



Application Notes for Blackchair Spotlight Audit and Release Management V6 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® System Manager R8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Spotlight Audit and Release Management from Blackchair with Avaya Aura® Communication Manager, using the System Management Service (SMS) connection on Avaya Aura® Application Enablement Services, and Avaya Aura® System Manager to gain access to information on both System Manager and Session Manager. Blackchair Spotlight is capable of monitoring changes that are made in each of the three platforms as well as making changes on Avaya Aura® Communication Manager and Avaya Aura® System Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to integrate Spotlight Audit and Release Management V6 from Blackchair with Avaya Aura® System Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication Manager R8.1 using Avaya Aura® Application Enablement Services R8.1.

Blackchair Spotlight Audit and Release Management (Spotlight) makes use of the following three connections to the Avaya Aura® platform to gain read/write access to Avaya Aura® Communication Manager and Avaya Aura® System Manager and for read only access on Avaya Aura® Session Manager.

1. Spotlight connects to Avaya Aura® Communication Manager using the System Management Service (SMS) Software Development Toolkit (SDK) on Avaya Aura® Application Enablement Services R8.1.
2. Spotlight connects to Avaya Aura® System Manager using the Routing Web Service SDK on Avaya Aura® System Manager.
3. Spotlight connects to Avaya Aura® Session Manager using a Secure Shell (SSH) connection to Avaya Aura® System Manager.

System Management Service (SMS) is a web service that exposes selected management features of Communication Manager. SMS enables SOAP clients to display, list, add, change and remove specific managed objects on Communication Manager. SMS allows programmatic access, via a standard protocol (SOAP), to functionality that is otherwise only accessible via a proprietary low-level protocol (OSSl) or terminal emulation via system administration (SAT) forms. Spotlight utilises the SMS web service to display changes that occur on Communication Manager.

The Routing Web Services API Programming interface is one of the Web Services comprising the System Manager Web Service. The Routing Web Service provides programmatic access to all routing administration data. The service provides access for adding, modifying, and deleting any of the routing data that may be modified using the System Manager GUI. The Web Service is designed to use without an SDK. There is however a Zip file which aids developers by providing JAXB mappings between Routing data model classes and JSON or XML content. It assumes use of one of the Java REST client frameworks such as Oracle Jersey, JBoss RESTEasy, Apache CXF, or HTTPClient.

The SSH connection to System Manager is used to gain access to the log files in the following /var/log/Avaya/mgmt/nrp folder, which provides data on changes to Session Manager configuration. A user is created on System Manager which has access to that folder. This user is used by Spotlight to read the information contained in these log files.

Note: Spotlight may connect to the Avaya Aura® platform or may be used in a Communication Manager only environment where there is an absence of System Manager and Session Manager. This would rarely be the case for a connection to either System Manager or Session Manager only. With this in mind all, three connections are described in these Application Notes.

2. General Test Approach and Test Results

Spotlight was installed on a Microsoft Windows 2016 Server virtual server, with a web browser used to access the Spotlight GUI. Changes were made manually on Communication Manager and System Manager with Spotlight giving the user an option to see both the changed value and the initial value and also allowing the user to revert back to the original value. Spotlight was also used to make changes on both Communication Manager and Session Manager. These changes published using Spotlight were then verified on System Manager and Communication Manager. The information audit on Session Manager was verified on System Manager.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Spotlight made use of a TLS connection to the AES SMS SDK and a HTTPS connection to the System Manager Routing Web Service with a Secure Shell connection to System Manager.

2.1. Interoperability Compliance Testing

The test cases that were performed were conducted according to the fields or service models described on the different SDKs. A list of the service models tested is shown in the **Appendix** of these Application Notes.

The connection to Communication Manager was tested by comparing the audit received on Spotlight with the information on Communication Manager that was read using the System Access Terminal (SAT) or a similar application connected to Communication Manager. Spotlight then added and removed various service models such as Stations, VDN's and Agents.

The connection to System Manager was tested again by comparing the audit received on Spotlight with the information viewed on System Manager. Spotlight then added and removed various service models such as Domains, SIP Entities and Adaptations.

The connection to Session Manager was tested by observing the audit received by Spotlight and comparing that to the information on Session Manager displayed on System Manager.

2.2. Test Results

Because of the nature of the testing, not every single service model change in Communication Manager and System Manager was tested. A broad slice of testing across a range of fields was conducted to prove that compliance was achieved.

The following observations were noted on the connection to Communication Manager using the AES SMS SDK.

- Spotlight allows the Trunk Group number to be changed, which is not supported by the SDK, and causes an error. Blackchair are aware of the issue and will remove the option.
- Spotlight allows the CTI Extension number to be changed, which is not supported by the SDK, and causes an error. Blackchair are aware of the issue and will remove the option.
- When making changes to the Class of Restriction (COR) there is some confusion as there is an option to change the COR number field, which actually enables changes to a different COR, than the initial one that was indicated. Blackchair are aware of this and will amend how this is presented to the user.
- Changes to the Class of Service (COS) name and identifier is not supported by the SDK and failed. Blackchair will remove the fields to ensure that the COS cannot be overwritten only copied from one system to another.

The following observations were noted on the connection to System Manager.

- There are some fields on the Entity Link that cannot be changed that are listed on Spotlight. Blackchair are aware of the issue and will remove the option.
- There are some fields on the Routing Policy that cannot be changed that are listed on Spotlight. Blackchair are aware of the issue and will remove the option.

2.3. Support

For technical support on Spotlight, contact Blackchair as shown below.

- Web: <https://theblackchair.com/contact-us/>
- Tel: +44 845 456 6751
- Email: enquiries@theblackchair.com

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Spotlight server was placed on the Avaya telephony LAN. The SMS SDK on the AES provides the Spotlight server a history of moves and changes from Communication Manager as well as the ability make changes on Communication Manager. The HTTPS connection to the Routing Web Service on System Manager facilitates similar actions where an audit of moves and changes are logged as well as the ability to make changes on System Manager. The SSH connection to System Manager allows the audit of certain field on Session Manager (listed in the **Appendix** of these Application Notes).

