

Spotlight Environment Wizard 1.6.0

Blackchair Spotlight Environment Wizard

Install Process

Version 1.6.0

- Introduction
- Wizard Setup
- Environment Installation
 - Welcome
 - Plugin Type
 - Environment Settings
 - Install Folder
 - Spotlight Service Account
 - Encrypt Passwords
 - SLConfig Database Connection
 - Environment Name
 - Time Zone
 - Plugin Database Connection
 - Plugin Settings
 - Avaya Communication Manager
 - Avaya Communication Manager - SDP Framework
 - Avaya Session Manager
 - Avaya Session Manager- SDP Framework
 - Avaya System Manager- SDP Framework
 - Cisco UCM
 - File Audit
 - Genesys Pure Connect
 - Genesys PureEngage
 - Genesys
 - GAX
 - Genesys PureEngage SDP Framework
 - Genesys
 - GAX
 - Session Border Controller
 - Placeholder/Empty Environment
 - Uninstall Environment
 - Spotlight License Details
 - Review
 - Administrator
 - Environment Key Vales
 - Perform Environment Install
 - Finishing Adding Plugin
 - Avaya Communication Manager
 - Avaya Communication Manager SDP Framework
 - Avaya Session Manager
 - Avaya Session Manager SDP Framework
 - Avaya System Manager SDP Framework
 - Cisco UCM
 - File Audit
 - Genesys Pure Connect
 - Genesys PureEngage
 - Genesys PureEngage SDP Framework
 - Session Border Controller
 - Placeholder/Empty Environment
- Commissioning
 - Website
 - Change Tracking Test
 - Log File Management
 - Service Alerts
 - Customer Logo
 - Not Supplied
 - Filtering
 - SDP
 - SDPFW
 - Multiple Message Servers
- Baseline/Sync

- Uninstall Environment
 - Troubleshooting
 - Issue Accessing UI
 - Resolution
 - Configuration Sync Error
 - Resolution
-

Introduction

The Spotlight Environment Wizard is a GUI driven tool designed to allow users to add Environments to a Spotlight Core Install. An Environment represents a system that Spotlight will track changes within, and the following technologies are currently supported

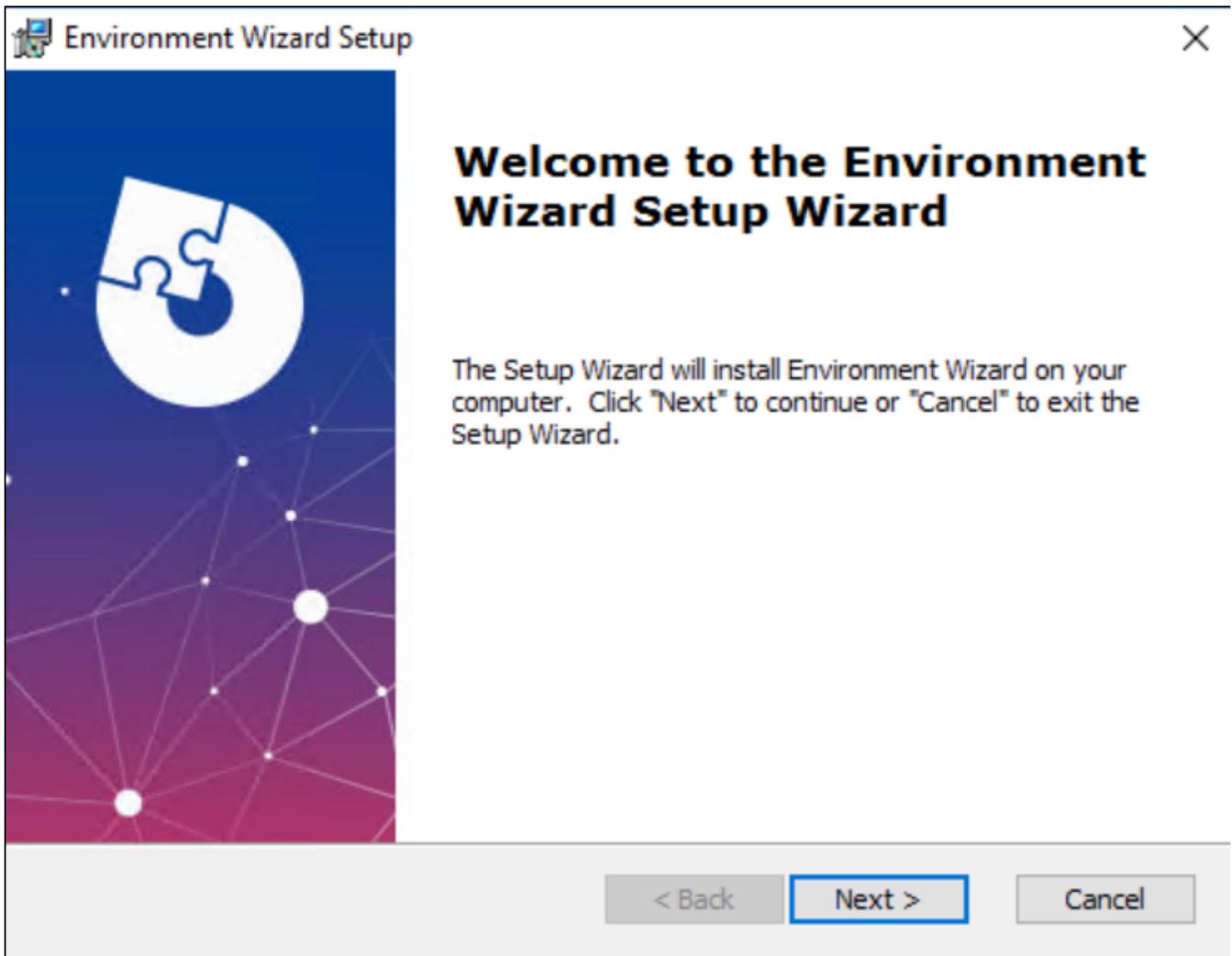
- Genesys PureEngage (CME/GAX)
- Genesys PureConnect
- Avaya CM
- Avaya SM
- Oracle/ACMW SBC
- File System Audit

In order to add environments, you must first have installed both Spotlight Core and the Environment Wizard.

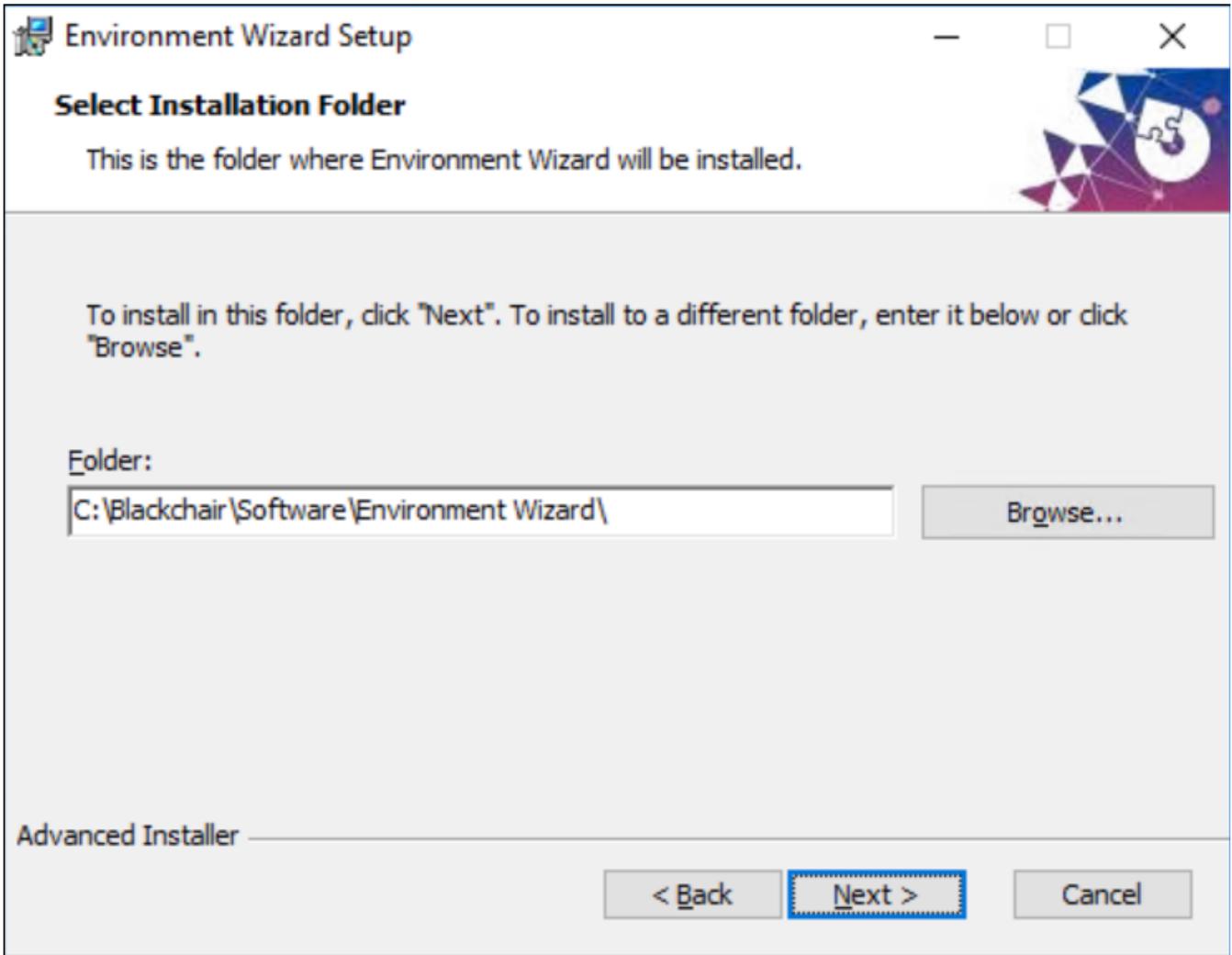
Wizard Setup

To install the Wizard:

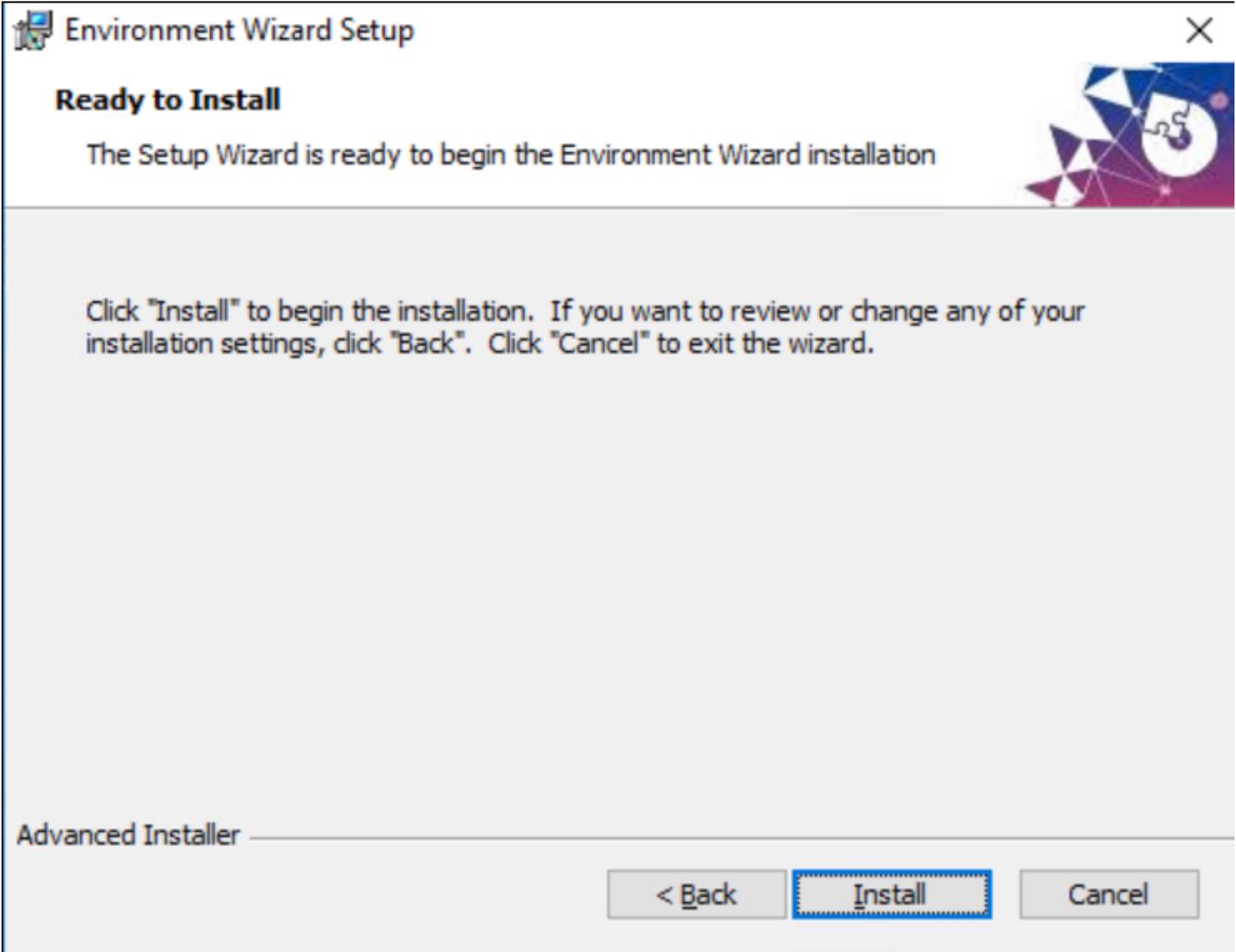
- Open the Windows Installer file - **Spotlight Environment Wizard - version number**
- Select **Next**



