task for the Change Management module:

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

   b. Select **Blank**, and then 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** as **Module Name**.

   e. In the **Training Sample Query** field, provide a query by using Query Builder. This query decides which Change records will be sent to Smart Analytics for Smart Ticket training.

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

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

2. Create new Smart Ticket rule sets for the Change workflow by referring to the following out-of-box Smart Ticket rule sets as examples.

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.

Tip: For information about how the design workflows and rule actions, refer to the Process Designer documents in the Service Manager help center.

3. Add the Smart Ticket rule sets that you created to the Change workflow:

a. From **Change Management** > **Configuration** > **Change Workflows**, select the workflow to which you want to apply the Smart Ticket rule. 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.

4. Create a new form or update the existing form to use the new Smart Ticket task for the Change Management module. You can refer to the "Create Smart interaction" form (idol.quick.new.interaction) as an example.

Execute OCR in other processes

User Role: Administrator

Optical Character Recognition (OCR) is an out-of-box feature for Smart Ticket, which can extract texts from images, and then put the text into the interaction records when submitting requests by using Smart Ticket.

If you want to execute OCR when proceeding with other processes such as escalating, saving, or closing records, you can refer to the following example to tailor your Service Manager.

The following example describes how to execute OCR when escalating an interaction to an incident in different Service Manager modes. You need to make changes accordingly if you want to execute OCR on other actions in different modules.

Execute OCR when escalating an interaction to an incident in the Service Manager Classic or Hybrid mode

To execute OCR when escalating an interaction to an incident in Service Manager Classic, follow these steps:

1. Add a new ScriptLibrary, such as IDOL_OCR_Esclation, as follows:

   ```
   function processOCRNonPD(interaction, language) {
     var ocrResult = lib.IDOL_Utilities.processOCR(interaction, 'description', 
   language);
     if (ocrResult) {
       interaction.doSave();
       system.functions.rtecall("refresh", vars['$L.errorcode'], interaction);
     }
   }
   ```

2. Update the "cc.first.log2" process:

   a. Open the "cc.first.log2" process, and then go to the **RAD** tab.

   b. Locate the "cc.save" RAD application.

   c. In the **Post RAD Expressions** section of the "cc.save" RAD application, add the following statement:

      ```
      if ($L.exit="normal") then ($L.void=jscall("IDOL_OCR_
      Esclation.processOCRNonPD", $L.file, $G.my.language))
      ```

Execute OCR when escalating an interaction to an incident in the Service Manager Codeless mode

To execute OCR when escalating an interaction to an incident in Service Manager Codeless, follow these steps:

1. Add a new ScriptLibrary, such as IDOL_OCR_Esclation, as follows:

   ```
   function processOCRPD(interaction, language) {
     var ocrResult = lib.IDOL_Utilities.processOCR(interaction, 'description',
   language);
     if (ocrResult) {
       interaction.doSave();
       system.functions.rtecall("refresh", vars['$L.errorcode'], interaction);
     }
   }
   ```

2. Update the "sd.escalate" process:

   a. Open the "sd.escalate" process, and then go to the **RAD** tab.

   b. Locate the "se.view.engine" RAD application.

   c. In the **Post RAD Expressions** section of the "se.view.engine" RAD application, add the following statement:

      ```
      if ($L.es.action={"added", "normal", "resetrec"}) then ($L.void=jscall
      ("IDOL_OCR_Esclation.processOCRPD", $L.file, $G.my.language))
      ```

Implement OCR in a field other than the Description field

User Role: Administrator

Optical Character Recognition (OCR) is an out-of-box feature for Smart Ticket, which can extract texts from images, and then put the text into the interaction records when you submit requests by using Smart Ticket.

In an out-of-box Service Manager system, the Smart Ticket OCR feature saves and displays the extracted image content in the **Description** field. The subsequent Smart Interaction suggestions are also based on the **Description** field. However, if you want to use a field other than the Description field for the Smart Interaction OCR feature, you can follow the instructions in this section to tailor your system.

To use a field other than the Description field for the Smart Interaction OCR feature, follow these steps:

1. Add your new field to the “incidents” table:

   a. From the System Navigator, click **Tailoring** > **Database Dictionary**.

   b. Search for and open the “incidents” table.

   c. Add a new field in the table. For example, you can use “description.ocr” as the name of the new field.

   > **Note:** To ensure the new field can store the strings extracted from images, we recommend that when you add the new field, select the array data type first, and then select the character data type.

   d. Save the table.

2. Add new Smart Ticket configuration tasks for your new field:

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

   b. Delete the out-of-box “Standard category field” and “Service category field” configuration tasks.

   c. Add a new “Category” configuration, and then add “Description Ocr” to the **Content Fields** list on the **Configurations** tab.

   d. Add a new “Affected Service” configuration, and then add “Description Ocr” to the **Content Fields** list on the **Configurations** tab.

3. Add the new “description.ocr” field to the OCR related Java scripts. To do this, follow the steps that are appropriate for your environment:

   Service Manager Codeless

   a. From the System Navigator, click **Tailoring** > **Process Designer** > **Rule Sets**.

   b. Search for and clone the “sd.idol.ocr” rule set.

   > **Note:** The out-of-box rule sets and workflows are HP Proprietary, you need to clone the

related rule sets and workflows, and then make changes as necessary so that your tailoring can take effect.