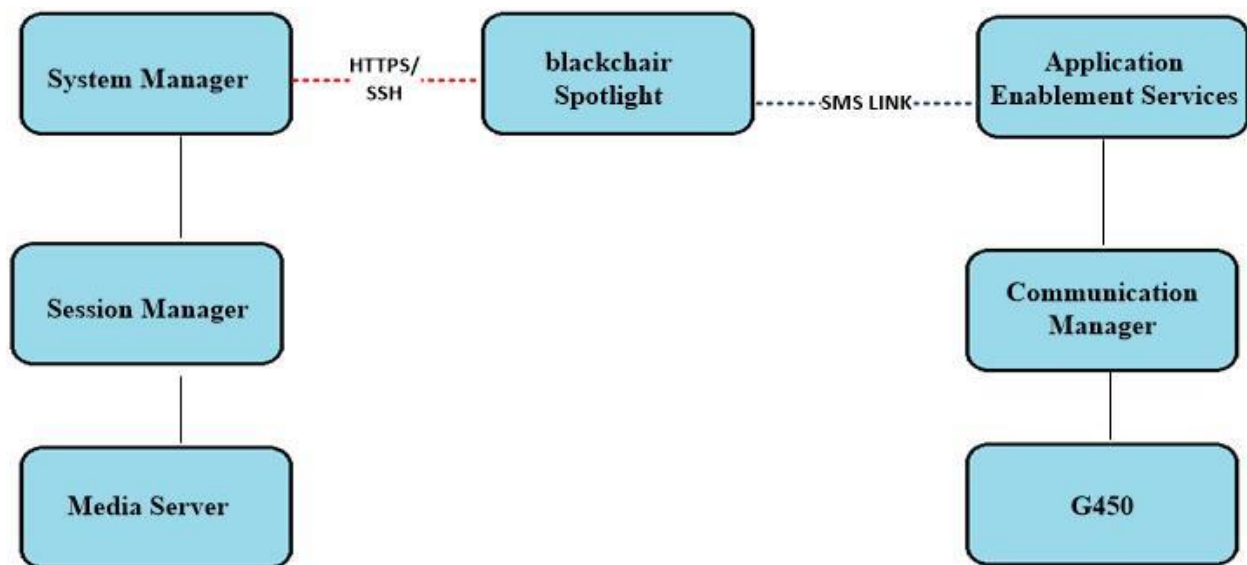


Figure 1: Network solution of Blackchair Spotlight V6 and Avaya Aura® R8.1

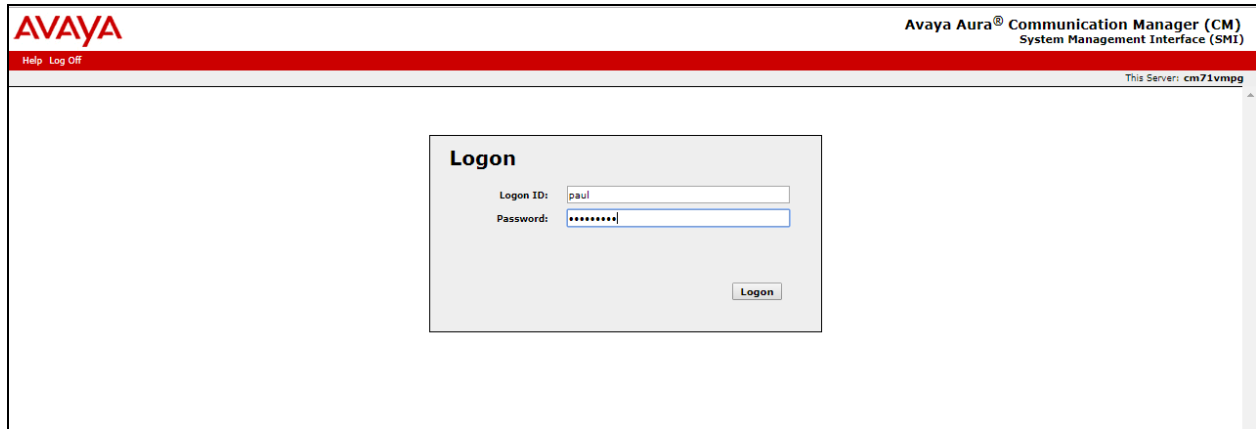
4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided.

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.079880
Avaya Aura® Session Manager	Session Manager R8.1 Build No. – 8.1.0.0.810007
Avaya Aura® Communication Manager	R8.1.0.1.0 – SP1 R018x.01.0.890.0 Update ID 01.0.890.0-25393
Avaya Aura® Media Server	Appliance Version R8.0.0.12 Media Server 8.0.0.169 Element Manager 8.0.0.169
Avaya Aura® Application Enablement Services	8.1.0.0.0.9-1
Blackchair Equipment	Software / Firmware Version
Blackchair Spotlight running on a virtual server with Windows 2016 Server	V6.45

5. Configure Avaya Aura® Communication Manager

A new user for a connection from Spotlight is created on Communication Manager. Open a browser session to Communication Manager and log in with the appropriate credentials as shown below.