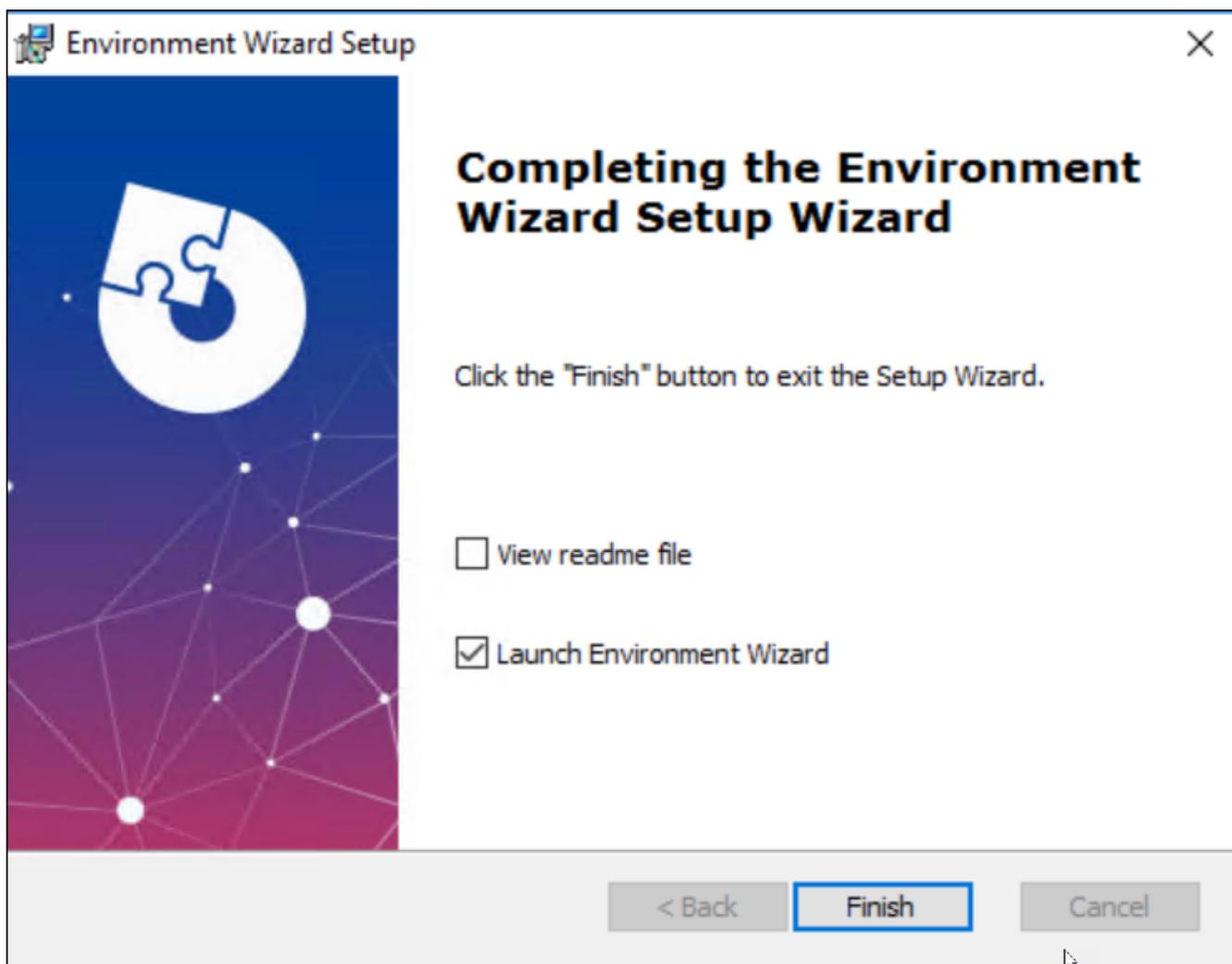
- Enter a Folder path - it is recommended to install in a folder within the main Spotlight folder. **C:\Blackchair\Software\Environment Wizard** is the default location
- You can also select **Browse** to locate and select an existing folder path
- Select **Next**



- Select **Install**



- When the wizard is installed, you can choose to view the **Read Me** file and/or launch the **Environment Wizard** by selecting the relevant check boxes



- A short cut to launch the wizard will also be placed on your desktop
- Select **Finish**

NB: The Read Me file contains the version history of the wizard

Environment Installation

Once installed, the Environment Wizard can be used to configure the systems that Spotlight is to track. To open the wizard:

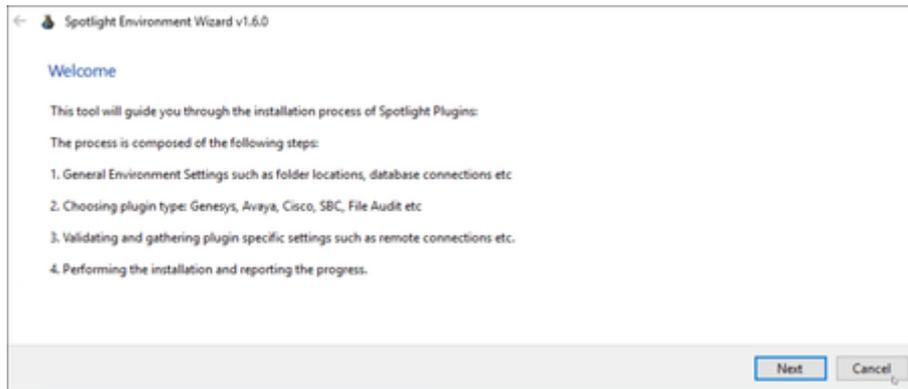
- Launch after install or
- Select the shortcut on your desktop or
- Double click the **EnvironmentWizard** application in the installed location eg **C:\Blackchair\Software\Environment Wizard**

Welcome

The wizard will guide you the process of adding an environment in the following areas. Much of this information will be the same regardless what type of Environment is being installed, however some information will be Plugin specific.

- General Environment Settings
- Choosing Plugin type
- Gathering Plugin settings and validating
- Review before installing

- Installing
- Post install actions



Select "**Next**" to continue

Plugin Type

- Select a **Plugin Type** using the relevant check box
- Select **Next**



NB: The Baseline/Sync option does not install an Environment. Please see the relevant section towards the end of this guide for further information

Environment Settings

The Environment Settings page is used to configure generic settings regardless of what Plugin type is to be installed, such as Install Folder, Database Connections etc as follows:

Install Folder

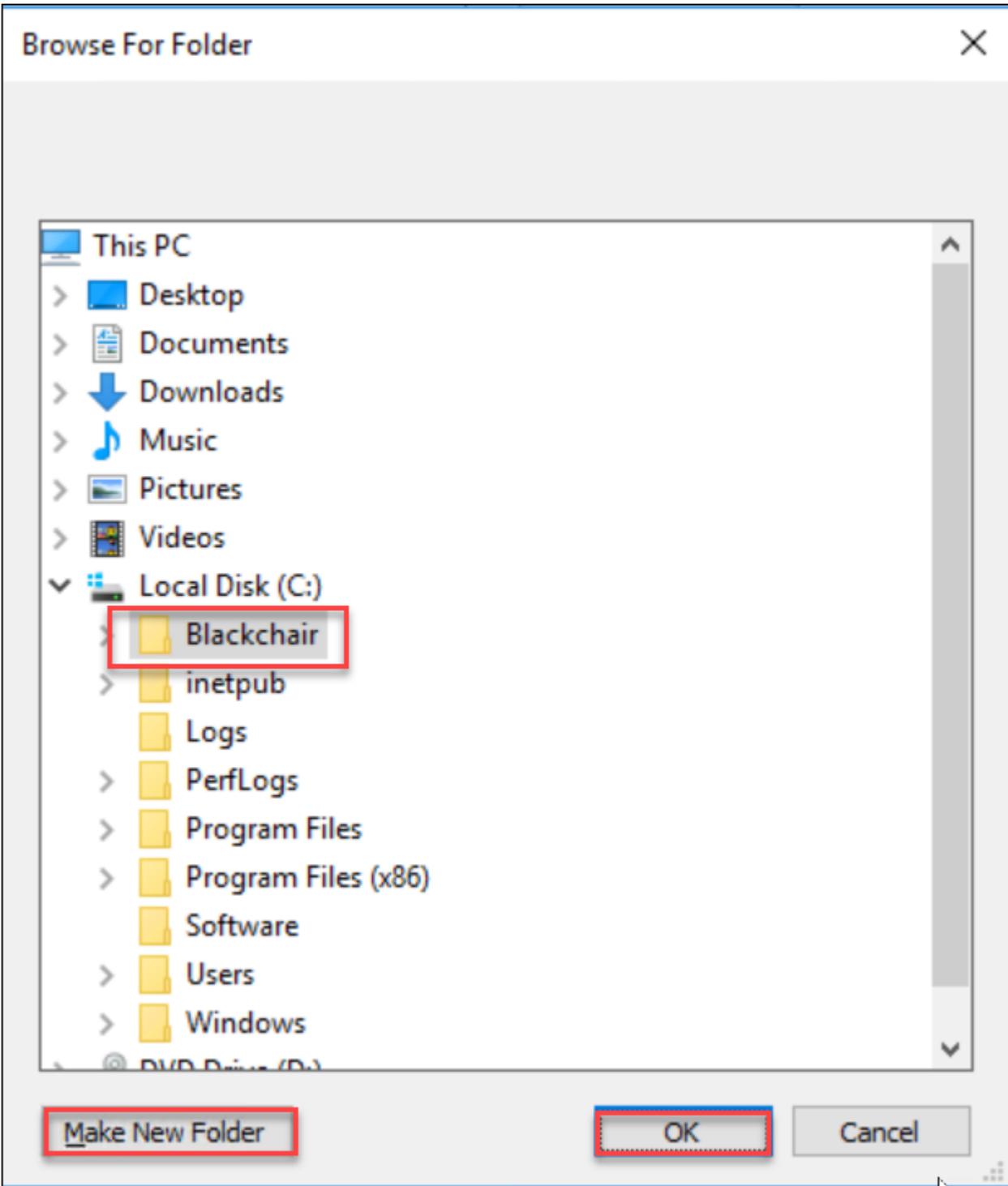
- Enter the folder path where the plugin is to be installed (default is **C:\Blackchair**) or

Base Install Folder:

Create loader in subfolder

If checked the subfolder name will be "BASEINTALLPATH\Loaders\Spotlight Loader (EnvironmentName)"

- Select **Browse** and select an existing folder, then **OK** or
- Select **Browse** and "Make a New Folder"
- Enter the folder name and then **OK**



- The Spotlight Loaders will be created in a sub folder (eg **BASEINSTALLPATH\Loaders\Spotlight Loader (Environment Name)**) unless the **Create Loader in sub folder** check box is deselected. **It is recommended that this is not deselected.**

Base Install Folder:

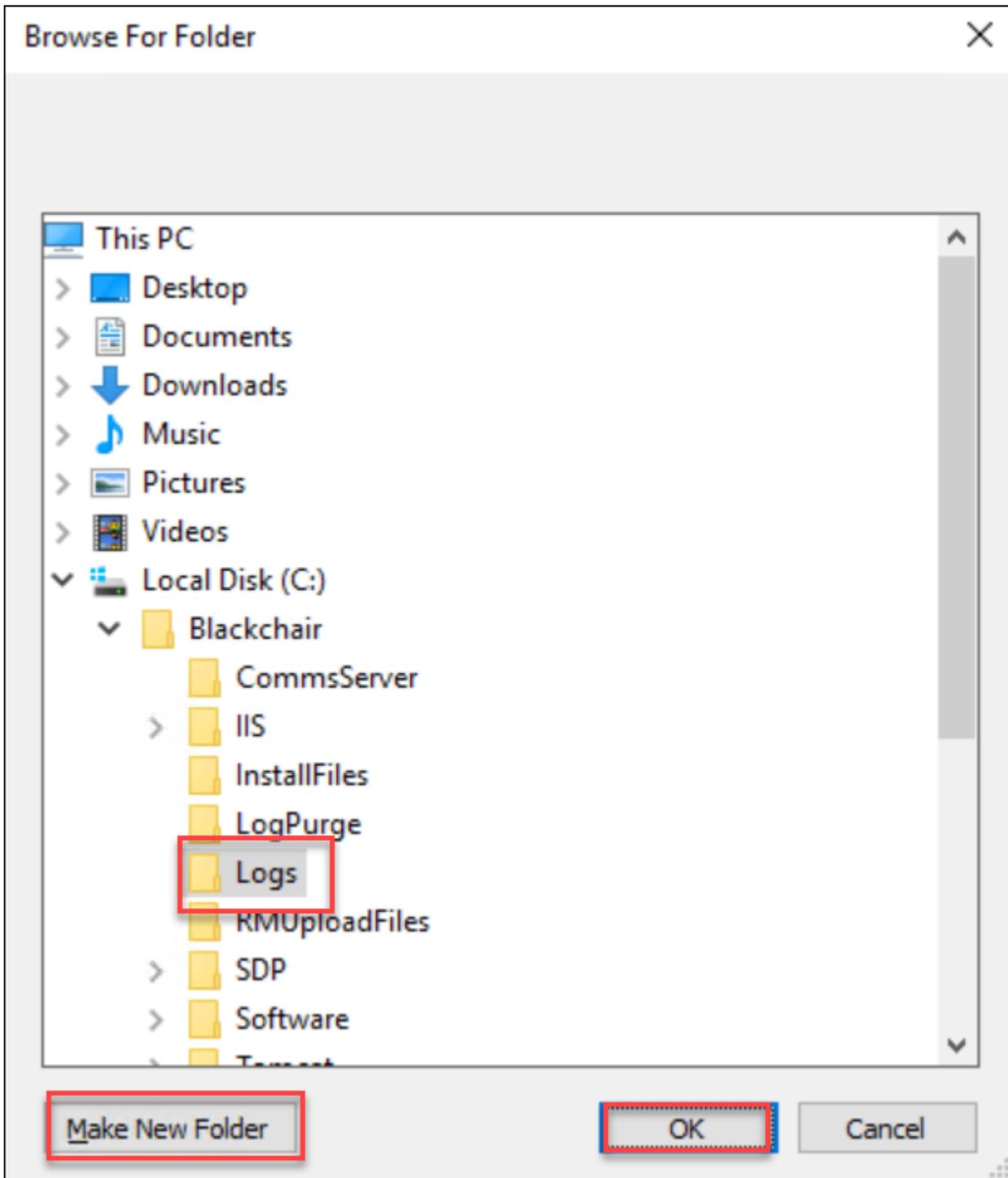
Create loader in subfolder

If checked the subfolder name will be "BASEINSTALLPATH\Loaders\Spotlight Loader {EnvironmentName}"

- Enter the folder path where the logs will be generated (default is **C:\Blackchair\Logs**) or

Base Logs Folder:

- Select **Browse** and select an existing folder, then **OK** or
- Select **Browse** and **"Make a New Folder"**
- Enter the folder name and then **OK**



Spotlight Service Account

By default all installed spotlight services will run using the Local System Account.