c. From the cloned the rule set, open the OCR rule, and then add the *description.ocr* parameter as appropriate to the “lib.IDOL_SMIS.addOCRTask” JS call. These are shown in bold in the following scripts.

```
if (vars.$G_src && (system.vars.$lo_idol_img_enabled || system.vars.$lo_
idol_enabled)) {
       if (vars['$G.multi']) {
       company = vars['$lo.operator']['company'];
       lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'OCR', company,
'description.ocr');
    } else {
       lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'OCR', '',
'description.ocr');
    }
} else {
       var attachments = record.getAttachments();
       var attLen = 0;
       for (var i = 0; i < attachments.length; i++) {
               if (lib.IDOL_Utilities.isImage(attachments[i])){
                       attLen++;
                       break;
               }
       }
       //call OCR interface
       if (vars.$G_ess && (system.vars.$lo_idol_img_enabled ||
system.vars.$lo_idol_enabled) && attLen > 0)
       {
       if (vars['$G.multi']) {
               company = vars['$lo.operator']['company'];
               lib.IDOL_SMIS.addOCRTask(record, 'OCR', company,
'description.ocr');
       } else {
               lib.IDOL_SMIS.addOCRTask(record, 'OCR', '', 'description.ocr');
       }
       } else if ((vars.$G_ess && (system.vars.$lo_idol_img_enabled ||
system.vars.$lo_idol_enabled) && attLen === 0)) {
               if (vars['$G.multi']) {
               company = vars['$lo.operator']['company'];
               lib.IDOL_SMIS.addOCRTask(record, 'AutoFill', company,
'description.ocr');
```

```
       } else {
               lib.IDOL_SMIS.addOCRTask(record, 'AutoFill', '',
'description.ocr');
       }
       }
}
```

d. Search for and clone the “sd.idol.ocr.action” rule set. Then, from the cloned rule set, in the Process OCR rule, add the “description.ocr” parameter to the “lib.IDOL_Utilities.processOCRFG” JS call as shown in bold in the following scripts.

```
lib.IDOL_Utilities.processOCRFG(record, 'description.ocr')
```

e. Make other changes as necessary so that the updated rule sets can take effect. For example, clone the related workflow, and then insert the updated rules sets to the cloned workflow.

Service Manager Classic or Hybrid

a. From the System Navigator, click **Tailoring** > **Document Engine** > **Processes**.

b. Search for and open the “cc.first.log” process.

c. Go to the **Final Javascript** tab.

d. Add the *description.ocr* parameter to the “lib.IDOL_SMIS.addOCRTask” JS call. These are shown in bold in the following scripts.

```
if (vars['$L.action'] == 'logcatalog'){
  return;
}

if (vars.$lo_idol_img_enabled || vars.$lo_idol_enabled) {
  //if is src, add to smis task
  if (vars.$G_src) {
    if (vars['$G.multi']) {
        company = vars['$lo.operator']['company'];
        lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'OCR', company,
'description.ocr');
      } else {
        lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'OCR', '',
'description.ocr');
      }
      return;
```

```
 }

 var attachments = vars['$L.file'].getAttachments();
 var attLen = 0;
 for (var i = 0; i < attachments.length; i++) {
  if (lib.IDOL_Utilities.isImage(attachments[i])){
   attLen++;
   break;
  }
 }

 //call OCR interface
 if (vars.$G_ess && attLen > 0) {
   if (vars['$G.multi']) {
    company = vars['$lo.operator']['company'];
    lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'OCR', company,
'description.ocr');
   } else {
    lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'OCR', '',
'description.ocr');
   }
 } else if (vars.$G_ess && attLen === 0) {
  if (vars['$G.multi']) {
    company = vars['$lo.operator']['company'];
    lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'AutoFill', company,
'description.ocr');
   } else {
    lib.IDOL_SMIS.addOCRTask(vars['$L.file'], 'AutoFill', '',
'description.ocr');
   }
 }
}
```

4. Re-train the two new Smart Ticket configurations that you added in step 2.

5. When the training is finished, try the OCR related feature. The Smart Ticket OCR feature now saves and displays the extracted image content in the new **Description Ocr** field.

Add filters to the Hot Topic Analytics form

User Role: Administrator

In the out-of-box system, the Hot Topic Analytics form contains some pre-defined 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. Select and open a Hot Topic Analytics configuration record from the configuration list. For example, Incident.

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

4. 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.

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

6. Click the **Start Index** button to re-index the module for the new filter fields to take effects.

7. Go to Forms Designer, and then add the new filter fields into the "Hot Topic Analytics" forms that are used for the specific module. You can search for "idol.hta" in Forms Designer to get a list of the "Hot Topic Analytics" forms. For example, the format name of the Hot Topic Analytics for incidents is "idol.hta.im.pd.advcontent" for Service Manager Codeless or Hybrid, and "idol.hta.im.advcontent" for Service Manager Classic.

Enable Hot Topic Analytics for other modules

User Role: Administrator

In the out-of-box system, Hot Topic Analytics is available in the Service Desk, Incident Management, and Problem Management modules. If you want to use Hot Topic Analytics to help you identify hot topics in other modules such as Change Management, you can tailor your Service Manager system.

For example, if you want to enable Hot Topic Analytics to help you identify hot topics in Change Management, follow these steps:

1. Add a new Hot Topic Analytics configuration record for the Change Management module:

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

    b. In the **Add Configuration** drop-down list, select **cm3r**, and then click **Add**.

    c. Enter information for all the required fields such as the title, contents, time stamp, and properties fields, and then click **Add**.

> **Tip:** To fill in these fields, you can refer to the out-of-box Hot Topic Analytics configuration, and then use the same or similar settings.

d. Click **Start Index** to start indexing.

2. Add a menu item to the System Navigator to display Hot Topic Analytics for Changes:

   a. From the System Navigator, click **Tailoring** > **Tailoring Tools** > **Menus**.

   b. In the **Menu Name** field, type the parent menu where you want to add the new "Hot Topic Analytics for Changes" menu item, and then click **Search** to open the menu.

   > **Tip:** For example, you can type `HOME` to add the new "Hot Topic Analytics for Changes" menu item to the main menu.

   c. Add a new row at the end of the menu table by entering information for the following settings:

Setting	Value
Description	Hot Topic Analytics for Changes
Application	launch.idol.problem.hunter
Parameter Name	{"name","query"}
Parameter Value	{"cm3r","true"}
Condition	true

   d. Click **Save**.

3. Tailor the "IDOLModuleConfiguration" script file:

   a. Click **Tailoring** > **Script Library**.

   b. In the **Name** field, type `IDOLModuleConfiguration`, and then click **Search**. The detailed script is displayed.

   c. Modify the script accordingly so that it can work for the change records in the Change Management module.

> **Note:** In out-of-box systems, the "IDOLModuleConfiguration" script file enables Hot Topic Analytics only for incidents, problems, and interactions.

> **Tip:** You can search for "rootcause" in the script file to see where you need to make changes for the script to support other modules.