AVAYA

Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Help Log Off

This Server: cm71vmpg

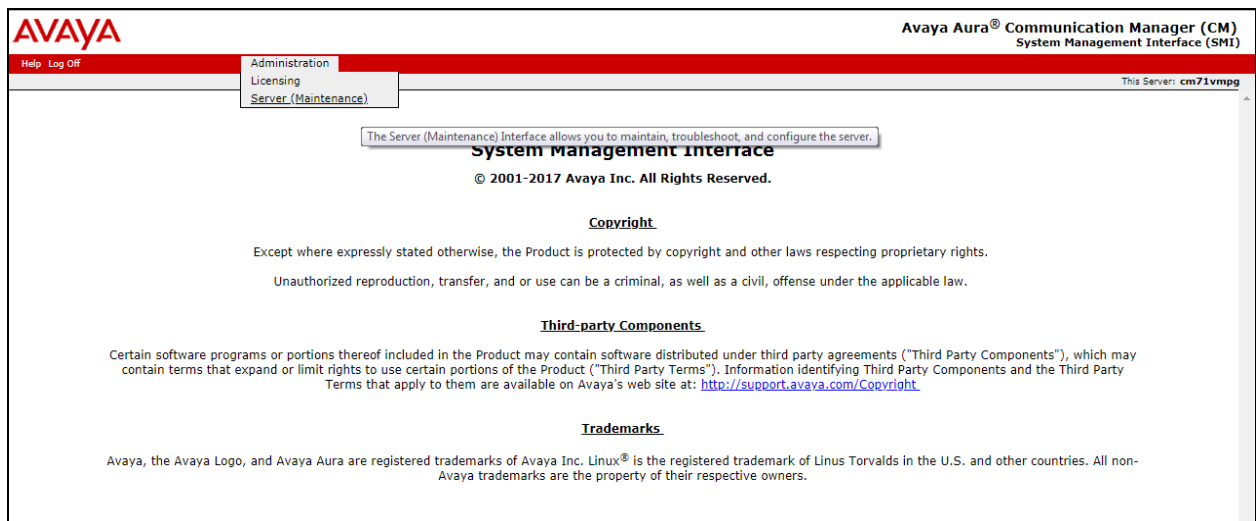
Logon

Logon ID: paul

Password: *****

Logon

Navigate to **Server (Maintenance)** as shown below.



AVAYA

Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Help Log Off

Administration
Licensing
Server (Maintenance)

This Server: cm71vmpg

The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.

System Management Interface

© 2001-2017 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information Identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: <http://support.avaya.com/Copyright>.

Trademarks

Avaya, the Avaya Logo, and Avaya Aura are registered trademarks of Avaya Inc. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All non-Avaya trademarks are the property of their respective owners.

In the left window select **Security**→**Administrator Accounts**. In the main window, select **Add Login**. For the compliance testing **Privileged Administrator** was chosen, but any account with privileges to use SAT is all that is required in order for a Spotlight user to read the fields in Communication Manager. Select **Submit** when done.

The screenshot shows the Avaya Aura Communication System Management interface. The top navigation bar includes 'Help', 'Log Off', 'Administration', and 'Upgrade'. The left sidebar lists various system management tasks, with 'Security' and 'Administrator Accounts' highlighted. The main content area is titled 'Administrator Accounts' and contains the following text: 'The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups. Select Action:'. Below this, there are several radio button options: 'Add Login' (selected), 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. There are also fields for 'Change Login', 'Remove Login', 'Lock/Unlock Login', and 'Add Group', each with a 'Select Login' dropdown. At the bottom, there are 'Submit' and 'Help' buttons.

Enter the **Login name** and a suitable **password**. Click on **Submit** when done.

The screenshot shows the Avaya Aura Communication System Management interface. The top navigation bar includes 'Help', 'Log Off', 'Administration', and 'Upgrade'. The left sidebar lists various system management tasks, with 'Alarms', 'SNMP', 'Diagnostics', 'Server', 'Server Configuration', and 'Server Upgrades' highlighted. The main content area is titled 'Administrator Accounts -- Add Login: Privileged Administrator' and contains the following text: 'This page allows you to add a login that is a member of the SUSERS group. This login has the greatest access privileges in the system next to root.' Below this, there are several form fields: 'Login name' (text input), 'Primary group' (text input), 'Additional groups (profile)' (dropdown menu), 'Linux shell' (text input), 'Home directory' (text input), 'Lock this account' (checkbox), 'SAT Limit' (dropdown menu), 'Date after which account is disabled-blank to ignore (YYYY-MM-DD)' (text input), 'Enter password' (password input), 'Re-enter password' (password input), and 'Force password change on next login' (radio buttons). At the bottom, there are 'Submit', 'Cancel', and 'Help' buttons.

6. Configure Avaya Aura® Application Enablement Services

Although the Spotlight server's connection to the Avaya solution is through the SMS SDK on the AES, there is no configuration required on the AES server. The username and password utilised by Spotlight is that which was created above in **Section 5**.

7. Configure Avaya Aura® System Manager

There are two connections made to System Manager.

1. A HTTPS connection to the Routing Web Service. This will require that the web username and password is setup for a Spotlight user to be able to gain access to the Routing section on System Manager. For compliance testing, the 'Admin' user was used. However, a unique user can be created for this purpose.
2. A Secure Shell (SSH) connection to System Manager. This requires that a user is created on Linux for Spotlight.

7.1. Configure Connection to Routing Web Service

User is created on System Manager to facilitate the connection to the Routing Web Service. Log into System Manager using the appropriate credentials to create a new user.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

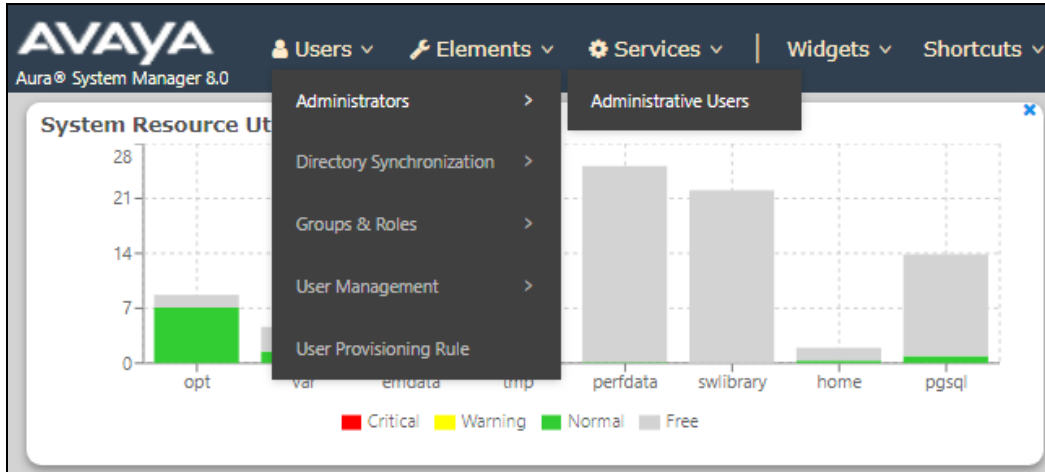
User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

Navigate to **Users** → **Administrators** → **Administrative Users**.