You can choose to use another account if you wish, and this is always required when db access is through **Windows Authentication**. To do so:

- Select **This Account** check box and enter the account name and password

Spotlight Service Account: Local System Account

This Account:

Password:

- or Select **Pick User** then

Spotlight Service Account: Local System Account

This Account:

Password:

- Enter the name of the account
- Select **Check Names** to validate
- Select **OK**

Encrypt Passwords

By default all passwords in spotlight configuration files will be encrypted. Deselect this check box if you wish these passwords to be displayed. This is normally only done when testing the system.

Encrypt Passwords on Configuration Files *Uncheck for testing purposes only!*

SLConfig Database Connection

Manually adjust the following information in the **SLConfig Database Connection** field:

- **Data Source** - the IP or Host name of the db server
- **Initial Catalog** - the name of the slconfig db
- **User ID** - the username of the spotlight db account
- **Password** - the password of the spotlight db account

SLConfig Database Connection:

Encrypt Passwords on Database

Alternatively you can instead :

- Select **Setup Connection**

SLConfig Database Connection:

Encrypt Passwords on Database

- For **MS SQL - SQL Server Authentication**
 - Enter the Server Name
 - Select **Use SQL Server Authentication**
 - Enter the spotlight db account username and password
 - Select **Save My Password**
 - Select or enter a database name
 - Select **slconfig** if the database has been created by the client
 - Enter **slconfig** if the database is yet to be created
 - Test the connection
 - Select **OK**

- For **MS SQL - Windows Authentication**
 - Enter the Server Name
 - Select **Use Windows Authentication**
 - Select **slconfig** if the database has been created by the client
 - Enter **slconfig** if the database is yet to be created
 - Test the connection
 - Select **OK**

NB: By default all passwords in the slconfig database will be encrypted

Environment Name

Enter the name of the Environment. This name will be displayed in the Spotlight UI and will be included in the names of all log files for that environment

It is recommended that the name should include descriptive text to indicate the system type and the system location - for example **Genesys Production** or **Avaya CM UAT**

Time Zone

Use the drop down to change the selected timezone. The timezone is only used by the Spotlight classic loader and does not impact the timezone of the Spotlight user interface

Plugin Database Connection

Manually adjust the following information in the **Plugin Database Connection** field:

- **Data Source** - the IP or Host name of the db server
- **Initial Catalog** - the name of the environment db
- **User ID** - the username of the spotlight db account
- **Password** - the password of the spotlight db account

NB: The default values are taken from the connection settings to slconfig database, with the database name adjusted to refer to the name of the environment.

Alternatively you can instead :

- Select **Setup Connection**

Plugin Database Connection:

Database is already created? *Check if database exists without any tables, view etc.*

Is an existing Spotlight Database? *Chek if database exists with all tables, views etc.*

All Settings are valid. Click Next To Continue

- For **MS SQL - SQL Server Authentication**
 - Enter the Server Name
 - Select **Use SQL Server Authentication**
 - Enter the spotlight db account username and password
 - Select **Save My Password**
 - Select or enter a database name
 - Select the name of the database if the database has been created by the client - normally **Spotlight_EnvironmentName**
 - Enter the name of the database to be created, if the database is yet to be created - normally **Spotlight_EnvironmentName**
 - Test the connection
 - Select **OK**

For **MS SQL - Windows Authentication**

- Enter the Server Name
- Select **Use Windows Authentication**
- Select or enter a database name
- Select or enter a database name
- Select the name of the database if the database has been created by the client - normally **Spotlight_EnvironmentName**
- Enter the name of the database to be created, if the database is yet to be created - normally **Spotlight_EnvironmentName**
- Test the connection
- Select **OK**

NB: By default all passwords in the slconfig database will be encrypted

- If the databases has already been created by the client, select **Database is already Created**
- If the database and the table structure has been created by the client, select **Is an existing Spotlight Database**

Plugin Database Connection:

Database is already created? *Check if database exists without any tables, view etc.*

Is an existing Spotlight Database? *Chek if database exists with all tables, views etc.*

All Settings are valid. Click Next To Continue

- Once the connection string has been set, select **Next**.
- If the installer is unable to connect to the db server, or the databases (where you say they have already been created) an error message will be displayed
- The screen will also highlight in which part of the provided data the issues relates to

Plugin Database Connection:

Database is already created? *Check if database exists without any tables, view etc.*

Is an existing Spotlight Database? *Chek if database exists with all tables, views etc.*

Please review the settings and make sure to correct the errors

- This needs to be resolved before continuing. The issue may be incorrect information provided or an inability to access the db server if it is separate from the software server
- When corrected, select **Next** to continue

Plugin Settings

The Plugin Settings that need to be configured will vary depending on what plugin was selected to be installed, The following section of this guide details the requirements for each type of plugin.

This information should be provided by the client before attempting to install an Environment.

Avaya Communication Manager

- In the **Communication Manager** section, enter the following information
 - Version
 - IP Address
 - Port number
 - Login
 - Password

1. Communication Manager

Version:

IP address:

Port:

Login:

Password:

- In the **AES** section, enter the following information
 - Version
 - IP Address
 - Port number
 - Confirm AES SMS SDK is enabled
 - TLS 1.2 - select if TLS 1.2 is enabled in Avaya

2. AES

Version:

IP address:

Port:

Confirm AES SMS SDK is enabled

TLS 1.2

- Select **Test Connection with ACM**
- A message will be displayed indicating if the connection was successful or not

Avaya Communication Manager Plugin Settings

1. Communication Manager

Version:

IP address:

Port:

Login:

Password:

2. AES

Version:

IP address:

Port:

Confirm AES SMS SDK is enabled

TLS 1.2

3. Test Connection with ACM Successfully connected to ACM. Click next to continue the process.

- Select **Next**

Avaya Communication Manager - SDP Framework

- Enter
 - Device ID - This should be the same name as the environment and should not have any spaces
 - Cluster ID -

Device Id: Cluster Id:

- In the **Communication Manager** section, enter the following information
 - Version
 - IP Address
 - Port number
 - Login
 - Password
 - ACM Request Interval (seconds)
 - Time zone
 - Scheduled Fixed Rate - default polling period

1. Communication Manager

Version: ACM Request Interval: seconds

IP address: Time zone:

Port: Scheduled Fixed Rate:

Login:

Password:

- In the **AES** section, enter the following information
 - Version
 - IP Address
 - Port number
 - Confirm AES SMS SDK is enabled
 - TLS 1.2 - select if TLS 1.2 is enabled in Avaya
 - Enable Splunk - enables the plugin to send change notification events to Splunk - see below for configuration

2. AES

Version:

IP address:

Port:

Confirm AES SMS SDK is enabled

TLS 1.2

Enable Splunk

If Splunk is enabled, further settings require to be entered (in a pop up window) as follows

- Splunk URL
- Timeout in milliseconds
- Splunk Token
- Splunk Source
- Select **Test Connection with ACM**
- A message will be displayed indicating if the connection was successful or not

Avaya Communication Manager SDP Framework Plugin Settings

Device Id: Cluster Id:

1. Communication Manager

Version: ACM Request Interval: seconds

IP address: Time zone:

Port: Scheduled Fixed Rate:

Login:

Password:

2. AES

Version:

IP address:

Port:

Confirm AES SMS SDK is enabled

TLS 1.2

Enable Splunk

3. Test Connection with ACM Successfully connected to ACM. Click next to continue the process.

- Select **Next**

Avaya Session Manager

- In the **Remote Host** section, enter the following information
 - IP Address
 - Port number - leave as 0 to use the default ssh port
 - Login name
 - Password

1. Remote Host

SMGR IP address:

Port: Leave 0 to use default ssh port, otherwise please specify

Login:

Password:

- Select **Test Connection with ASM**
- A message will be displayed indicating if the connection was successful or not

1. Remote Host

SMGR IP address:

Port: Leave 0 to use default ssh port, otherwise please specify

Login:

Password:

2. Test Connection with ASM Successfully connected to ASM. Click next to continue the process.

- Select **Next**

Avaya Session Manager- SDP Framework

- Enter
 - Device ID - This should be the same name as the environment and should not have any spaces
 - Cluster ID -

Device Id: Cluster Id:

- In the **Remote Host** section, enter the following information
 - SMGR IP Address
 - Port number - leave as 0 to use the default ssh port
 - Login name
 - Password
 - Admin Log Path
 - Audit Files path
 - Scheduled Fixed Rate - default polling period
 - Enable Splunk - enables the plugin to send change notification events to Splunk - see below for configuration

1. Remote Host

SMGR IP address: 192 . 168 . 48 . 201

Port: 22

Login: blackchair

Password: *****

Admin Log path: /var/log/Avaya/mgmt/asm/admina

Scheduled Fixed Rate: 15000

Enable Splunk

If Splunk is enabled, further settings require to be entered (in a pop up window) as follows

- Splunk URL
- Timeout in milliseconds
- Splunk Token
- Splunk Source
- Select **Test Connection with ASM**
- A message will be displayed indicating if the connection was successful or not
- Select **Next**

Avaya System Manager- SDP Framework

- Enter
 - Device ID - This should be the same name as the environment and should not have any spaces
 - Cluster ID -

Device Id: Cluster Id:

- In the **Remote Host** section, enter the following information
 - IP Address
 - Port number - leave as 0 to use the default ssh port
 - SSH Login name
 - Password
 - Web Username
 - Web Password
 - Protocol - http or https
 - NRP Log Path
 - Audit Files path
 - Time zone
 - Scheduled Fixed Rate - default polling period
 - Enable Splunk - enables the plugin to send change notification events to Splunk - see below for configuration

1. Remote Host

IP address: 172 . 10 . 10 . 50

Port: 22

SSH Login: dadmin

Password: *****

Web Username: admin

Password: *****

Protocol: http https

Nrp Log path: /var/log/Avaya/mgmt/nrp/nrpaudit.log

Time zone: Europe/London

Scheduled Fixed Rate: 60000

Enable Splunk

If Splunk is enabled, further settings require to be entered (in a pop up window) as follows

- Splunk URL
- Timeout in milliseconds
- Splunk Token
- Splunk Source
- Select **Test Connection**
- Select **Next**

Cisco UCM

- In the **Device** section, enter the following information
 - Device ID
 - Cluster ID
 - Hostname/IP
 - Username
 - Password
 - Port
 - Routing Source IP/Hostname
 - Router Port
 - WSDL Path or browse for it
 - Scheduled Fixed Rate - default polling period
 - Enable Splunk - enables the plugin to send change notification events to Splunk - see below for configuration

If Splunk is enabled, further settings require to be entered (in a pop up window) as follows

- Splunk URL
- Timeout in milliseconds
- Splunk Token
- Splunk Source
- Select **Test Connection with CUCM**
- A message will be displayed indicating if the connection was successful or not
- Select **Next**

File Audit

- Enter the following -
 - Device ID
 - Cluster ID

Device Id: Cluster Id:

- In the **Directories to monitor** section, select **Add Directory**

Directories to monitor: # Directory

File Extensions to monitor: # Extension

Add Directory Remove Add Extension Remove

Scheduled Fixed Rate: 3000 Enable Splunk

- Select an existing folder, then **OK** or
- Select **"Make a New Folder"**
- Enter the folder name and then **OK**

- In the **File Extensions to monitor** section, select **Add Extension**

Directories to monitor: # Directory

File Extensions to monitor: # Extension

Add Directory Remove **Add Extension** Remove

Scheduled Fixed Rate: 3000 Enable Splunk

- Type in a extension type into the search box
- Select **Search**
- Once located, select **Add** or
- Choose an extension type from the list - the search box will populate with the extension name
- Select **Add**

NB: Further directories and extensions can be added by repeating both processes above

- To remove a directory or extension already added:
 - Select the directory or extension
 - Select **Remove**

Directories to monitor:		File Extensions to monitor:	
#	Directory	#	Extension
1	C:\inetpub	1	reg

File Provisioning monitors folders/extensions on a remote server - MAY BE REMOVED AS NOT STANDARD

- Select **Enable File Provisioning** if applicable
- In the **Remote Host** section, enter the following information