4. Create new display screens, formats, and processes accordingly.

> **Tip:** You can refer to the "idol.hta.pm" display screen, the "idol.hta.pm.advcontent" format, and the "idol.hot.topic.create.problem" process as examples for your tailoring.

5. Log off and log back on to Service Manager. Now you can access and use "Hot Topic Analytics for Changes" from the System Navigator.

Customize actions in hot topic map

User Role: Administrator

If you want to customize the actions available in the hot topic map, you can tailor the out-of-box Hot Topic Analytics. For example, for the out-of-box Hot Topic Analytics for Incidents, the Create Problem action (button) is available. You can change this action or add a new action according to your business needs.

To customize the actions in hot topic map, follow these steps:

1. Click **Tailoring** > **Script Library**.

2. In the **Name** field, type `IDOLModuleConfiguration`, and then click **Search**. The detailed script is displayed.

3. Locate the "MODULE_CONFIGS" Javascript Object. Inside MODULE_CONFIGS, you can see the configuration entries for different modules. The entry "key" must correspond to the table name of an SM module. For example: "probsummary."

   The "actions" configuration section is a Javascript array. The items defined in this array will be rendered as "the action button" in the Hot Topic Analytics chart. For example, you can see the following lines in the script:

```
   actions : [{
     id: 'idol-action-list',
     text: scmsg(1023, 'idol'),
     aria: scmsg(1023, 'idol'),
     process: 'idol.hot.topic.view'
   }, {
     id: 'idol-action-link-incident',
     text: scmsg(1025, 'idol'),
     aria: scmsg(1025, 'idol'),
     process: function() {
       return PDE.isIncidentEnabled() ? 'idol.hot.topic.create.pd.incident' :
'idol.hot.topic.create.incident';
     }
   }]
```

4. Modify the "actions" configuration section to add the definition for the new action. The parameters that you need to specify are described in the following table.

Parameter	Description
id	A unique value to identify which "action button" is clicked. The "id" value also has the CSS style attached. Currently, two styles are available: ○ "idol-action-list" has an "Open" icon. ○ "idol-action-link" has a "Link" icon.
text	The "action button" label that is displayed on the chart
aria	Texts used for accessibility
process	Represents the SM process name. The process is invoked when the "action button" is clicked. The configuration value can be either a text string or a function that returns a text string. When the process is invoked, two additional variables are available: ○ "$L.idol.selected.filename": the current module table name ○ "$L.idol.selected.query": the SM query to retrieve the selected records in the Hot Topic Analytics chart

For example, you can modify the following lines accordingly and add them to the script:

```
{
   id: 'idol-action-link-others',
   text : 'Link to some other module',
   aria : 'Link to some other module',
   process : 'idol.link.to.other.module'
 }
```

5. Click **Save** to save your change in the script file.

6. Create the process that you use for the new action button. For example, you need to create the "idol.link.to.other.module" process that you specified in step 4. In the process, you can define the behaviors when the action button is clicked.

Add more "Analytics Action" queries in the Hot Topic Analytics for Incidents

In the out-of-box system, the **Analytics Action** setting in the Hot Topic Analytics for incidents include the following three out-of-box action queries: Set Parent, Create Problem, and Create Change/Article.

If you want to add more custom action queries in the Hot Topic Analytics for Incidents, follow these steps:

1. Tailor the form of the Hot Topic Analtyics for Incidents to add one more option to the drop-down list of "Analytics Action".

2. Add the new action to the "IDOL HTA Action Type" globallist that is used in the Hot Topic Analytics configuration record for the Incident module.

3. In the **Advanced** tab of the Hot Topic Analytics configuration record for Incidents, select the new action that you added, and then define the query for this newly added action.

   Tip: The query also supports jscall function.

4. From the script library, open "IDOLModuleConfiguration" and then configure which actions can be shown in the action form. For example:

```
if (vars['$hta.analytics.action']==="createproblem") {
         return [list, createProblem];
       }
```

Configure Smart Analytics to support more languages

User Role: Administrator

With the out-of-box configuration, Smart Analytics supports the same language list that Service Manager supports. If the texts entered in the records (such as in title and description) are not in a language that is included in the supported language list of Service Manager, these texts cannot be indexed and analyzed by Smart Analytics.

However, Smart Analytics can be configured to index and analyze texts in other languages in addition to the out-of-box supported languages. To do this, follow these steps:

1. In the IDOL configuration file (AutonomyIDOLServer.cfg), add the desired language type into the [LanguageTypes] section. For example, if you want to support Vietnamese, you can add the following line into the [LanguageTypes] section:

   ```
   19=Vietnamese
   ```

   > **Tip:** You can refer to the AutonomyIDOLServer.cfg.default file (in the same directory as AutonomyIDOLServer.cfg) for a full list of language types and encoding settings.

2. Add encoding format and stoplist into the [LanguageTypes] section. For example, you can add the flowing configurations for Vietnamese:

   ```
   [vietnamese]
   Encodings=UTF8:vietnameseUTF8
   Stoplist=vietnamese.dat
   ```

   > **Note:** The stoplist file is a text file placed in the <Smart Analytics>/IDOL/langfiles folder, which contains words that you do not want to be treated as keywords in the query requests to IDOL.

3. Save the file.

> **Note:** The AutonomyIDOLServer.cfg configuration file does not affect the language support for the Optical Character Recognition (OCR) feature. OCR recognizes images based on the language setting specified in the contact record of a user in Service Manager. If no language is set in the user’s contact record, English is used as the default value in image recognition by Smart Analytics.

Chapter 7: Troubleshooting

This section contains the following topics to help administrators to troubleshoot 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 three different levels: the main proxy level, the Smart Search proxy level, and the content level. Each connector also has its own log folder. All the log files that are related to content are now in the corresponding content folder.

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

File name	Description
content_query.log	Logs messages relating to query processes.
content_queryterms.log	Logs the 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.