Click on **Add**, highlighted below to add a new user.

The screenshot shows the 'Administrative Users' page in the AVAYA Aura System Manager 8.0 interface. The 'Add' button is highlighted in red. Below the table, there is a list of administrative users with their details.

User ID	Name	Roles	Type	Account
admin	Default security administrator	System Administrator	Local	Enabled
avaya_services_administrator	avaya_services_administrator	Avaya Services Administrator	External	Enabled
avaya_services_maintenance_and_support	avaya_services_maintenance_and_support	Avaya Services Maintenance and Support	External	Enabled
craft	craft	Avaya Services Maintenance and Support	External	Enabled
init	init	System Administrator	External	Enabled
mentolpro	Mentol Pro	MentolPro	Local	Enabled

Enter the new **User ID** and a **Temporary password**. Click on **Commit and Continue**.

The screenshot shows the 'Add New Administrative User' form in the AVAYA Aura System Manager 8.0 interface. The form is titled 'Step1: Identify the new user.' and contains fields for 'User ID', 'Authentication Type', 'Full Name', 'E-Mail', 'Temporary password', and 'Re-enter password'. The 'Add' button is highlighted in red.

Host Name: smgr80vmpg.devconnect.local **User Name:** admin

Add New Administrative User

Step1: Identify the new user.
Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.

* User ID: (1-31) (Allowed characters are a-z, A-Z, 0-9, ., -, and _)

Authentication Type: ☒ Local ☐ External

* Full Name:

E-Mail:

The user will receive notifications on this E-Mail address.

* Temporary password:

* Re-enter password:

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9[()<>./,=][*_*@%&+*?*\; The length of your password must be at least 5 characters.

Note: The new user must be saved before you may assign roles.

* Required

The following screen is then shown where a role is assigned to the new user. Two roles are added that being **Session Manager and Routing Administrator** and **Session Manager and Routing Auditor**. This will allow this user access to the Routing Web Service. Click on **Commit** to save the user.

Note: For compliance testing the ‘Admin’ user was used.

Host Name: smgr80vmmpg.devconnect.local User Name: admin

Add New Administrative User

Step2: Assign Role(s)
Selected roles authorize the user for associated features and element permissions.

Roles	Description
<input type="checkbox"/> 28 ServiceTechnician	The system assigns the role to the service personnel when the service personnel connects to customer systems through the e-token. The Service Technician role has limited privileges as compared to the Avaya Services Administrator role.
<input checked="" type="checkbox"/> 29 Session Manager and Routing Administrator	Session Manager and Routing Administrator
<input checked="" type="checkbox"/> 30 Session Manager and Routing Auditor	Session Manager and Routing Auditor
<input type="checkbox"/> 31 SIPAS Auditor	Gives read-only access to all SIP Foundation server management functionality.
<input type="checkbox"/> 32 SIPAS Security Administrator	Gives access to the security features provided by the SIP Foundation server. For example, Security Extension.
<input type="checkbox"/> 33 SIPAS System Administrator	Gives read and write access to all the SIP Foundation server management functionality.
<input type="checkbox"/> 34 System Administrator	Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules

Commit **Cancel**

This new user can then be verified as per **Section 9.2.1**.

7.2. Configure the Secure Shell connection

Log into System Manager using an application such as PuTTY to open an SSH session. Once logged in under “root” or some other user with administrator privileges run the command ‘useradd xxxx’, where xxxx is the new user name. For example, the command **useradd Blackchair** was run to add the user Blackchair. Once added, the command **passwd Blackchair** was run to assign a password to the user Blackchair. With this username and password setup this user will have access to the logfiles at **/var/log/Avaya/mgmt/nrp**. These log files provide information on the changes performed to certain Session Manager fields outlined in the **Appendix**.

8. Configure Blackchair Spotlight Audit and Release Management

The installation and configuration of the Spotlight server from Blackchair is performed by a Blackchair engineer and is therefore outside the scope of these Application Notes. The information for support for Blackchair can be found in **Section 2.3**.

9. Verification Steps

This section provides the tests that can be performed to verify that Blackchair Spotlight has successfully connected with the Avaya solution.

9.1. Verify Connection to Avaya Aura® Application Enablement Services

AES contains a test web page that can be used to test the connection to Communication Manager using the SMS service.

Open a browser session to **https://<AEServerIP>/smsxml/smsxml_test.php**. The web page shown below should be opened. Enter the appropriate **CM Login ID** and **Password** and enter some **Request Parameters** as shown below, where the “list station” command is entered. Click on **Submit Request** highlighted below.