Enable File Provisioning

Remote Host

IP address: 192 . 168 . 48 . 201

Port: 22
Leave 0 to use default ssh port, otherwise please specify

Username: blackchair

Password: *****

Directory: c:\\Blackchair

File Extensions to provision:

#	Extension
1	ssmssqlproj

- IP Address
- Port - leave 0 to use the default port
- Username
- Password
- Directory
- In the **File Extensions to provision** section, select **Add Extension**
- Type in a extension type into the search box
- Select **Search**
- Once located, select **Add** or
- Choose an extension type from the list - the search box will populate with the extension name
- Select **Add**

NB: Further extensions can be added by repeating the processes above

- To remove an extension already added:
- Select the extension
- Select **Remove**
- Select **Test SSH Connection**

Enable File Provisioning

Remote Host

IP address: 192 . 168 . 48 . 201

Port: 22
Leave 0 to use default ssh port, otherwise please specify

Username: blackchair

Password: *****

Directory: c:\\Blackchair

File Extensions to provision:

#	Extension
1	ssmssqlproj

Genesys Pure Connect

- In the **Pure Connect** section, enter the following information
 - Device ID
 - Cluster ID
 - Server Address
 - Server Port
 - Username
 - Password
 - Static Objects Retrieve - default is 120 thousand seconds
 - Resub Interval - default is 480 thousand seconds
 - License Retrieval Interval - default is 120 thousand seconds
 - Scheduled Fixed Rate - polling period default
 - Enable Splunk - enables the plugin to send change notification events to Splunk - see below for configuration

If Splunk is enabled, further settings require to be entered (in a pop up window) as follows

- Splunk URL
- Timeout in milliseconds
- Splunk Token
- Splunk Source

- Select **Test Connection with Device**
- A message will be displayed indicating if the connection was successful or not

- Select **Next**

Genesys PureEngage

Configuring Genesys PureEngage requires information for both CME and GAX, which can be added using the appropriate tabs

Genesys

- In the **Config Server** Section, enter the following information
 - Primary Hostname or IP
 - Primary Port
 - Backup Hostname or IP
 - Backup Port



- You can use the **Copy** buttons to save entering this data twice if there is no backup server
- The **Switch** button can be used to move primary data to backup fields and vice versa
- In the **MessageServer** Section, enter the following information
 - Primary Hostname or IP
 - Primary Port
 - Backup Hostname or IP
 - Backup Port

- You can use the **Copy** buttons to save entering this data twice if there is no backup server
- The **Switch** button can be used to move primary data to backup fields and vice versa
- In the **Authentication and Options** Section, enter the following information
 - CME Username
 - Password
 - Application Name
 - SDP Producer Application Name - default SpotlightAuditServer
 - SDP Consumer Application Name - default SpotlightAuditServerEC
 - Select **Is Genesys TLS Enabled** if this applies

- Select **Test Connection**
- A message will be displayed indicating if the connection to **Config Server and Message Server** was successful or not
- Select **Next** - this can only be selected once **GAX** data has been populated also

GAX

- Select **Enable GAX Monitoring** and enter the following details:
 - Is GAX version <= v8.5.1
 - Hostname or IP
 - Is GAX on https
 - Port
 - Username
 - Password

- Select **Test Connection with GAX**
- A message will be displayed indicating if the connection was successful or not
- Select **Next** - this can only be selected once **CME** data has been populated also

Genesys PureEngage SDP Framework

Configuring Genesys PureEngage requires information for both CME and GAX, which can be added using the appropriate tabs

Genesys

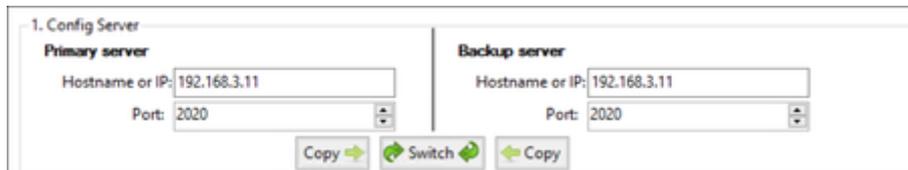
- Enter
 - Device ID - This should be the same name as the environment and should not have any spaces
 - Cluster ID -



Genesys GAX

Device Id: Cluster Id:

- In the **Config Server** Section, enter the following information
 - Primary Hostname or IP
 - Primary Port
 - Backup Hostname or IP
 - Backup Port



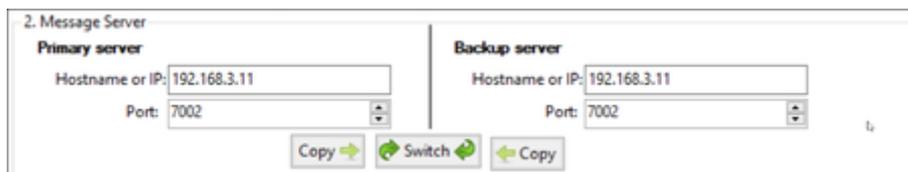
1. Config Server

Primary server
Hostname or IP:
Port:

Backup server
Hostname or IP:
Port:

Copy Switch Copy

- You can use the **Copy** buttons to save entering this data twice if there is no backup server
- The **Switch** button can be used to move primary data to backup fields and vice versa
- In the **MessageServer** Section, enter the following information
 - Primary Hostname or IP
 - Primary Port
 - Backup Hostname or IP
 - Backup Port



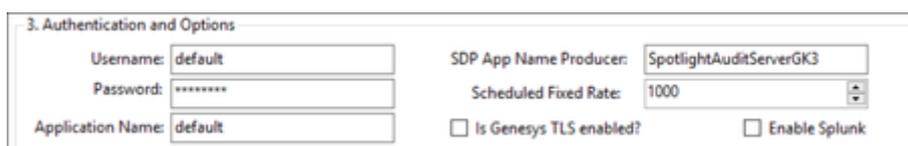
2. Message Server

Primary server
Hostname or IP:
Port:

Backup server
Hostname or IP:
Port:

Copy Switch Copy

- You can use the **Copy** buttons to save entering this data twice if there is no backup server
- The **Switch** button can be used to move primary data to backup fields and vice versa
- In the **Authentication and Options** Section, enter the following information
 - CME Username
 - Password
 - Application Name
 - SDP App Name Producer - default SpotlightAuditServer
 - Select **Is Genesys TLS Enabled** if this applies
 - Enable Splunk - enables the plugin to send change notification events to Splunk - see below for configuration



3. Authentication and Options

Username: SDP App Name Producer:

Password: Scheduled Fixed Rate:

Application Name: Is Genesys TLS enabled? Enable Splunk

If Splunk is enabled, further settings require to be entered (in a pop up window) as follows

- Splunk URL
- Timeout in milliseconds

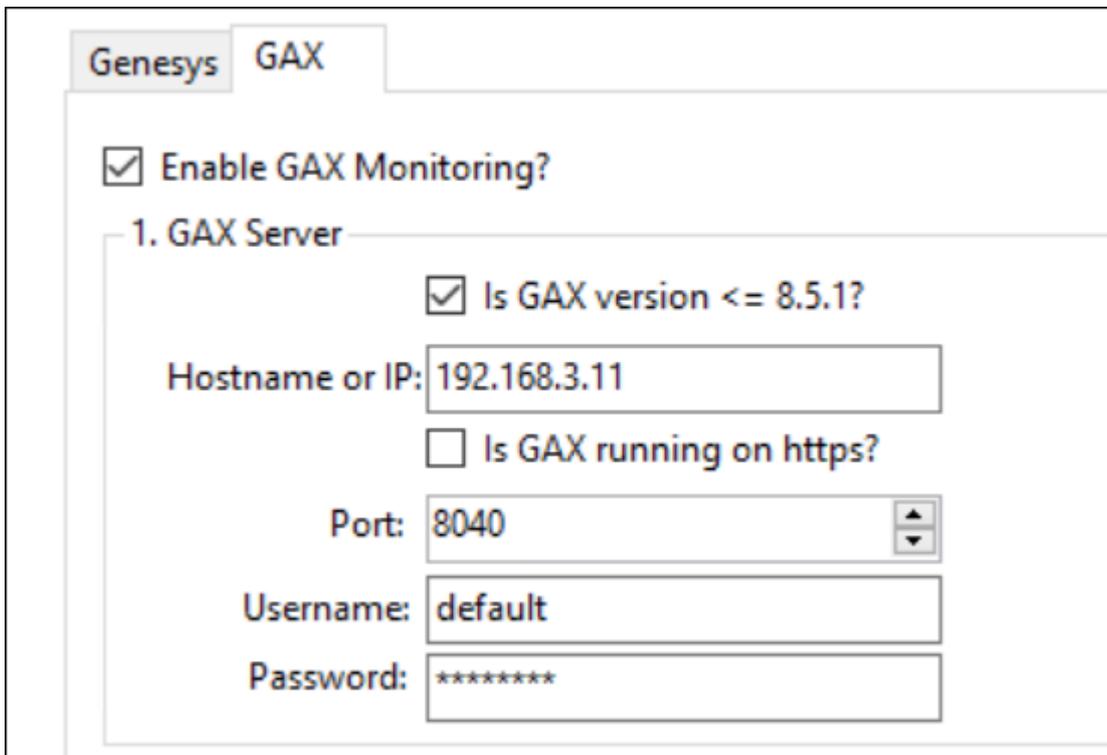
- Splunk Token
- Splunk Source
- Select **Test Connection**
- A message will be displayed indicating if the connection to **Config Server and Message Server** was successful or not



- Select **Next** - this can only be selected once **GAX** data has been populated also

GAX

- Select **Enable GAX Monitoring** and enter the following details:
 - Is GAX version <= v8.5.1
 - Hostname or IP
 - Is GAX on https
 - Port
 - Username
 - Password



- Select **Test Connection with GAX**
- A message will be displayed indicating if the connection was successful or not



- Select **Next** - this can only be selected once **CME** data has been populated also

Session Border Controller

- In the **SBC Host** section, enter the following information
 - Device ID
 - Cluster ID
 - IP Address
 - Username
 - Password
 - SSH Port
 - SNMP Port
 - SNMP Community
 - SNMP Trap Port
 - Enable Splunk - enables the plugin to send change notification events to Splunk - see below for configuration

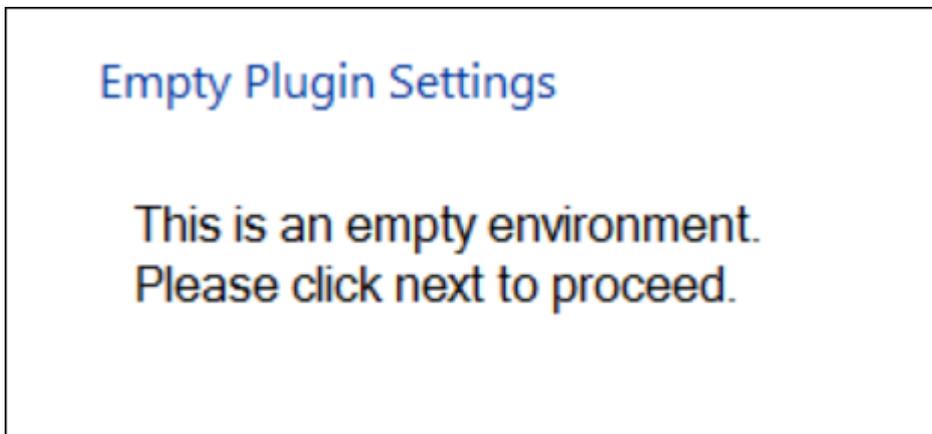
If Splunk is enabled, further settings require to be entered (in a pop up window) as follows

- Splunk URL
- Timeout in milliseconds
- Splunk Token
- In the **Receiver** section, enter the following information
 - IP Address
 - Router Type
 - Router Port
 - Routing Source IP
- Select **Test Connection with SBC**
- A message will be displayed indicating if the connection was successful or not
- Select **Next**

Placeholder/Empty Environment

The Environment Wizard can be used to create a blank/placeholder environment that can be fully configured at a later point. This could be necessary where a Plugin (type of environment) has been built , however has yet to be accommodated within the Environment Wizard.

This, therefore allows new types of plugins to be quickly built and utilised without the need to develop further the wizard



- No settings are required, select **Next** to proceed

Uninstall Environment

Further information on this option can be found subsequently in this document

Spotlight License Details

The **Environment Wizard** will generate a 30 day temporary Spotlight and SDP License. These can be replaced with permanent licenses during the installation process in the **Spotlight License Details** section.

- Select **Spotlight License Provided?**
- Select **Browse** and locate the Spotlight license - **InstallLicense.dat** file
- Select **Browse** and locate the SDP license - **license.properties** file
- Select **Next**

Spotlight license provided?

Spotlight License	<input type="text" value="C:\Blackchair\Software\Licenses\InstallLicense.dat"/>	<input type="button" value="Browse..."/>
Sdp License	<input type="text" value="C:\Blackchair\Software\Licenses\license.properties"/>	<input type="button" value="Browse..."/>

NB: If no license is provided a trial one with 30 days validity will be used

Review

The Review screen is used to review the installation steps and provided data before continuing with the installation. This screen will contain the same sections regardless of what Plugin is being installed, however the steps and values may differ

Administrator

This section can be used to change the username of the user that will be used to install the Environment. When installed, this user will be the only user that has access to the Environment, until that user creates more. To change the user info, manually enter a new windows domain account, display name and email address in the fields provided

Values for step are:

Logon:	<input type="text" value="WIN-4RK9KDGTL\Administrator"/>	Name:	<input type="text" value="Administrator"/>	Email:	<input type="text"/>
--------	--	-------	--	--------	----------------------

Environment Key Values

This section lists the Environment values that will be populated into the **slconfig** database **EnvironmentKV** table during the installation process.