By default, the IDOL Server keeps the log files in the `./logs` folder and compresses the log files into the 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 items are the default logging configuration of 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:

```
<SmartAnalytics Installation>\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`

Parameter	Description
LogEcho	Displays logging messages on the console. Possible values: `TRUE` or `FALSE`
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.
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

Parameter	Description
	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.
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 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 Server, Image Server, or CFS server

If your Service Manager failed to connect the Smart Analytics Server, check the `application.log` file in the *<SM Smart Analytics>*`\IDOL\logs\` directory to make sure that the Smart Analytics IDOL Server is started. You also need to make sure that the following six components are started: agent, community, category, DIH, DAH, and view at the main level. Smart Search level has two components: DIH and DAH. If any component is not running normally, restart the Smart Analytics Server.

> **Note:** If the category and community components are not running, check if all your content servers and Smart Search proxy server are running. If not, start all of them and make sure they are available by the proxy server. And then restart the Smart Analytics main proxy server.

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

```
19/08/2015 12:47:26 [0] 00-Always: Determining child engine status...

19/08/2015 12:47:26 [0] 00-Always: Engine [dah] state : RUNNING

19/08/2015 12:47:26 [0] 00-Always: Engine [dih] state : RUNNING

19/08/2015 12:47:26 [0] 00-Always: Engine [community] state : RUNNING

19/08/2015 12:47:26 [0] 00-Always: Engine [category] state : RUNNING

19/08/2015 12:47:26 [0] 00-Always: Engine [agentstore] state : RUNNING

19/08/2015 12:47:26 [0] 00-Always: Engine [view] state : RUNNING

19/08/2015 12:47:26 [0] 00-Always: All 6 components started successfully.

19/08/2015 12:47:26 [0] 30-Normal: ACI Server validated operations key.

19/08/2015 12:47:26 [0] 30-Normal: ACI Server has no QPS limit.

19/08/2015 12:47:26 [0] 30-Normal: ACI Server is licensed for SSL encryption.

19/08/2015 12:47:26 [0] 30-Normal: Performed hostname lookup and converted
USERCLIENTS from
[16.187.190.64,127.0.0.1,127.0.0.1,SGDLITVM0581.hpswlabs.adapps.hp.com,fe80::d802:a
a38:e68c:435] ->
[16.187.190.64,127.0.0.1,::1,127.0.0.1,::1,16.187.190.81,fe80::d802:aa38:e68c:435].

19/08/2015 12:47:26 [0] 30-Normal: Performed hostname lookup and converted
ADMINCLIENTS from
[16.187.190.64,127.0.0.1,127.0.0.1,SGDLITVM0581.hpswlabs.adapps.hp.com,fe80::d802:a
a38:e68c:435] ->
[16.187.190.64,127.0.0.1,::1,127.0.0.1,::1,16.187.190.81,fe80::d802:aa38:e68c:435].

19/08/2015 12:47:26 [0] 30-Normal: This ACI Server will not accept unencrypted
communications from ACI clients.

19/08/2015 12:47:26 [0] 30-Normal: ACI Server setting MaxInputString to 64000.

19/08/2015 12:47:27 [0] 30-Normal: ACI Server successfully loaded online help.

19/08/2015 12:47:27 [0] 30-Normal: ACI Server successfully loaded admin UI.

19/08/2015 12:47:27 [100] 30-Normal: ACI thread 100 attached to port 9000

19/08/2015 12:47:27 [101] 30-Normal: ACI thread 101 attached to port 9000

19/08/2015 12:47:27 [102] 30-Normal: ACI thread 102 attached to port 9000
```

If your Service Manager failed to connect the Image Server, check the `application.log` file in the *<Smart Analytics>*`\Imageserver\logs` directory to make sure that the Image Server is started.

The following is a sample message in the log file that indicates your Image Server is started successfully:

```
19/08/2015 10:55:43 [1] 00-Always: ACI Server starting at xxx.xxx.xxx.xxx:18000

19/08/2015 10:55:43 [54] 00-Always: ACI Server thread 1 initialized

19/08/2015 10:55:43 [55] 00-Always: ACI Server thread 2 initialized

19/08/2015 10:55:43 [57] 00-Always: ACI Server thread 3 initialized

19/08/2015 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 Service Manager 9.41 is successful. Check that all the libraries are of the Service Manager 9.41 version. The default folder is `C:\Program Files (x86)\HP\Service Manager 9.41\Server\RUN\lib`.

3. If the issue still exists, you might use an old license. In this case, launch the Service Manager 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 9.41\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 125.

How to troubleshoot if Test Connection in Smart Analytics fails?

Enter the Smart Analytics Assistance by typing **SAA** in trhe command box. Check the status of all components that are listed in the table and see if any component is in the **Offline** status. The components and their corresponding processes are listed as below.

Services and corresponding processes

- HP IDOL Smart Analytics Main Server:

  `<SmartAnalytics>\IDOL\AutonomyIDOLServer.exe`

  `<SmartAnalytics>\IDOL\Community\community.exe`

  `<SmartAnalytics>\IDOL\view\view.exe`

  `<SmartAnalytics>\IDOL\Category\category.exe`

  `<SmartAnalytics>\IDOL\AgentStore\agentstore.exe`

  `<SmartAnalytics>\IDOL\dih\dih.exe`

  `<SmartAnalytics>\IDOL\dah\dah.exe`

- HP IDOL CFS Connector:

  `<SmartAnalytics>\IDOL\CFS\cfs.exe`

- HP IDOL Image Server1

  `<SmartAnalytics>\IDOL\ImageServer1\ImageServer1.exe`

- HP IDOL Content1

  `<SmartAnalytics>\Content1\Content1.exe`

- HP IDOL Content2

  `<SmartAnalytics>\Content2\Content2.exe`

- HP IDOL Content3

  `<SmartAnalytics>\Content3\Content3.exe`

- HP IDOL Smart Search Proxy

  `<SmartAnalytics>\IDOL\level2proxy\AutonomyIDOLServer.exe`

```
<SmartAnalytics>\IDOL\level2proxy\dah\dah.exe

<SmartAnalytics>\IDOL\level2proxy\dih\dih.exe
```

Check the log file first. All log files are in the logs folder of the corresponding service.

Check the general log file of the application.log file first to find if there is any error message showing that some process does not start, such as the following error message:

```
Engine [category] state : FAILED (no process detected)
```

Find the corresponding component log file, for example, the Category_application.log file.