The screenshot shows a web browser window with the URL https://10.10.40.43/smsxml/smsxml_test.php. The page title is "XML Based - Web Service Request Form" and the Avaya logo is in the top left. The form is divided into several sections:

- SMS Resources**: A sidebar menu with links to [Model Documentation](#), [Model Doc \(No-Frames\)](#), [SMS XML WSDL](#), and [SMS XML Schema](#).
- Connection Information**: Fields for CM Login ID (blackchair@10.10.40.4), Password (masked), SMS Host (https://10.10.40.43), and SOAP Request Timeout (Seconds) (30).
- Session Recording**: Checkboxes for "Record SMS Request" and "Record Result Data", and buttons for "Get Record" and "Clear Record".
- Request Parameters**: A section for defining request parameters. It includes a table with columns for Model, Field, Value, and Position. The "Model" dropdown is set to "Station". The "Field" dropdown is set to "...". The "Value" field is empty. The "Position" field is empty. There is a "Use For ArrayType Fields" checkbox and an "ADD Field" button.
- ModelFields - Generated XML**: A section for generating XML. It includes a note: "Note: You may also manually enter valid XML or modify the populated data, then click Update XML". There is an "Update XML" button and a text area containing the following XML:

```
<?xml version="1.0"?>
<modelFields>
  <Station/>
</modelFields>
```
- Submit Request**: A button highlighted with a red box, next to a "Release" button.
- Last Request Response**: A section for displaying the response. It includes a "Session ID" field and a "Duplicate Session" link.

The **Response** at the bottom of the screen should return data as shown below.

ModelFields

Model

Station

Field

...

Value

Position

Use For ArrayType Fields

ADD Field

Operation

list

Objectname

Qualifier

ModelFields - Generated XML

Note: You may also manually enter valid XML or modify the populated data, then click **Update XML**

Update XML

```
<?xml version="1.0"?>
<modelFields>
  <Station/>
</modelFields>
```

Submit Request

Release

Last Request Response

Session ID

f12229f2a6574814c43cc7ed756650df

[Duplicate Session](#)

Response

```
<Extension>1000</Extension>
<Type>9608</Type>
<Port>S00000</Port>
<Name>4000, H323User</Name>
<Coverage_Path_1>1</Coverage_Path_1>
<Coverage_Path_2/>
<Hunt_to_Station/>
<COR>1</COR>
<COS>1</COS>
```

9.2. Verify Connection to System Manager

There are two connections to System Manager that can be verified, these are the connection to the web interface and the Secure Shell connection.

9.2.1. Verify Connection to Routing Web Service

Open a web browser to System Manager and log in using the credentials setup from **Section 7.1**. This user should be able to log in provided that the password was changed upon the initial login which is not shown here.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

User ID:

Password:

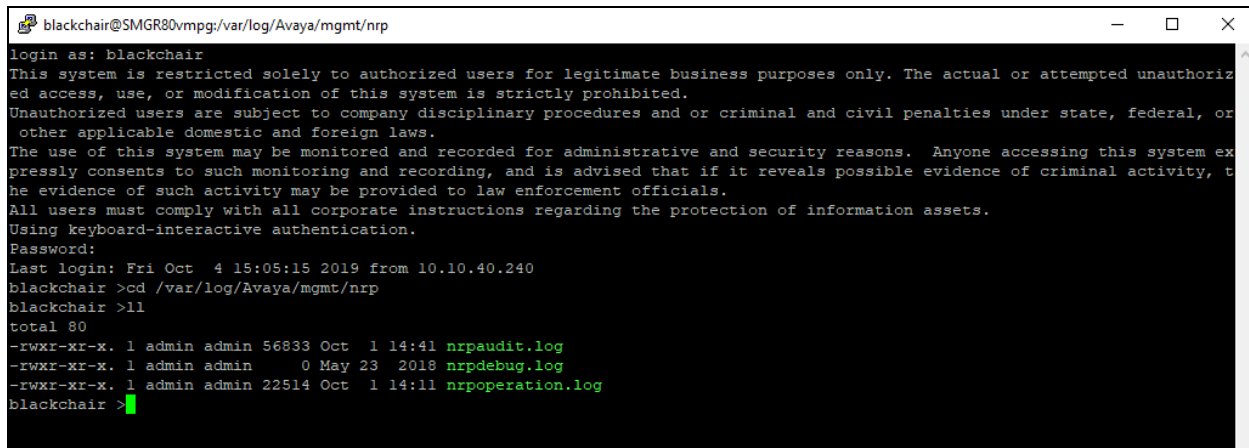
[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

Once this user is logged in correctly, the following screen is shown, where access to **Routing** and all its elements is possible. This verifies that this user can access the Web Routing Service.

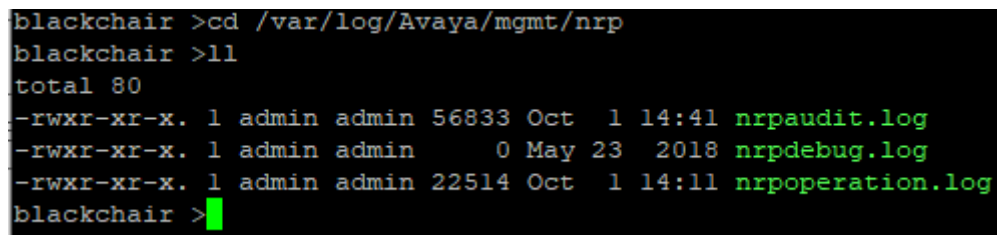
9.2.2. Verify Secure Shell Connection

The Secure Shell connection can be verified by connecting to System Manager using the username and password setup in **Section 7.2**. Navigate to the folder **/var/log/Avaya/mgmt/nrp**, list the log files contained in the folder using the command **ll**.