- Review these for errors
- Adjust manually if desired

Values for step are:

Key	Value
ENV_DB_BASE_URL	http://WIN-4RX9KDG7G8L/Spotlight
ENV_CUST_URL_REPORTS	http://WIN-4RX9KDG7G8L/Reports
ENV_DB_URL_JAVA	jdbc:tds:sqlserver://192.168.3.4/Spotlight_PureEngage_SDPFW_645_191003_GK/?loginTimeout=15
ENV_DB_USERNAME	spotlight
ENV_DB_PASSWORD	tlz69WszCf5L9OuvARg==
ENV_DB_URL	Data Source=192.168.3.4;Initial Catalog=Spotlight_PureEngage_SDPFW_645_191003_GK;Persist Sec.
ENV_PERM_ENABLECONFIGPA...	true
ENV_PERM_ENABLEBASELINE	true
ENV_CYARA_BASEURL1	https://www.cyaraportal.uk

Additional Key Values can be added if required. Please reach out to Blackchair to understand when it would be necessary to add new key values. Some important examples are listed below

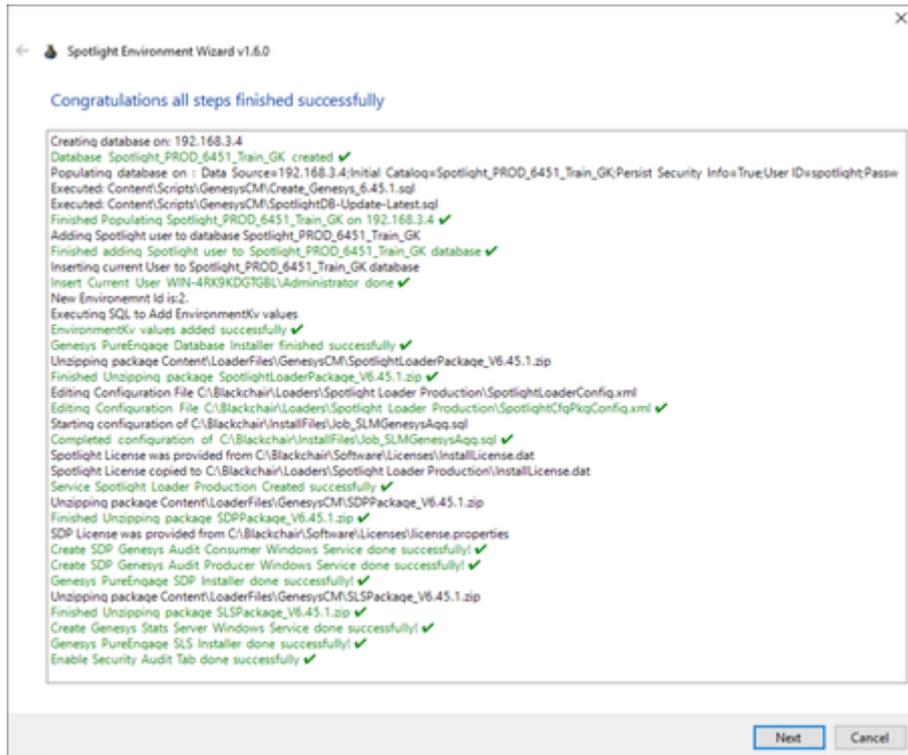
Key	Value	Description
ENV_CP_NORBPKG_	TRUE	Disables the auto rollback package creation feature in Release Management
ENV_CYARA_BASEURL	eg https://www.cyaraportal.us	This is the default Cyara Portal address used in Release Management and is created by the Core Installer. This URL can be amended if required.
ENV_CYARA_BASEURL1	eg https://www.cyaraportal.uk	Multiple Cyara Portal addressees can be added per environment by adding a new numbered entry, eg 1, 2, 3 etc
ENV_SHOW_ALERT	False	Will remove on screen alerts on the Spotlight UI for the environment being installed
ENV_PERM_SLM_GRP_RPT	True	Enables SAM License Group Reporting

To add a new key value:

- Select the last line of the table, where the key value is blank - a drop down will appear
- Choose the applicable key value
- Enter a value in the **Value** field
- Select **Next** to begin the installation

Perform Environment Install

During installation of the Environment, the screen will display a progress of the steps being performed. Once complete, the screen will indicate that the installation is successful. If any errors are highlighted (in red text), you will need to correct where necessary and re-run the installation



- Select **Next** to continue

Finishing Adding Plugin

The Finishing Adding Plugin page lists the actions required to finalise the installation to make the plugin fully operational, and provides shortcuts to perform these actions. The actions required to be performed will depend on what plugin has been installed as follows:

Avaya Communication Manager

Select the relevant buttons in numerical order to perform the following actions:

- Start the **Spotlight Loader** service - a message will indicate if the service started successfully
 - The loader will begin the process of syncing data between Avaya Configuration Manager and Spotlight
- Go to Start up page to add a new environment

Avaya Communication Manager SDP Framework

Select the relevant buttons in numerical order to perform the following actions:



- Restart all services (**SDP Consumer/Producer**) - a message will indicate if the services started successfully

- Restart all services (**IIS** and **Tomcat**) - a message will indicate if the services started successfully
- Start **baseline of the Device "Name"**- A message will be displayed indicating that the baseline has started
- Go to Start up page to add a new environment

Avaya Session Manager

Select the relevant buttons in numerical order to perform the following actions:

- Start the **Spotlight Loader** service - a message will indicate if the service started successfully
 - The loader will begin the process of syncing data between Avaya Session Manager and Spotlight
- Go to Start up page to add a new environment

Avaya Session Manager SDP Framework

Select the relevant buttons in numerical order to perform the following actions:



- Restart all services (**SDP Consumer/Producer**) - a message will indicate if the services started successfully
- Restart all services (**IIS and Tomcat**) - a message will indicate if the services started successfully
- Start **baseline of the Device "Name"**- A message will be displayed indicating that the baseline has started
- Go to Start up page to add a new environment

Avaya System Manager SDP Framework

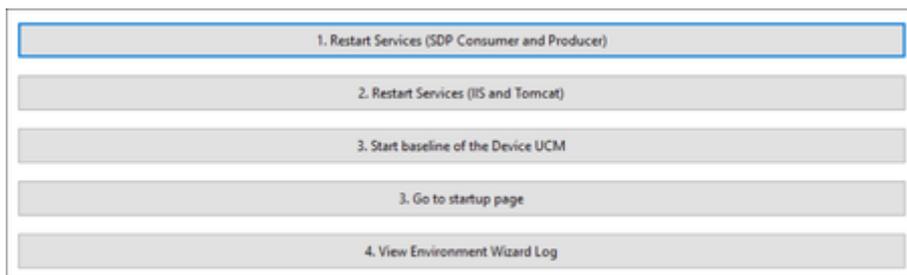
Select the relevant buttons in numerical order to perform the following actions:



- Restart all services (**SDP Consumer/Producer**) - a message will indicate if the services started successfully
- Restart all services (**IIS and Tomcat**) - a message will indicate if the services started successfully
- Start **baseline of the Device "Name"**- A message will be displayed indicating that the baseline has started
- Go to Start up page to add a new environment

Cisco UCM

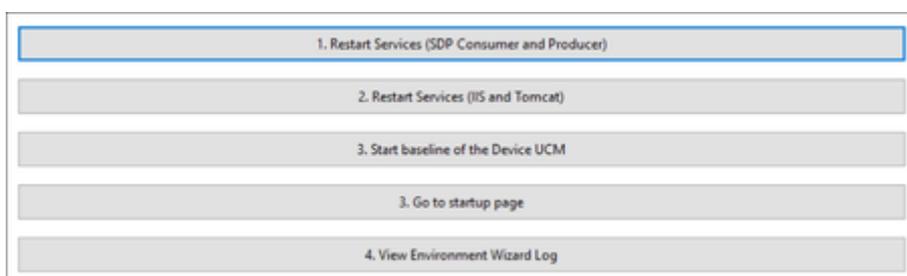
Select the relevant buttons in numerical order to perform the following actions:



- Restart all services (**SDP Consumer/Producer**) - a message will indicate if the services started successfully
- Restart all services (**IIS and Tomcat**) - a message will indicate if the services started successfully
- Start **baseline of the Device "Name"**- A message will be displayed indicating that the baseline has started
- Go to Start up page to add a new environment

File Audit

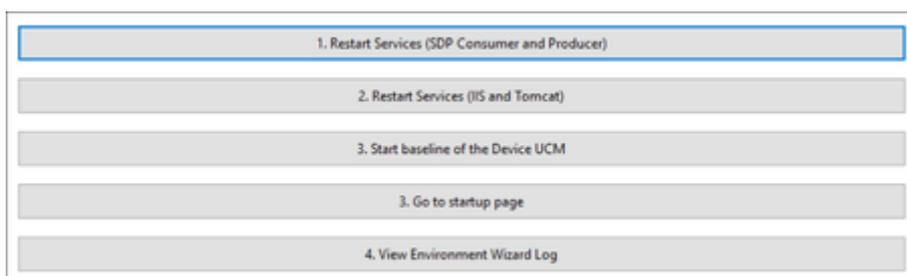
Select the relevant buttons in numerical order to perform the following actions:



- Restart all services (**SDP Consumer/Producer**) - a message will indicate if the services started successfully
 - Restart all services (**IIS and Tomcat**) - a message will indicate if the services started successfully
 - Start **baseline of the Device "Name"**- A message will be displayed indicating that the baseline has started
 - Go to Start up page to add a new environment
-
- Go to Start up page to add a new environment

Genesys Pure Connect

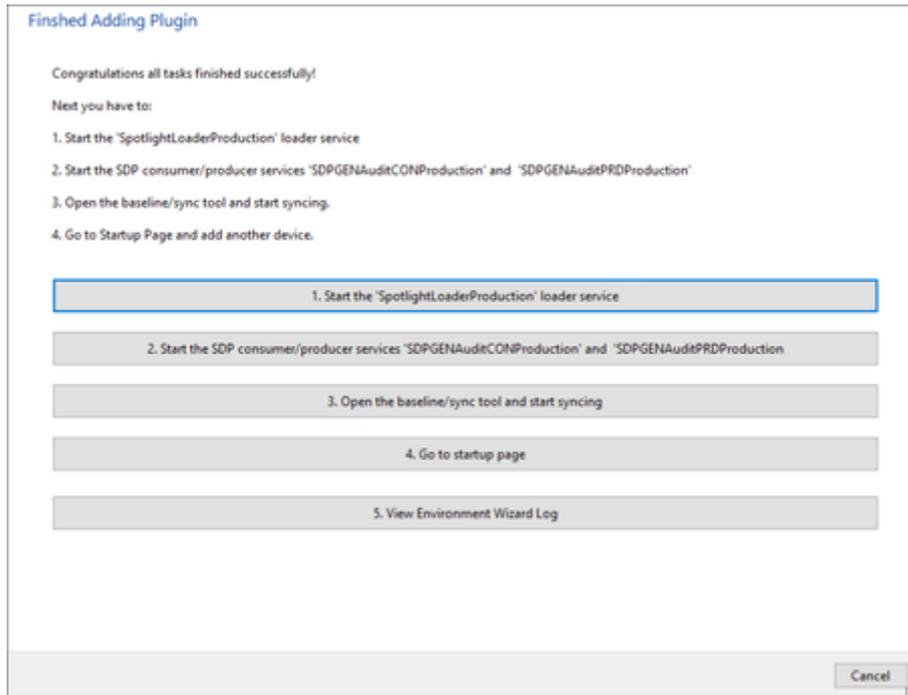
Select the relevant buttons in numerical order to perform the following actions:



- Restart all services (**SDP Consumer/Producer**) - a message will indicate if the services started successfully
- Restart all services (**IIS and Tomcat**) - a message will indicate if the services started successfully
- Start **baseline of the Device "Name"**- A message will be displayed indicating that the baseline has started
- Go to Start up page to add a new environment

Genesys PureEngage

Select the relevant buttons in numerical order to perform the following actions:

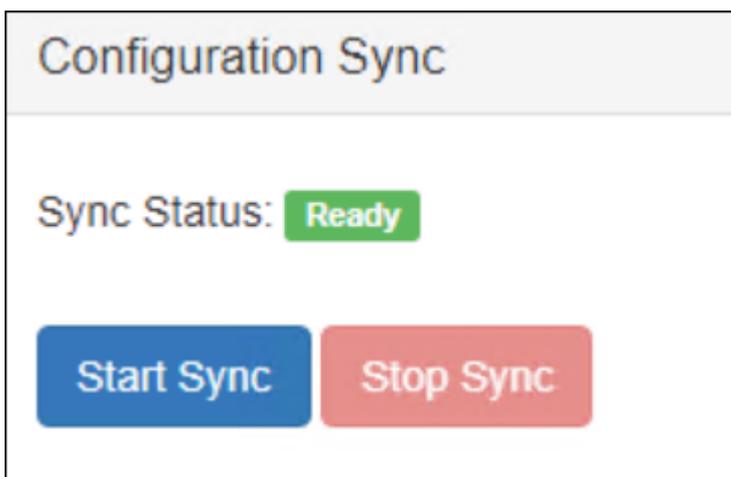


- Start the **Spotlight Loader** service - a message will indicate if the service started successfully
 - The loader will begin the process of syncing data between the Genesys GAX database and Spotlight

If the Spotlight database is on a named instance, the connection string in the **Consumer** and **Producer application.properties** files require to be adjusted to follow the below format. This needs to be done before starting the consumer and producer services

spotlight.db.url=jdbc:sqlserver://[ServerName];instanceName=[InstanceName];database=[DatabaseName];loginTimeout=30;

- Start the **SDP Consumer/Producer** services- a message will indicate if the service started successfully
- **Wait approx 2 minutes after the service start before continuing**
- Open the baseline tool to start syncing Genesys Configuration database data to Spotlight
 - Select **Start Sync**
 - The **Configuration Sync** tool will indicate it is running



- You will see the progress as data is loaded from each Genesys table
- Upon completion, the tool will display a ready message and the environment wizard will indicate that the sync is complete.
- The Configuration Sync can run in the background - it does not need to complete before you continue to add further environments or use Spotlight

Configuration Sync

Sync Status: **Running**

Started: **Mon Nov 25 2019 12:43:45 GMT+0000 (Greenwich Mean Time)**

Current Object Type: **CfgAlarmCondition**

Start Sync **Stop Sync**

Select All **Select None**

Selected	Item Type	Completed/Total
<input checked="" type="checkbox"/>	CfgTenant	1/1
<input checked="" type="checkbox"/>	CfgHost	2/2
<input checked="" type="checkbox"/>	CfgActionCode	3/3
<input checked="" type="checkbox"/>	CfgAlarmCondition	19/38
<input checked="" type="checkbox"/>	CfgApplication	0/235

- Go to Start up page to add a new environment

Genesys PureEngage SDP Framework

Select the relevant buttons in numerical order to perform the following actions:

Spotlight Environment Wizard v1.6.0

Finished Adding Plugin

Congratulations all tasks finished successfully!