Make sure the port number is not in conflict with others. The port number is occupied by other processes when the following message is displayed:

```
70-Error: Could not create TCP listener (Bad Parameter Value).
```

If detailed log information is required, set the value of **logLevel** to full (in the **[Logging]** section of the corresponding component) and restart the service for troubleshooting purpose. Rmember to modify the value back to normal afterwards.

How to troubleshoot if the upgraded content server is not running in Linux system?

1. Check the application.log file of the upgraded content server first to find if there is any error message displayed as below:

   ```
   26/08/2015 15:25:55 [1] 70-Error: Error: SecurityCode '1' is incorrectly
   configured, '1' was previously used with Security Type 'AUTONOMY_SECURITY_V4_
   NT_MAPPED' in library file '/usr/local/IDOLServer/IDOL/modules/mapped_security'

   26/08/2015 15:25:55 [1] 70-Error: Please see 'SecurityCode1.txt' for the
   correct settings for this type.

   26/08/2015 15:25:55 [1] 70-Error: Error: Failed to validate security settings

   26/08/2015 15:25:55 [1] 70-Error: Error: SecurityCode '2' is incorrectly
   configured, '2' was previously used with Security Type 'AUTONOMY_SECURITY_V4_
   ```

```
NETWARE_MAPPED' in library file '/usr/local/IDOLServer/IDOL/modules/mapped_security'

26/08/2015 15:25:55 [1] 70-Error: Please see 'SecurityCode2.txt' for the correct settings for this type.

26/08/2015 15:25:55 [1] 70-Error: Error: Failed to validate security settings
```

2. Locate the `[Security]` section in the .cfg file of the content server, and then add the // comment characters to the parameters as displayed in the following:

   ```
   [Security]

   SecurityInfoKeys=123,144,564,231

   DebugDecrypt=true

   //0=NT_V4

   //1=SharePoint
   ```

3. Restart your Smart Analytics.

Why a removed task is still displayed in the connector task list?

After you remove a task from the HTTP connector configuration, this removed task may still appear in the task list options.

For example, the **MYSITE** task is removed from HTTP connector but still shows in the task options.

To remove this task from this list, follow these steps:

1. Delete the folder of the deleted task.

   In this example, delete the *<Smart Analytics>*/HTTPConnector/MYSITE folder.

2. Delete the actions folder for this deleted task.

   In this example, delete the *<Smart Analytics>*/HTTPConnector/actions folder.

3. Restart the HTTP Connector service

Content servers are not running after installation

If your content servers are not running and the following error message is displayed in the application.log file for each content server, you need to modify the configuration file of the content server:

```
[1] 70-Error: Error: Attempt to open [ =…)0] failed. (No such file or directory).
The file open mode [rb] does not permit creation of a new file.
```

To fix this problem, follow these steps:

1. Modify the value of the **Threads** parameters in the configuration file of the content server. Make sure the number of **x+y** is no more than 32.

   ```
   [Server]

   Threads=x

   [AsyncActions]

   Threads=y
   ```

2. Restart the content server.

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 the cache to the disk.

Hot Topic Analytics is slow

If you experience slow performance when using Hot Topic Analytics, one possible reason is the field type configuration in the HTA content server. Check your action history in SAA to find out which fields are used in the `fieldtext=MATCH{`*`<value>`*`}:`*`<Field_Name>`* parameter. Then, you can add the field name to the `PropertyFieldCSVs` parameter in the `[SetMatchFields]` section of the IDOL configuration file (*<Smart Analytics Installation>*/IDOL/AutonomyIDOLServer.cfg). Doing so may help to enhance the performance. For example, you can add "COMPANY" and "CATEGORY" as shown in the following example:

```
[SetMatchFields]
PropertyFieldCSVs=*/*_MATCH,*/EDK_*,*/MATCH_*,*/COMPANY,*/CATEGORY
```

The new added match fields will automatically take effect for new data indexing after you restart the IDOL Server.

To regenerate the modified MatchType fields for the existing indexed data without re-indexing, you can add the `RegenerateMatchIndex=true` parameter to the Content.cfg file of the HTA content server, and then restart your content server.

```
[Server]
RegenerateMatchIndex=true
```

Tip: This regeneration is executed every time when the IDOL Server restarts. To save the start-up time of the IDOL Server, disable this option after you finish your performance tuning.

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, follow these steps.

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

2. Add a new definition with “probsummary” as **File Name** and “company” as **Mandant Field Name**.

Smart Analytics Assistant

Smart Analytics Assistant is a build-in tool that can help administrators to perform administrative tasks and troubleshoot Smart Analytics. To use this tool, see "Use Smart Analytics Assistant" on page 64.

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, Smart Analytics have three types of SMIS instances:

- **SMIDOL**

  The SMIDOL instance is for the training, testing, index, and tuning processes, which are triggered in **Smart Analytics Configuration**. Normally, one Service Manager server only has one SMIDOL instance named as SMIDOL*. The asterisk sign is the sequence number, which is usually 0.

- **SMIDOLOCR**

  The SMIDOLOCR instance is for the image analyzing process, which is triggered when users submit requests from the ESS portal (including SRC and the Mobility client). 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* (The asterisk is the sequence number). The Optical Character Recognition (OCR) task will be added to one of these instances after an interaction is created in ESS, depending on which instance has the least tasks in queue.

- **SMIDOLAutoFill**

  The SMIDOLAutoFill instance is for the auto-fill process. If an interaction is submitted to ESS without an attachment, a task will be added into this instance. In addition, if SMIDOLOCR is done, a SMIDOLAutoFill task will be also added . For performance consideration, one SM server has multiple SMIDOLAutoFill instances. The number of instances equals to the thread number of the IDOL Server. If the IDOL Server cannot be connected, only one instance will be created. The instance name is SMIDOLAutoFill* (The asterisk is the sequence number).

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

Manually create and enable an instance in SMIS

The SMIDOL and SMIDOLAutoFill instances are created and enabled automatically when you enable Smart Analytics in the **Smart Analytics Configuration** menu. The SMIDOLOCR is created and enabled automatically when you enable the Image Server in the **Smart Analytics Configuration** menu. These instances are also created when corresponding processes are triggered, such as the training, testing, tuning, index, or image process.