A terminal window titled 'blackchair@SMGR80vmpg:/var/log/Avaya/mgmt/nrp'. The user 'blackchair' logs in and sees a system warning about unauthorized access. After password authentication, the user enters 'cd /var/log/Avaya/mgmt/nrp' and then 'll'. The output shows three log files: nrpaudit.log, nrpdebug.log, and nrpoperation.log, all with permissions -rwxr-xr-x and owned by admin:admin.

```
blackchair@SMGR80vmpg:/var/log/Avaya/mgmt/nrp
login as: blackchair
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.
Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.
All users must comply with all corporate instructions regarding the protection of information assets.
Using keyboard-interactive authentication.
Password:
Last login: Fri Oct  4 15:05:15 2019 from 10.10.40.240
blackchair >cd /var/log/Avaya/mgmt/nrp
blackchair >ll
total 80
-rwxr-xr-x. 1 admin admin 56833 Oct  1 14:41 nrpaudit.log
-rwxr-xr-x. 1 admin admin    0 May 23  2018 nrpdebug.log
-rwxr-xr-x. 1 admin admin 22514 Oct  1 14:11 nrpoperation.log
blackchair >
```

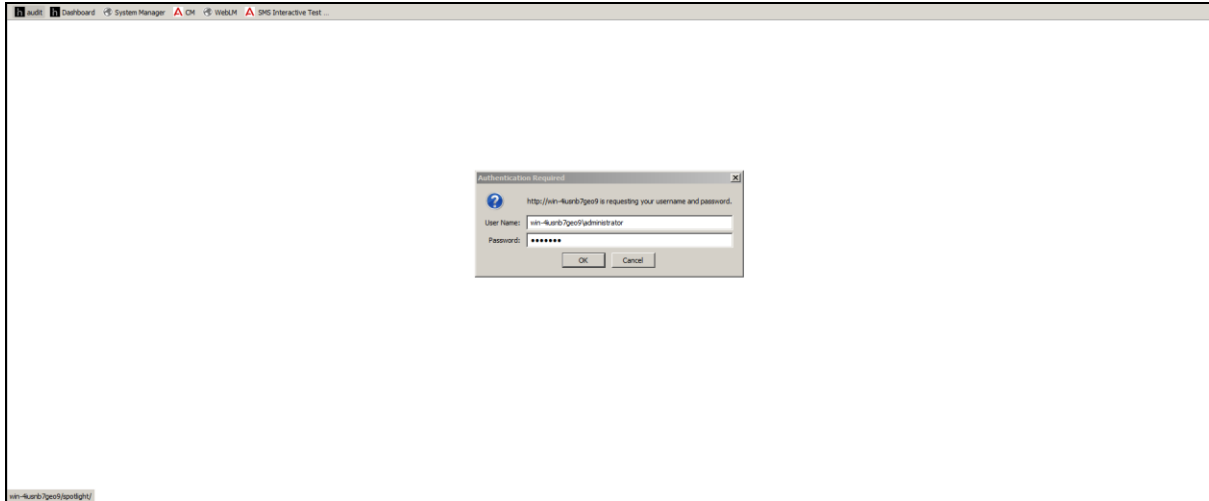
A closer shot of the commands and log files as shown below. With access to these log files this user can obtain the necessary information on Session Manager.

A close-up terminal screenshot showing the 'll' command output in the /var/log/Avaya/mgmt/nrp directory. It lists three log files with their permissions, ownership, size, and timestamps.

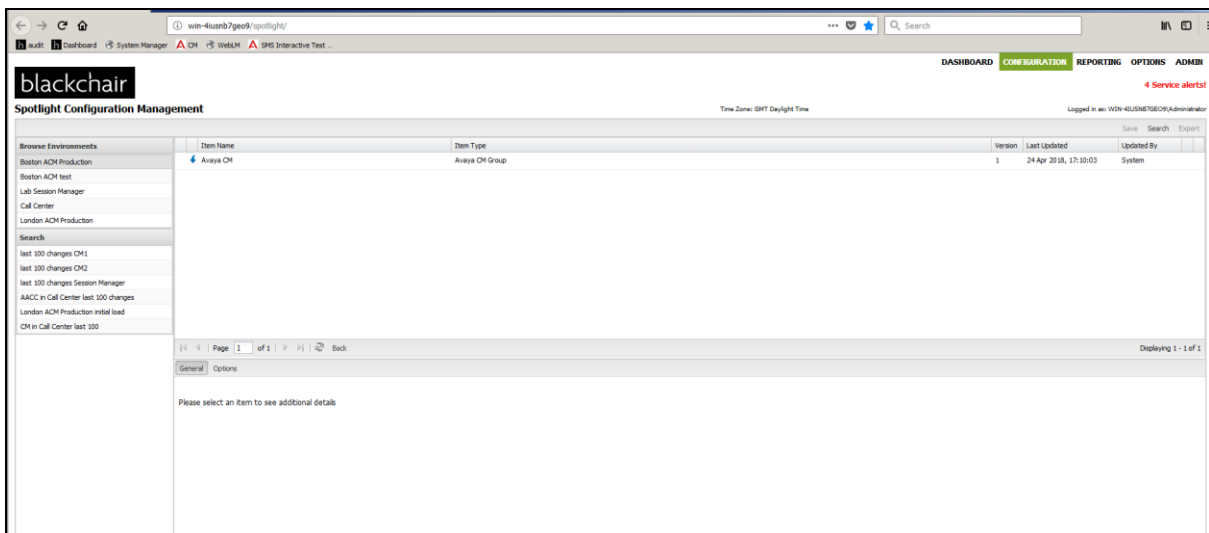
```
blackchair >cd /var/log/Avaya/mgmt/nrp
blackchair >ll
total 80
-rwxr-xr-x. 1 admin admin 56833 Oct  1 14:41 nrpaudit.log
-rwxr-xr-x. 1 admin admin    0 May 23  2018 nrpdebug.log
-rwxr-xr-x. 1 admin admin 22514 Oct  1 14:11 nrpoperation.log
blackchair >
```

9.3. Verify Changes Shown on Blackchair Spotlight

Open a web browser to the Spotlight server **http://<ServerAddress>/spotlight**. Enter the Windows credentials, then click on **OK** as shown below.



In the **Browse Environments** left pane, click on the appropriate environment and then in the main window click on the appropriate **Item**.



The main page shows various items that can be chosen to display. **Agent Login Status** is clicked on below and this displays the status of the agents configured on the system as shown below.