Next you have to:

1. Restart the SDP Consumer and Producer services to pickup the added Device Test
2. If the device needs baseline triggering the Start baseline Test button will be enabled and you can press that or
3. Go to Startup Page and add another device.

1. Restart Services (SDP Consumer and Producer)

2. Restart Services (IIS and Tomcat)

3. Start baseline of the Device Test for CME and GAX

4. Go to startup page

5. View Environment Wizard Log

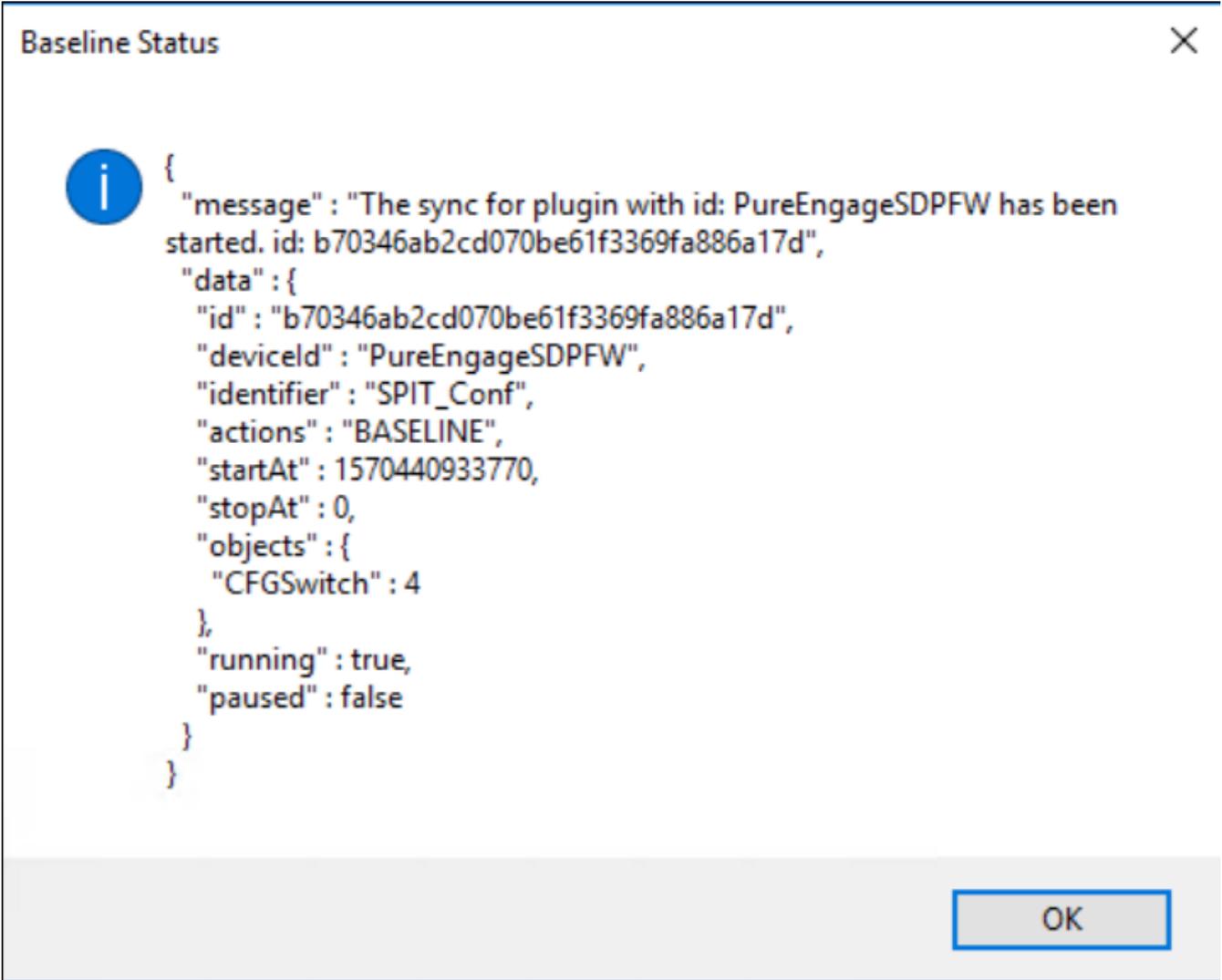
- Restart the SDP Consumer/Producer - a confirmation message will be displayed when complete
- IIS and Tomcat - a confirmation message will be displayed when complete
- Start baseline of the device
- 2 messages will be displayed on screen if the baseline starts successfully
 - The first message indicates the number of items that will be loaded from each Genesys Config DB table
 - The second message indicates that the GAX baseline has started
- Select **"OK"** at each message

Baseline Status



```
{  
  "message": "The sync for plugin with id: PureEngageSDPFW has been  
started. id: 3ef27aaf8a01e548b79c3d3309156430",  
  "data": {  
    "id": "3ef27aaf8a01e548b79c3d3309156430",  
    "deviceId": "PureEngageSDPFW",  
    "identifier": "SPIT_Conf",  
    "actions": "BASELINE",  
    "startAt": 1570440976125,  
    "stopAt": 0,  
    "running": true,  
    "paused": false  
  }  
}
```

OK



- The baseline will then run in the background
- Go to Start up page to add a new environment

Session Border Controller

Select the relevant buttons in numerical order to perform the following actions:

- Restart the **SDP Consumer/Producer** services- a message will indicate if the service started successfully
- Start baseline Session Border Controller data to Spotlight
- Go to Start up page to add a new environment

Placeholder/Empty Environment

Select the relevant buttons in numerical order to perform the following actions:



- Go to Start up page to add a new environment

Commissioning

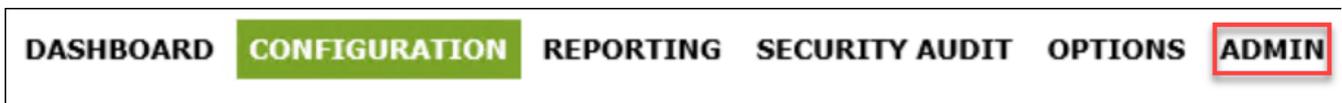
Once The Initial Load has been completed, it is necessary to undertake a few further steps in order to commission Spotlight for ongoing use as follows:

Please note that the sections on **Enable Security Audit, Filtering, Multiple Message Servers** and **Not Supplied** are specific to a **Genesys Pure Engage** install.

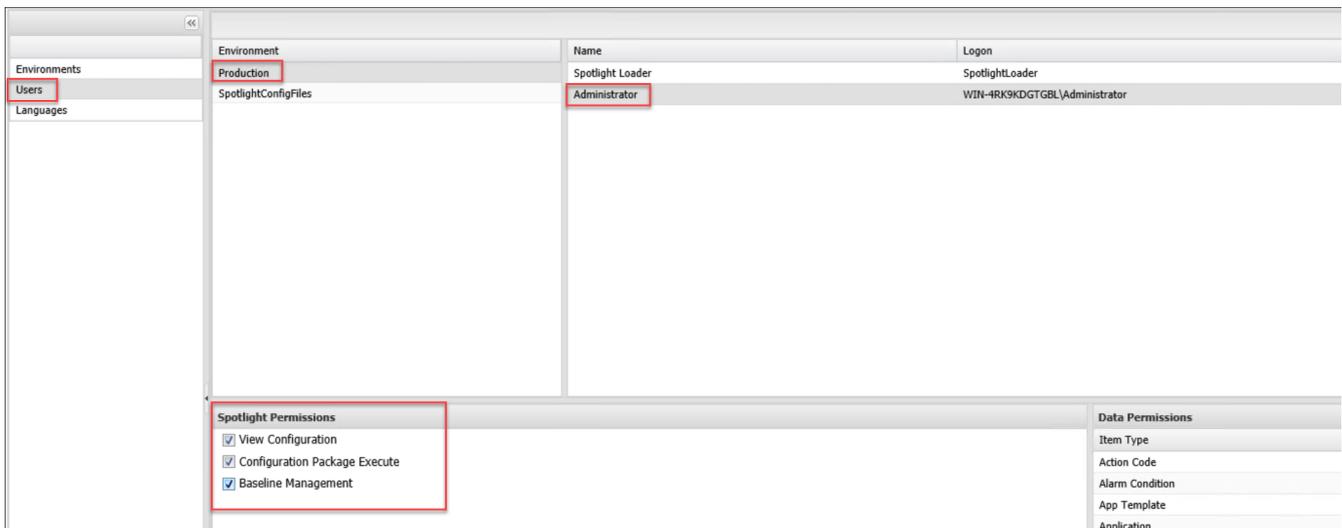
Website

The Windows user that the Install Assistant was run from is automatically made an administrator of the Spotlight system. This user is given **iew** permission to the Environment and its data in Spotlight, check this permission has been applied

- On the Spotlight server login to the web UI at <http://localhost/spotlight+>. If challenged for login credentials the username is domain\username, the password is the Windows password.
- Select **ADMIN**



- Click on **Users**
- Click on the environment name
- Click on the administrator user that installed spotlight
- In the **Spotlight Permissions** section, ensure **View Configuration** is selected



- Confirm the user can access data in the **Dashboard** tab

Change Tracking Test

To test change tracking in Spotlight, make a simple addition to the source system, for example create a test Person if Genesys pure engage is being tracked. When that new Person appears in the Spotlight website the data processing is current.

If the person does not appear in Spotlight, check the Spotlight logs for any exceptions, and escalate to Blackchair if necessary.

Log File Management

Log files are created in the folder you specified for application log files in the Install Assistant tool.

These log files should be managed by a daily scheduled job on the windows server that deletes files older than a specified age, 7 days is recommended.

Use Windows **Task Scheduler** to run the batch **LogPurge.bat** file provided which is located in the ...**Blackchair\LogPurge** folder after install.

The bat file should automatically be set up to point to the ...**Blackchair\Log** folder by the **FolderStructure.cmd** file run earlier in this document. An example of the command in the **LogPurge.bat** file is shown below:

```
forfiles /p "D:\Blackchair\Logs" /m *.log /s /c "cmd /c del @file" /d -7
```

If the number of days of log file needs to be increased or decreased then the numeric value at the end, following the **/d** parameter, can be changed accordingly.

Service Alerts

Service Alerts are used to indicate if each Spotlight database has been updated in the last day. If the answer is NO, an alert appears in the top right corner of each spotlight screen.

Service Alerts can be turned off for individual environments by entering new key values in the **EnvironmentsKV** sconfig table as follows.

- **Envid** – the environment id as found in the Environment table
 - **Envkey** – ENV_SHOW_ALERT
 - **Envvalue** - False
-

Customer Logo

A nice touch is to replace the Blackchair logo in the Spotlight UI with that of the customer. To do so:

- Navigate to the Spotlight Images folder on the Spotlight Server: <drive>\Blackchair\IIS\Spotlight\wwwroot\images\
 - Locate the "**bc_logo.png**" file and rename it to "**bc_logo_ORG.png**"
 - Put the customer logo in that directory and rename it to "**bc_logo.png**"
 - It must be EXACTLY this name and extension.
 - The ideal size for the logo should be **190w x 50h** (pixels) but anything close to these dimensions will work fine.
 - The file MUST be named as in #3, and MUST be a .png file
 - Easy to find any customer logo by googling it
 - Refresh your browser
-

Not Supplied

Spotlight is informed of changes made in Genesys via two messages sent by Genesys, one by the Config Server and one by the Message Server. If Spotlight does not receive the Message Server message within 5 seconds of the Config Server message, then Spotlight is unable to record which Genesys user made the change. Spotlight, therefore records this change in the User Interface as Not Supplied.

This situation also occurs when an agent is assigned to a Virtual Agent Group (VAG) in Genesys, as Genesys does not inform Spotlight of which user made the change. In these circumstances, it may be appropriate to either exclude these changes from Spotlight or identify them as a user other than "Not Supplied"

The following changes can be made in the Producer Applications.Properties file

- **producer.filterVirtualAgentGroupMessages = false**- The default value is true and excludes any VAG changes. Set it false to include these
- **producer.technicalUserName = Genesys** - The user that will be recorded against any VAG changes. Any name can be used, eg Genesys, VAG etc
- Once these changes have been made, save the file and restart the Producer service

- Repeat in further environments as required
-

Filtering

Spotlight supports the ability to filter out changes to **Flexible Property** and **Application Option** key/value pairs and whole sections based on some simple text pattern matching rules.