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

To create and enable a 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** , **SMIDOLAutoFill**, 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 an instance in SMIS

The SMIDOL and SMIDOLAutoFill instances are removed when you disable Smart Analytics while the SMIDOLOCR instances are removed when you disable the Image Server in the **Smart Analytics Configuration** menu.

If you want to manually disable or delete an SMIS 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 SMIS instances

If the SMIDOL, SMIDOLAutoFill, and SMIDOLOCR instances are created automatically, the default configuration is defined as follows:

Name:	SMIDOL*, SMIDOLAutoFill*, or SMIDOLOCR* **Note:** The asterisk sign (*) is the sequence number starting from 0.
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 the 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 Service Manager System Status page.

Chapter 8: Limitations

Smart Analytics contains the following limitations in the current release:

- **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 Process Designer is enabled, IT agents can use the “Image2Text” feature to copy and paste messages to the interaction records.

Appendix A: Smart Analytics APIs

Smart Analytics provides the following out-of-box APIs:

Smart Analytics RESTful APIs

Note: You must add the capability word "RESTful API" to a 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 136.

Smart Analytics provides the following RESTful APIs:

- "Smart classification" below
- "Hot topic" on the next page
- "Smart search" on page 132
- "Smart classification (by specifying IDOL adapters)" on page 134

Smart classification

This smart classification RESTful API is used to get the classifications suggested by Smart Analytics.

Request:

```
POST http://<SM Server Address>:13080/SM/9/rest/SmartAnalytics/1/action/suggest
```

An example of the request body:

```
{
  SmartAnalytics:{
    in:'{filename: "incidents", title: "test", description: ["test"], callback_
contact: "AARON, JIM"}',
  }
}
```

Response example:

> **Note:** You can ignore the messages in the response as these messages are printed by the Restful framework.

```
{
    "Messages": [
        "Invalid syntax for query.  Failed parsing",
        "in=\"1\"",
        "Invalid syntax for query.  Failed parsing",
        "in=\"1\""
    ],
    "ReturnCode": 0,
    "SmartAnalytics": {
        "in": "{filename: \"incidents\", title: \"test\", description: [\"test\"],
callback_contact: \"AARON, JIM\"}",
        "out": "
{\"category\":\"incident\",\"subcategory\":\"hardware\",\"product.type\":\"hardware
failure\",\"affected.item\":null}"
    }
}
```

Hot topic

This hot topic RESTful API is used to get the hot topics suggested by Smart Analytics.

Request:

`POST http://`*`<SM Server Address>`*`:13080/SM/9/rest/SmartAnalytics/1/action/`**`hottopic`**

An example of the request body:

```
{
  SmartAnalytics:{
    in:'{filename: "probsummary",  keyword:"email"}',
  }
}
```

Response example:

> **Note:** You can ignore the messages in the response as these messages are printed by the Restful framework.

```
{
    "Messages": [
        "Invalid syntax for query.  Failed parsing",
        "in=\"1\"",
        "Invalid syntax for query.  Failed parsing",
        "in=\"1\""
    ],
    "ReturnCode": 71,
    "SmartAnalytics": {
        "in": "{filename: \"probsummary\",  keyword:\"email\"}"
        "out": ‘{"recommends":["Shared MailBox"," Unable to access"," Email
receiving"],"subtopics":[{"topic":"Shared MailBox","subtopics":[{"topic":"New mail
sending","docs":["IM10122","IM10056"],"id":2},{"topic":"box is not accessible on
outlook","docs":["IM10121"],"id":4}],"docs":["IM10121","IM10056"],"id":1},
{"topic":"Unable to access","subtopics":[{"topic":"group mailbox's","docs":
["IM10131","IM10128"],"id":7,"subtopics":[{"id":8,"topic":"CHAR-Intranet / Internet
(North America)","raw":"Intranet / Internet (North America)","trivial":true,"docs":
["IM10131"]},{"id":9,"topic":"CHAR-
Applications","raw":"Applications","trivial":true,"docs":["IM10128"]}]},
{"topic":"Communication mail","docs":["IM10084","IM10128"],"id":10,"subtopics":
[{"id":11,"topic":"CHAR-E-mail / Webmail (North America)","raw":"E-mail / Webmail
(North America)","trivial":true,"docs":["IM10084"]},{"id":12,"topic":"CHAR-
Applications","raw":"Applications","trivial":true,"docs":["IM10128"]}]}],"docs":
["IM10131","IM10021"],"id":6},{"topic":"Email receiving","subtopics":
[{"id":14,"topic":"CHAR-E-mail / Webmail (North America)","raw":"E-mail / Webmail
(North America)","trivial":true,"docs":["IM10081","IM10125","IM10021"]},
{"id":15,"topic":"CHAR-Handheld, PDA & Telephony","raw":"Handheld, PDA &
Telephony","trivial":true,"docs":["IM10012"]}],"docs":
["IM10081","IM10125","IM10021","IM10012"],"id":13},{"topic":"mail
issues","subtopics":[{"id":17,"topic":"CHAR-
Applications","raw":"Applications","trivial":true,"docs":["IM10126"]},
{"id":18,"topic":"CHAR-E-mail / Webmail (North America)","raw":"E-mail / Webmail
(North America)","trivial":true,"docs":["IM10084","IM10081","IM10056"]}],"docs":
["IM10126","IM10084","IM10081","IM10056"],"id":16},{"topic":"User","subtopics":
[{"id":20,"topic":"CHAR-E-mail / Webmail (Asia)","raw":"E-mail / Webmail (Asia)
","trivial":true,"docs":["IM10186"]},{"id":21,"topic":"CHAR-E-mail / Webmail (North
America)","raw":"E-mail / Webmail (North America)","trivial":true,"docs":
["IM10091","IM10039","IM10081","IM10021"]},{"id":22,"topic":"CHAR-E-mail / Webmail
(Africa)","raw":"E-mail / Webmail (Africa)","trivial":true,"docs":["IM10059"]},
{"id":23,"topic":"CHAR-Applications","raw":"Applications","trivial":true,"docs":
["IM10105"]}],"docs":
["IM10186","IM10091","IM10059","IM10039","IM10105","IM10081","IM10021"],"id":19},
{"topic":"outlook","subtopics":[{"id":25,"topic":"CHAR-
Applications","raw":"Applications","trivial":true,"docs":
["IM10126","IM10011","IM10105","IM10128"]},{"id":26,"topic":"CHAR-E-mail / Webmail
(North America)","raw":"E-mail / Webmail (North America)","trivial":true,"docs":
["IM10091","IM10039","IM10121","IM10084"]},{"id":27,"topic":"CHAR-Intranet /
Internet (North America)","raw":"Intranet / Internet (North America)
","trivial":true,"docs":["IM10131"]}],"docs":
```

```
["IM10126","IM10091","IM10039","IM10011","IM10121","IM10105","IM10084","IM10131","I
M10128"],"id":24}],"summaries":{"IM10011":{"reference":"IM10011","title":"problems
with the send mails from outlook","summary":"problems with the send mails from
outlook. problems with the send mails from
outlook\n","weight":84.67,"type":"Applications"},"IM10012":
{"reference":"IM10012","title":"Email receiving error when using mobile phone as
email client.","summary":"Email receiving error when using mobile phone as email
client.. report error about 'connection fail' when attempt to connect to mail
server.\n","weight":83.83,"type":"Handheld, PDA & Telephony"},"IM10021":
{"reference":"IM10021","title":"User did not receive the reset password email
notification","summary":"User did not receive the reset password email
notification. I was unable to access Spend Management as it would not accept my
password. I chose Forgot  Password and I still have not received an e-mail with the
correct password.\n","weight":83.83,"type":"E-mail / Webmail (North America)
"},"IM10039":{"reference":"IM10039","title":"outlook flags have disappeared from
her e-mails","summary":"outlook flags have disappeared from her e-mails. user uses
the flags to organize her e-mails, flags have disappeared from her
mailbox.\n","weight":84.67,"type":"E-mail / Webmail (North America)"},"IM10056":
{"reference":"IM10056","title":"Shared MailBox issue","summary":"Shared MailBox
issue. We are receiving the delivery failure from Generic mailbox while sending new
mails.\n","weight":83.83,"type":"E-mail / Webmail (North America)"},"IM10059":
{"reference":"IM10059","title":"User is not recieving mails on
blackberry","summary":"User is not recieving mails on blackberry. User is not
recieving mails on blackberry and still not work after
restarting.\n","weight":84.67,"type":"E-mail / Webmail (Africa)"},"IM10081":
{"reference":"IM10081","title":"mail issues","summary":"mail issues. User not
receiving salary slips on email\n","weight":84.46,"type":"E-mail / Webmail (North
America)"},"IM10084":{"reference":"IM10084","title":"Communication mail
issue","summary":"Communication mail issue. I’ am not getting any communication
email to my outlook email id.\n","weight":84.46,"type":"E-mail / Webmail (North
America)"},"IM10091":{"reference":"IM10091","title":"Users are not rcving mails on
all the campaings of the COR on Altitude and Outlook both","summary":"Users are not
rcving mails on all the campaings of the COR on Altitude and Outlook both. Users
are not rcving mails on all the campaings of the COR on Altitude and Outlook both.
Please assist asap.\n","weight":84.67,"type":"E-mail / Webmail (North America)
"},"IM10105":{"reference":"IM10105","title":"User unable to send receive mails on
outlook","summary":"User unable to send receive mails on outlook. outlook state
keeps changing from trying to connect to connected...browser setttings are fine and
owa link is also not working\n","weight":84.46,"type":"Applications"},"IM10121":
{"reference":"IM10121","title":"Shared mail box is not accessible on
outlook","summary":"Shared mail box is not accessible on outlook. I am not able to
access shared mailbox from outlook and Lync since Thursday after the
migration.\nTried adding and removing the mailbox but still it is not
working.\n","weight":84.46,"type":"E-mail / Webmail (North America)"},"IM10122":
{"reference":"IM10122","title":"New mail sending error","summary":"New mail sending
error. When I tried to send new mail from GSRPA mailbox I’m receiving the below
error msg. please do the needful.\n","weight":84.67,"type":"E-mail / Webmail (North
America)"},"IM10125":{"reference":"IM10125","title":"Not able to send
emails","summary":"Not able to send emails. Not able to send emails..mails are
```

```
stucking in outbox.user is able to receive emails how ever mails are stucking in
the Outbox.so raising the request for the same.\n","weight":83.83,"type":"E-mail /
Webmail (North America)"},"IM10126":{"reference":"IM10126","title":"outlook mail
delivery issue","summary":"outlook mail delivery issue. I am receiving e-mail in
batches, about once an hour. Also, my smartphone keeps synchronizing e-mail, even
though I have set the Sync setting to
'Manual'.\n","weight":84.88,"type":"Applications"},"IM10128":
{"reference":"IM10128","title":"Outlook problem","summary":"Outlook problem.
Communication mail for my Group mailbox\n\nError for your reference –\n\n\"Cannot
Expand the folder\"\n","weight":83.83,"type":"Applications"},"IM10131":
{"reference":"IM10131","title":"Unable to access group mailbox's
archive","summary":"Unable to access group mailbox's archive. CSCS group mailbox is
recently migrated on outlook and we are unable to access our group mailbox archive
mails. Please do the needful ASAP.\n","weight":83.83,"type":"Intranet / Internet
(North America)"},"IM10186":{"reference":"IM10186","title":"Not getting mail from
external customer","summary":"Not getting mail from external customer. user report
cannot getting mail from external customer\n","weight":84.67,"type":"E-mail /
Webmail (Asia)"}},"docs":[],"id":0,"topic":"e-mail"}’
    }
}
```

Smart search

This hot topic RESTful API is used to get the search results suggested by Smart Analytics.