The screenshot shows the 'Spotlight Configuration Management' interface. The 'Agent Login Status' item is selected in the left sidebar. The main table displays the configuration for 'Agent Login Status'.

Item Name	Item Type	Version	Last Updated	Updated By
Agent Login Status	Agent Login Status Group	1	24 Apr 2018, 17:10:04	System

Below the table, there is a 'General' tab and a 'Filter' section. The 'General' tab shows the following details:

Date Retrieved	Login ID	Name	Extension	Skill Number 1	Skill Number 2	Skill Number 3	Skill Number 4	Skill Number 5	Skill Number 6	Skill Number 7	Skill Number 8	Updated By
Apr 25, 2018 10:20:15	4462	Dave EMC Agt2	4001									System
Apr 25, 2018 10:20:15	4461	Paul EMC Agt1	4000									System
Apr 25, 2018 10:08:05	4462	Dave EMC Agt2	4001									System
Apr 25, 2018 10:08:05	4461	Paul EMC Agt1	4000									System

Another item can be chosen such as **Announcement**, as is shown below. The information on that announcement chosen is displayed.

The screenshot shows the 'Spotlight Configuration Management' interface. The 'Announcement' item is selected in the left sidebar. The main table displays the configuration for 'Announcement'.

Item Name	Item Type	Version	Last Updated	Updated By
Extension 4700	Announcement	1	24 Apr 2018, 18:45:04	System

Below the table, there is a 'General' tab and an 'Options' section. The 'General' tab shows the following details:

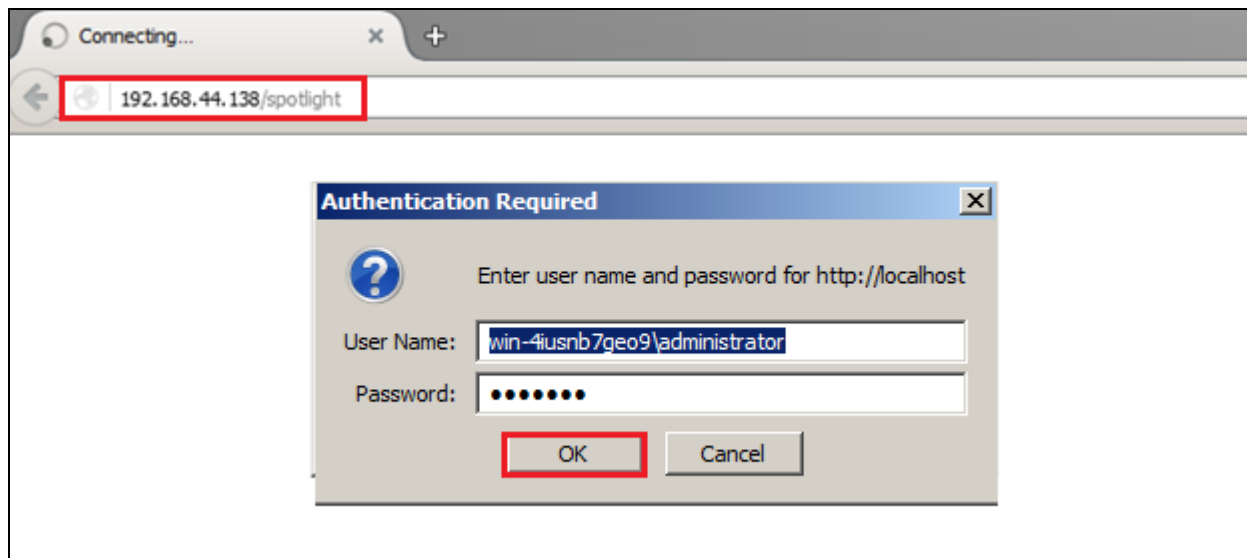
Property	Value
Name	Extension 4700
Version	1
Last Updated By	System
Updated Date	24 Apr 2018, 18:45:04
Announcement Type	Integrated
Name	PGTEXT1
Num Files	
Board	001V9
Announcement Number	

9.4. Verify Spotlight Connection to Avaya Aura® Communication Manager

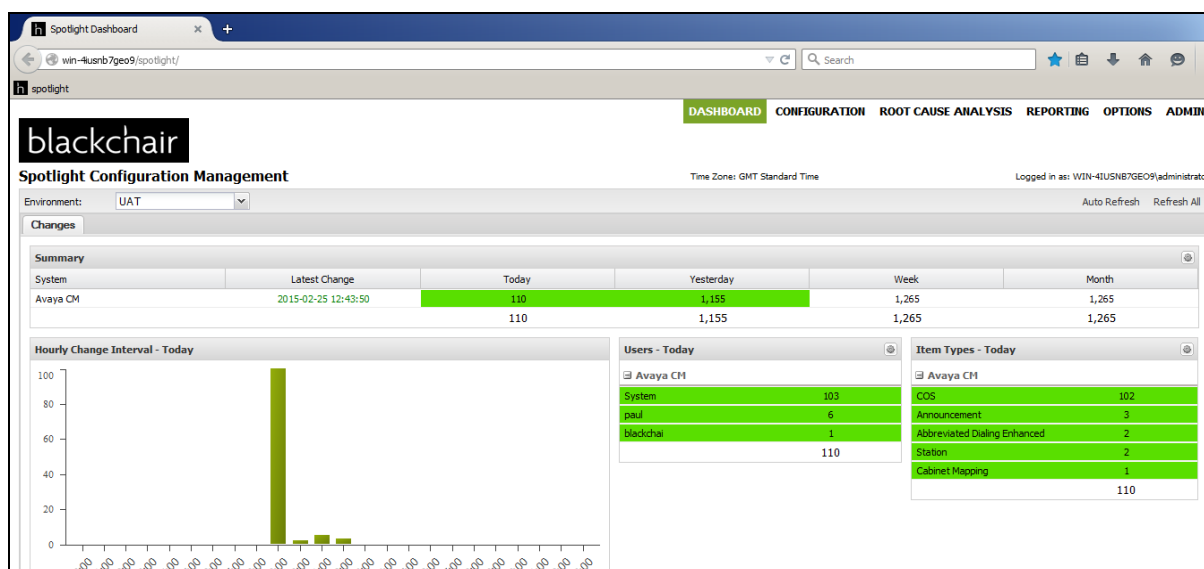
This section will outline the steps necessary to place a configuration object into a Spotlight package, tailor the package, test the package and publish this package into a different Communication Manager environment.