SDP

For a SDP Genesys Environment the rules for these are stored in the **Blackchair\SDP\Environment Name\GENAuditCON\config\FilterList.json** file

You place the pattern matching rules in the **excludeSectionList** and **excludeKeysList** sections of the file. Note that the [] denotes that it should contain a comma separated list of items.

There is a rudimentary pattern matching format which consists of a keyword followed by a string in single quotes. The keywords are:

- *contains* 'item1' - contains the string somewhere, similar to '%item1%'
- *starts* 'item1' - starts with the string
- *ends* 'item1' - end with the string
- *is* 'item1' - equals the string

Note: Pattern matching is case insensitive

Example 1 - Filter out all sections and keys that start with the string '**agent**' and all sections that have a section name called '**virtual**'.

Example 2 - Exclude property names that begin with '**customcontact**' or '**contactucs**'.

Aside from the keywords above, there are also 'negative' versions:

- notcontains
- notstarts
- notends
- isnot

It is unlikely these would be used in production as they will filter out all sections/keys apart from the ones that match. However they would be useful in development or test where you are testing changes to a single value.

Once a filter has been put in place, the **Consumer** service needs to be restarted

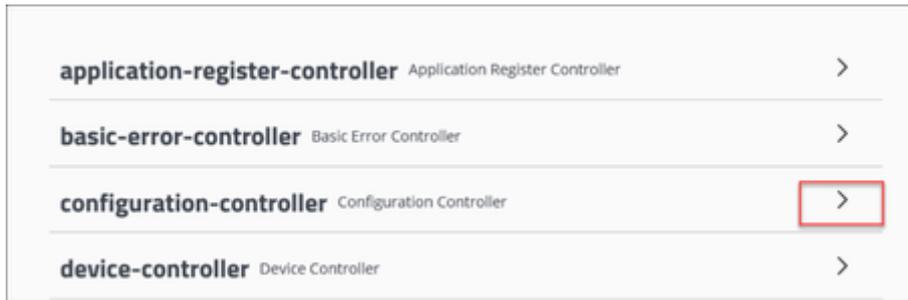
NB: From Spotlight v6.41.2 onward, the **FilerList.json** file by default is configured to exclude **Interaction Workspace** flexible properties

SDPFW

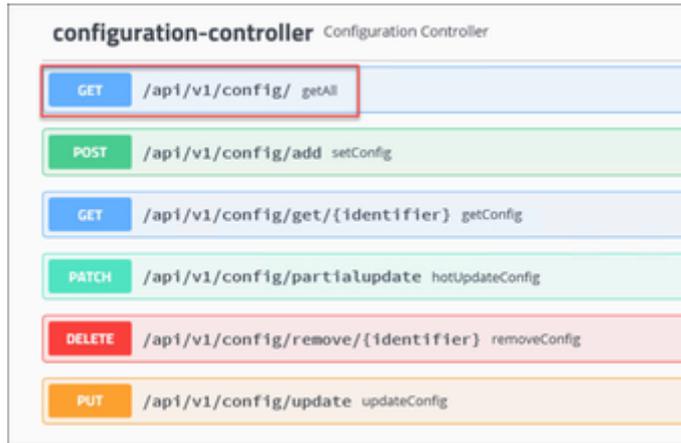
For a SDPFW Genesys environment, the filtering rules require to be adjusted in Swagger as follows

Launch Swagger in order to get the current SDPFW configuration

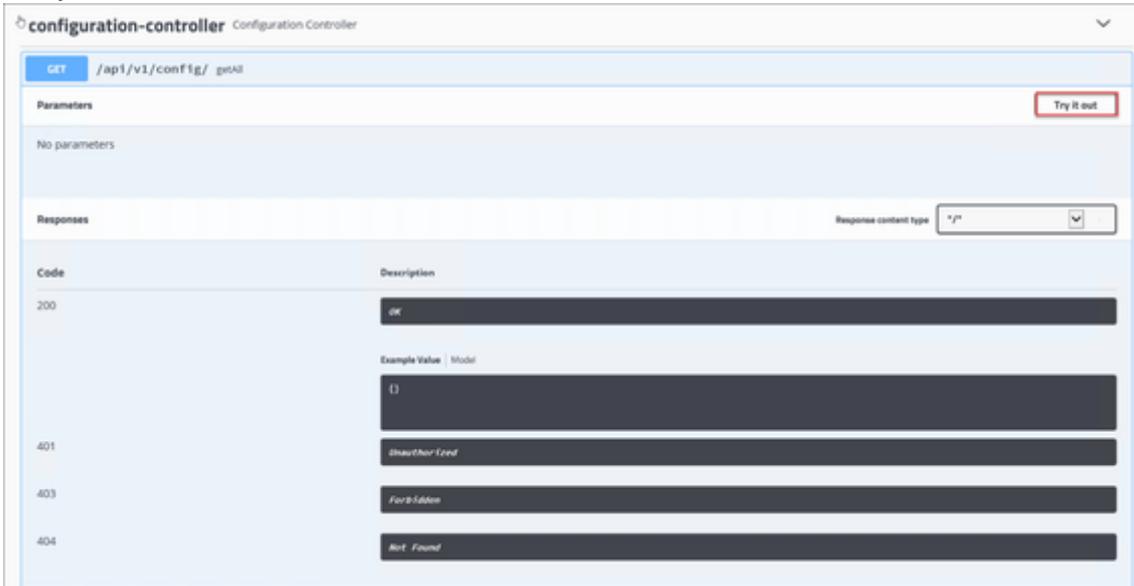
- Open : <http://localhost:8888/swagger-ui.html>
- Expand the **Configuration Controller**



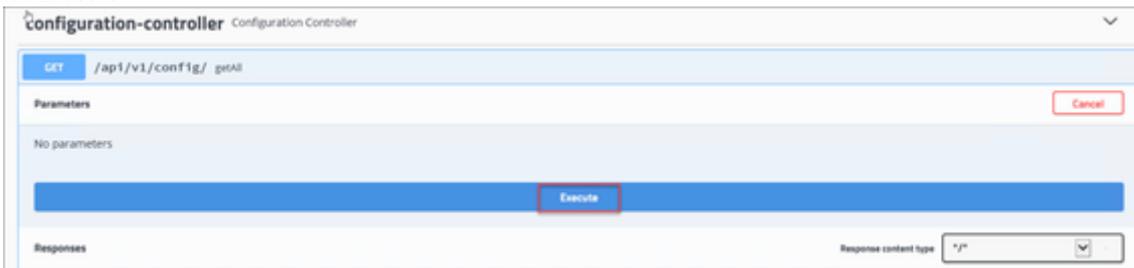
- Expand the **GET** section



- Click **Try it Out**



- Click **Execute**



- Download and save the **Response** body to a JSON file

The screenshot shows the Swagger UI interface for a Configuration Controller. The endpoint is `GET /api/v1/config/getAll`. The response status is 200. The response body is a JSON array containing configuration details for a RabbitMQ instance and other system settings. A red box highlights the 'Download' button in the bottom right corner of the response area.

```

[
  {
    "identifier": "SPIT_Conf",
    "usingHA": false,
    "messageBroker": [
      {
        "type": "RabbitMQ",
        "config": {
          "address": "localhost",
          "password": "guest",
          "port": "5672",
          "username": "guest"
        }
      }
    ],
    "producerConfig": {
      "usingHA": false,
      "application": {
        "healthCheckSchedule": 5000,
        "loggingLevelRoot": "DEBUG",
        "scheduledFixedRateAll": 5000,
        "splunkLogger": false,
        "traceService": true,
        "trustAllSsl": true
      }
    },
    "devices": [
  
```

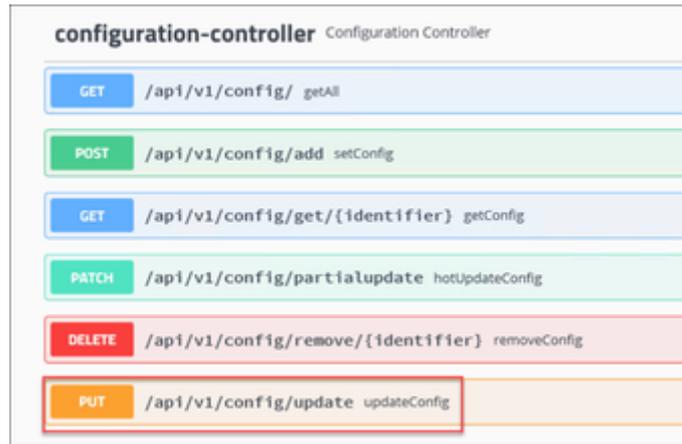
- Make a copy of the downloaded JSON file - so we have the original if required
- Edit the JSON file in any text editor by adjusting the Filter sections for each environment

```

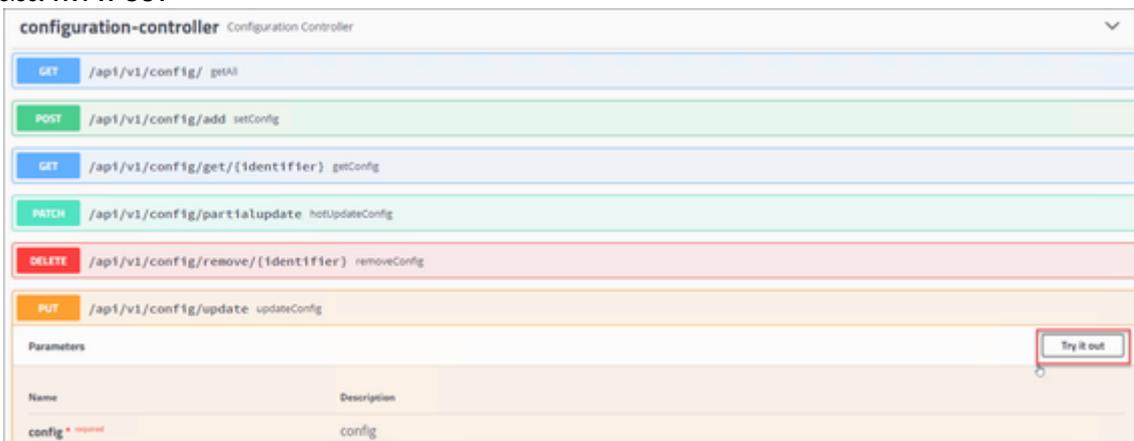
"debug": true,
"gaxConfiguration": {
  "hostname": "http://82.68.156.34",
  "password": "Tkeq1v363g3Lax3rcXqV6g\u003d\u003d",
  "port": 8040,
  "timeout": 10,
  "username": "default"
},
"oneEnvironmentName": "Genesys26",
"objectURL": "http://100.99.57.17/Spotlight/ConfigurationItem.aspx?ID\u003d\u003d\u0026Env\u003d\u003d",
"filters": {
  "FlexProp": {
    "excludeSectionsList": [
      "starts 'interaction-workspace' CfgPerson"
    ]
  }
},
"database": "Genesys26",
"password": "LA4GMR+gqx100wI9k8pb2Q\u003d\u003d",
"environmentID": 79,
"integratedSecurity": false,
"host": "100.99.57.17",
"initialize": false,
"additionalAction": "none"

```

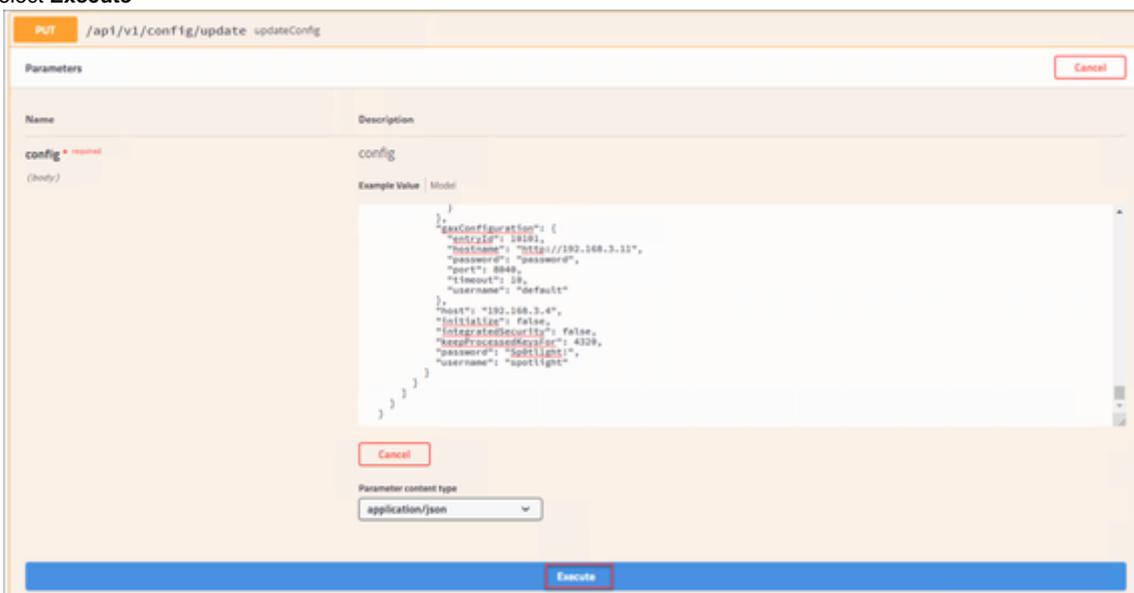
- Copy the full contents of the edited JSON file
- In **Swagger**, expand the **PUT** section