Request:

POST http://*<SM Server Address>*:13080/SM/9/rest/SmartAnalytics/1/action/**smartsearch**

An example of the request body:

```
{
  SmartAnalytics:{
    in:'{keyword: "test",  start:1, pagesize:2}',
  }
}
```

Response example:

Note: You can ignore the messages in the response as these messages are printed by the Restful framework.

```
{
    "Messages": [
        "Invalid syntax for query.  Failed parsing",
        "in=\"1\"",
        "Invalid syntax for query.  Failed parsing",
        "in=\"1\""
    ],
    "ReturnCode": -1,
    "SmartAnalytics": {
        "in": "{keyword: \"test\",  start:1, pagesize:2}",
        "out": "<autnresponse
xmlns:autn=\"http://schemas.autonomy.com/aci/\"><action>QUERY</action><response>SUC
CESS</response><responsedata>\n<autn:numhits>2</autn:numhits><autn:totalhits>18</au
tn:totalhits><autn:totaldbdocs>346</autn:totaldbdocs><autn:totaldbsecs>346</autn:to
taldbsecs><autn:hit><autn:reference>scactivelink%3A%2F%2Fkmdocument%3Aid%3D%26quot%
3BKM0580%26quot%3B%26nbsp%3Band%26nbsp%3Bkbname%3D%26quot%3BKnowledge_
Library%26quot%3B</autn:reference><autn:id>1588</autn:id><autn:section>0</autn:sect
ion><autn:weight>57.09</autn:weight><autn:links>TEST</autn:links><autn:database>Kno
wledge_Library</autn:database><autn:title>test error message by Jora(Title)
</autn:title><autn:summary>&lt;_em_&gt;test&lt;/_em_&gt; error message by Jora
(Title). 2015/06/22 14:07:46. falcon. external. errormsg. &lt;_em_&gt;test&lt;/_em_
&gt; error message by Jora(Error Message). &lt;_em_&gt;test&lt;/_em_&gt; error
message by Jora(cause). &lt;_em_&gt;test&lt;/_em_&gt; error message by Jora
(Wordaround/Fix).</autn:summary><autn:content><DOCUMENT><KMSEARCHCATEGORY>KM01CAT:K
M03CAT:KM05CAT</KMSEARCHCATEGORY><KMSTATUS>external</KMSTATUS><DOCTYPE>errormsg</DO
CTYPE><ID>KM0580</ID><SYSMODTIME_DATE>2015/06/22 14:47:00</SYSMODTIME_
DATE><CATEGORY>Service Manager&gt;Knowledge Management&gt;Document Maintenance and
Lifecycle;</CATEGORY><DRETITLE>test error message by Jora(Title)
</DRETITLE></DOCUMENT></autn:content></autn:hit><autn:hit><autn:reference>scactivel
ink%3A%2F%2Fkmdocument%3Aid%3D%26quot%3BKM0580%26quot%3B%26nbsp%3Band%26nbsp%3Bkbna
me%3D%26quot%3BKnowledge_
Library%26quot%3B</autn:reference><autn:id>1588</autn:id><autn:section>0</autn:sect
ion><autn:weight>57.09</autn:weight><autn:links>TEST</autn:links><autn:database>Kno
wledge_Library</autn:database><autn:title>test error message by Jora(Title)
</autn:title><autn:summary>&lt;_em_&gt;test&lt;/_em_&gt; error message by Jora
(Title). 2015/06/22 14:07:46. falcon. external. errormsg. &lt;_em_&gt;test&lt;/_em_
&gt; error message by Jora(Error Message). &lt;_em_&gt;test&lt;/_em_&gt; error
message by Jora(cause). &lt;_em_&gt;test&lt;/_em_&gt; error message by Jora
(Wordaround/Fix).</autn:summary><autn:content><DOCUMENT><KMSEARCHCATEGORY>KM01CAT:K
M03CAT:KM05CAT</KMSEARCHCATEGORY><KMSTATUS>external</KMSTATUS><DOCTYPE>errormsg</DO
CTYPE><ID>KM0580</ID><SYSMODTIME_DATE>2015/06/22 14:47:00</SYSMODTIME_
DATE><CATEGORY>Service Manager&gt;Knowledge Management&gt;Document Maintenance and
Lifecycle;</CATEGORY><DRETITLE>test error message by Jora(Title)
</DRETITLE></DOCUMENT></autn:content></autn:hit><autn:engines><autn:used>0</autn:us
ed><autn:unused>1</autn:unused></autn:engines><autn:warning>Engine 0: Engine 0: At
least one of the fields in a parameter (probably 'printfields') does not
exist</autn:warning><autn:warning>Engine 0: Engine 0: One of the fields used in the
field text does not exist</autn:warning><autn:warning>Engine 0: Engine 0: The
languagetype of the text could not be determined. The default languagetype was
used.</autn:warning><autn:warning>Engine 0: Engine 1: At least one of the fields in
a parameter (probably 'printfields') does not
exist</autn:warning><autn:warning>Engine 0: Engine 1: One of the fields used in the
field text does not exist</autn:warning><autn:warning>Engine 0: Engine 1: The
```

```
languagetype of the text could not be determined. The default languagetype was
used.</autn:warning></responsedata></autnresponse>"
    }
}
```

Smart classification (by specifying IDOL adapters)

This section introduces another way to perform auto-classification by using two 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 the 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 the 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 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.

APIs for Hot Topic Analytics indexing

If you want to tailor the index schedule of Hot Topic Analytics, you can use the following out-of-box Javascript APIs to control when to run the index task:

- lib.aciindex.manualFullReindex

  You can use this API to manually run a full index for the specified file that is used by Hot Topic Analytics.

- lib.aciindex.manualIncrementalIndex

  You can use this API to manually run an incremental index for the specified file that is used by Hot Topic Analytics.

These two functions will run in synchronous mode. We recommend that you run these two functions in the background schedule of HP Service Manager.

Syntax

```
lib.aciindex.manualFullReindex(file)
lib.aciindex.manualIncrementalIndex(file)
```

Arguments

Name	Data type	Required	Description
file	Datum object	Yes	This argument is the Service Manager table (for example, "probsummary") that holds the input source data. **Note:** Make sure that the fields of this "file" have been added into the **Filter Fields** section in the Hot Topic Analytics configuration (**System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**). For more information, see "Configure Hot Topic Analytics" on page 40.

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 and User Guide (Service Manager 9.41)

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!

hp

Java™
COMPATIBLE