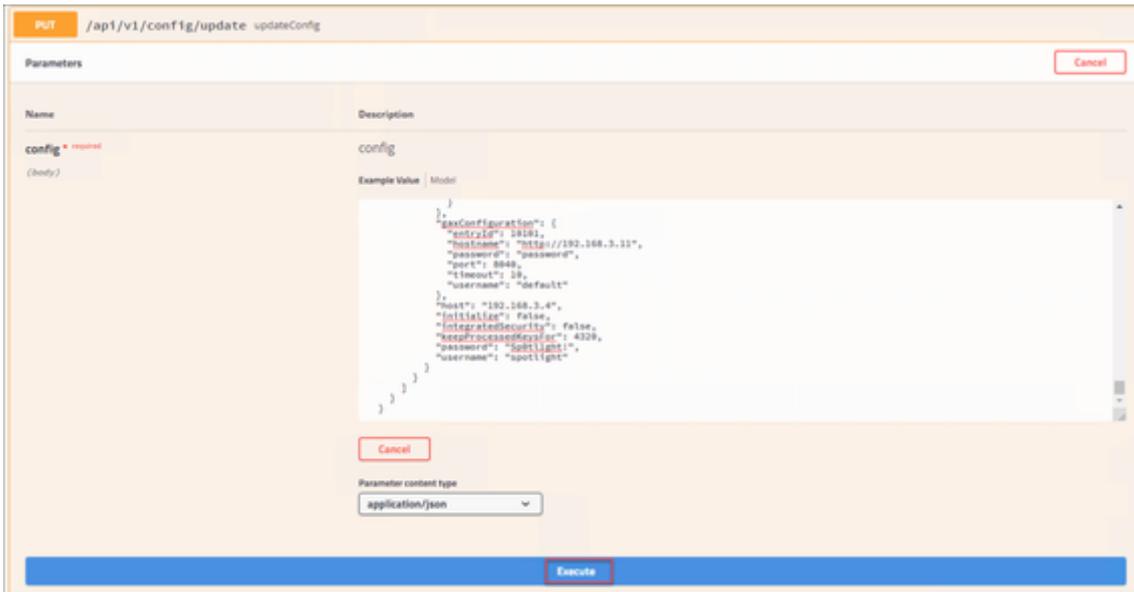
- Select **TRY IT OUT**



- Delete the contents of the request Body, including the square brackets
- Paste in the copied Json text
- Delete the square brackets at the start and end of the pasted text []
- Select **Execute**



- Verify the response received is **200**



- Restart the Spotlight-Consumer in services

Multiple Message Servers

Spotlight can be configured to use multiple message servers per Genesys environment. To do so

- Open the `messageserver-configuration.json` file located in the `Blackchair\SDP\Environment Name\GENAuditPRD\Config` folder
- Copy lines 3 to 41
- Enter a comma after the bracket on line 41
- Paste the copied text into line 42
- Adjust the copied text to reflect the settings of the second message server
- Close and save the file
- Restart the **GENAuditPRD** service

Baseline/Sync

The **Baseline/Sync** option is available within the Environment Wizard Plugin selection page and can be used to Baseline an environment (if this has not already be done), or to sync an environment. You may require to sync an environment for any reason which results in Spotlight not being able to receive change messages for that environment.

NB: This option can only be used for SDPFW environments currently

To Baseline an environment -

- On the **Baseline/Sync** page, select the **Environment**
- Select the **Action of Baseline**
- The values in the following fields will be pre-populated
 - Device ID
 - Cluster ID
 - CS URL

Resync/Baseline

Select an environment

#	Name	Type
2	Production	PureEngage
3	Development	PureEngage
4	Test	PureEngageSDPandGAX

Device Id:

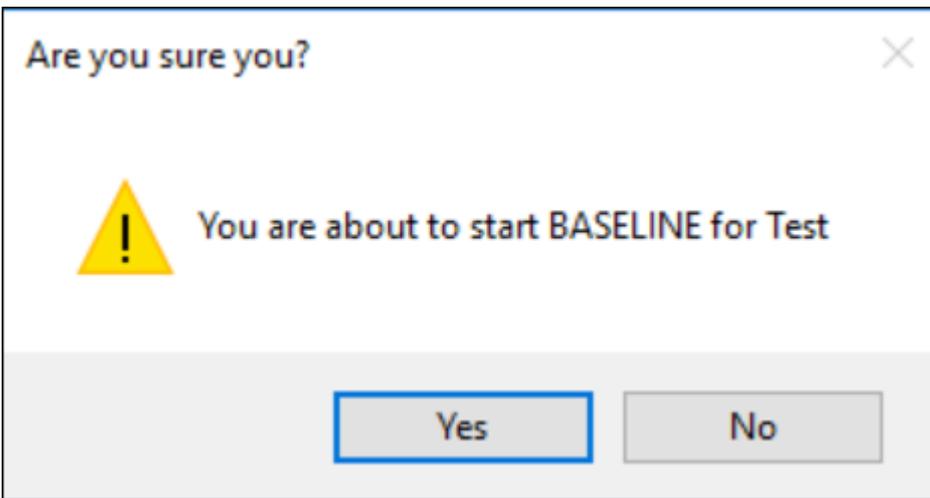
Cluster Id:

CS Url:

Commands:

Actions: Baseline Sync

- Select the **Command - Start**
- Confirm if you wish to proceed



- When the baseline starts - a pop up will be displayed 1st for CME
- Select **OK**

Response ×

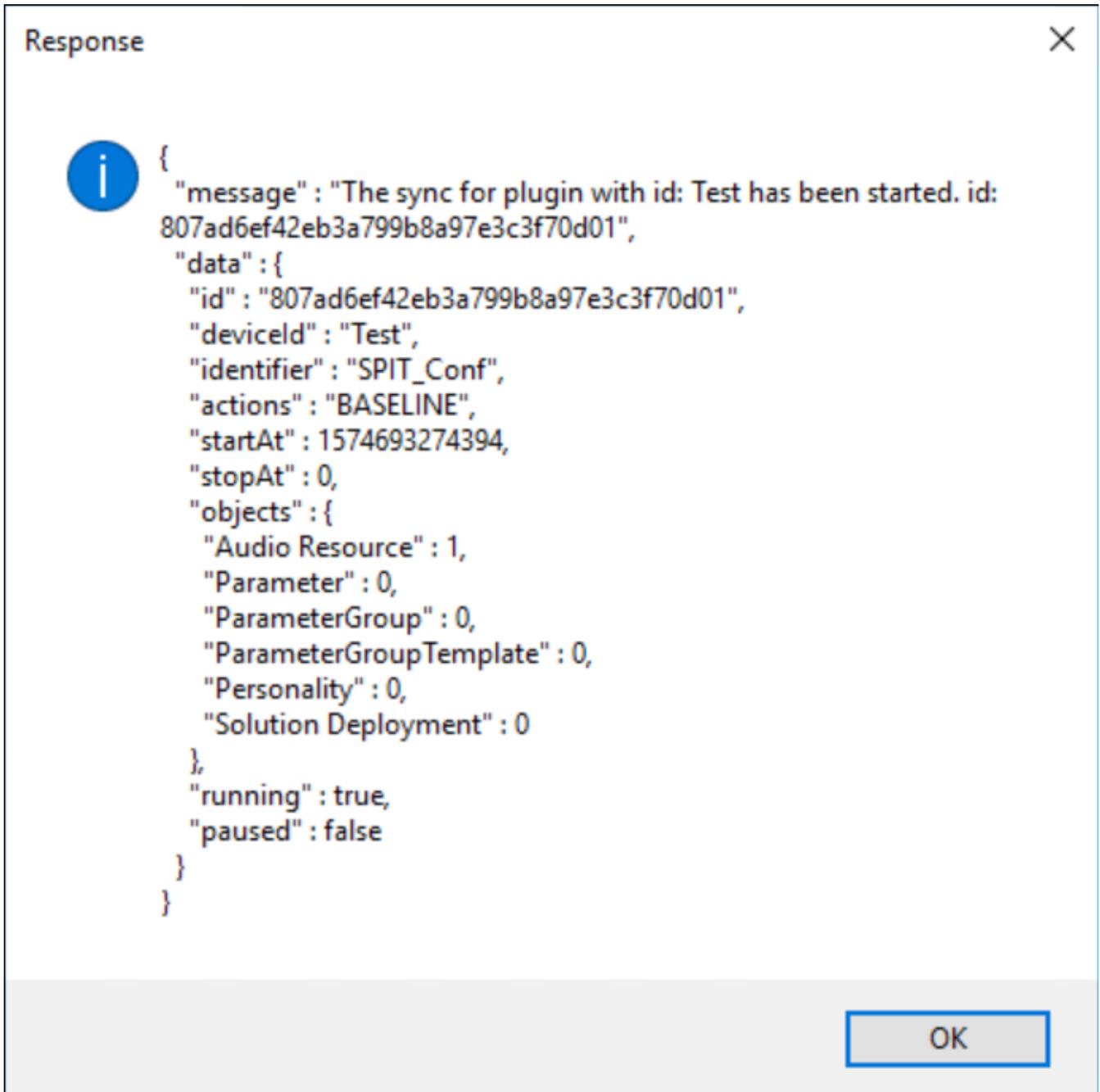
 {
 "message" : "The sync for plugin with id: Test has been started. id:
 2e9c44773a2d031d6406536abea5b910",
 "data" : {
 "id" : "2e9c44773a2d031d6406536abea5b910",
 "deviceId" : "Test",
 "identifier" : "SPIT_Conf",
 "actions" : "BASELINE",
 "startAt" : 1574693236672,
 "stopAt" : 0,
 "objects" : {
 "CFGDN" : 879,
 "CFGSwitch" : 6
 },
 "running" : true,
 "paused" : false
 }
}

- If GAX is installed on the environment, you will next receive a pop up asking if you wish to baseline this
- Select **Yes**

Are you sure you? ×

 GAX detected on Test do you want to start BASELINE for gax?

- A 2nd pop up will be displayed indicating that the GAX baseline has started
- Select **OK**



The process to Sync an environment is the same, except the **Action** selected should be **Sync**:

- On the **Baseline/Sync** page, select the **Environment**
- Select the **Action** of **Sync**
- Select the **Command - Start**

Whilst a **Baseline/Sync** is running, the following commands can be used

- Stop - will cancel the baseline.sync
- Pause - will pause the baseline/sync
- Resume - will resume a paused baseline/sync

Commands <input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Pause"/> <input type="button" value="Resume"/>	Actions <input checked="" type="radio"/> Baseline <input type="radio"/> Sync
--	--

NB: Currently there is no way to know if the baseline has been completed successfully from this screen. Selecting Cancel will not cancel the baseline, it will continue to run

Uninstall Environment

An **Uninstall Environment** option is available in the **Install** page of the wizard and can be used to remove an existing environment. This can be used to remove all components related to the environment, including

- sconfig database entries
- Spotlight Services
- Deployed files
- Log files - optional
- Spotlight database - optional

To remove an environment -

- On the **Environment Settings** page enter the name of the environment to uninstall in the **Environment Name** field
- Select **Uninstall** or select **Next**

- On the **Uninstall** page, select the **Environment**
- Optionally select **Delete Logs**
- Optionally select **Delete Database**
- Optionally select **Purge Queue** - to remove any change messages not yet processed
- Select **Proceed**

Uninstall

Select environment

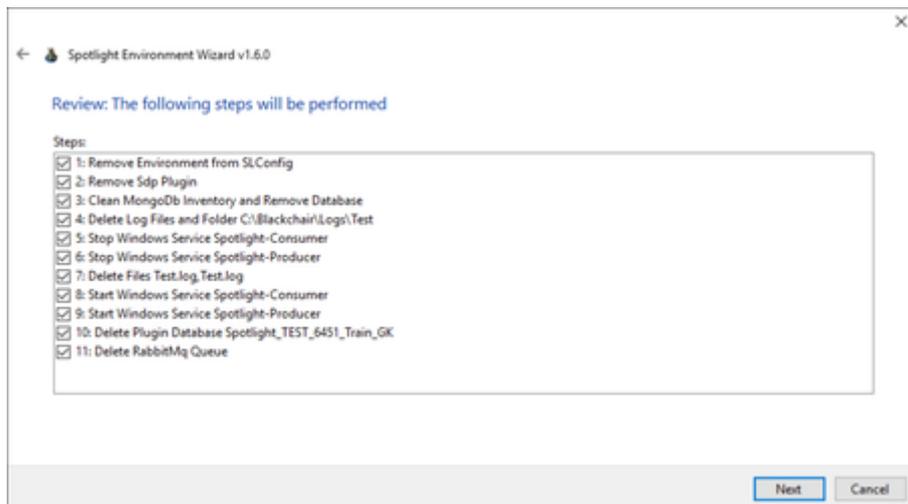
#	Name	Type
2	Production	PureEngage
3	Development	PureEngage
4	Test	PureEngageSDPandGAX

Uninstall Options

Delete Logs Delete Database Purge Queue

Proceed

- A page will be displayed showing the steps to be undertaken - the actions will depend on what type of environment is being uninstalled
- Select **Next**



During the removal of the Environment, the screen will display a progress of the steps being performed. Once complete, the screen will indicate that the environment has been removed successfully.

- Select **Next**
- Select **Go to Startup Page**

Troubleshooting

Issue Accessing UI

The following error is received when trying to access the UI

Resolution

The fix is to unblock each dll on the bin directory of the Spotlight UI.

In order to do that in one step please open an admin powershell session following command **gci c:\blachchair\IIS\Spotlight\bin | Unblock-File**

Configuration Sync Error

The following error is received when the Configuration Sync is started

Resolution

This can be caused if the Spotlight databases are on SQL 2008. To resolve, add the following line to the **Consumer application.properties** file and then restart the **Consumer** service

spring.jpa.properties.hibernate.dialect = org.hibernate.dialect.SQLServer2008Dialect