Open a web browser to the Spotlight Release Management server

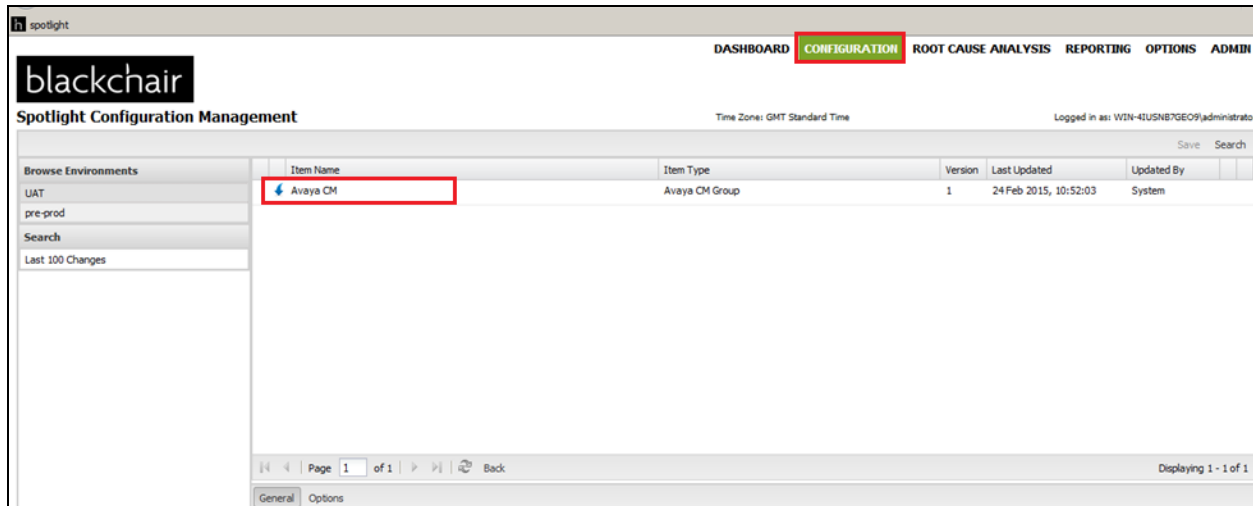
[<http://<IPAddressSpotlightRMServer>/spotlight>] and enter the appropriate credentials, this will be the windows domain\username and password. Spotlight Release Management uses pass-through windows authentication. Click on **OK** as shown below.



Once logged in the screen below is presented to the user.



Select the **CONFIGURATION** tab from the top of the page. Double click on the **Avaya CM** item highlighted; note this may be a different name depending on the system.

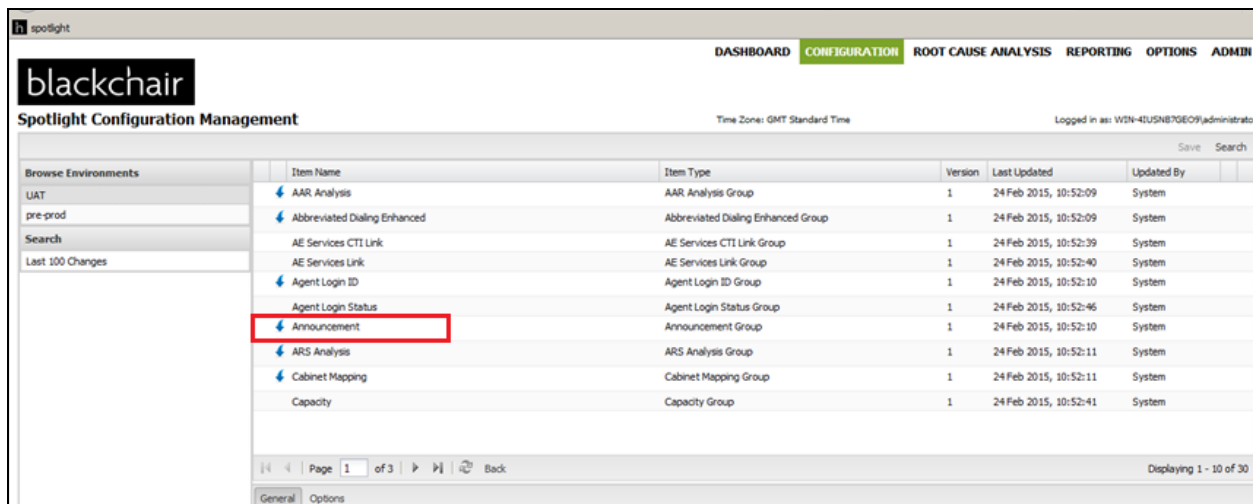


The screenshot shows the 'Spotlight Configuration Management' interface. The top navigation bar includes 'DASHBOARD', 'CONFIGURATION' (highlighted), 'ROOT CAUSE ANALYSIS', 'REPORTING', 'OPTIONS', and 'ADMIN'. The left sidebar shows 'Browse Environments' with options like 'UAT', 'pre-prod', 'Search', and 'Last 100 Changes'. The main table lists configuration items. The 'Avaya CM' item is highlighted with a red box.

Item Name	Item Type	Version	Last Updated	Updated By
Avaya CM	Avaya CM Group	1	24 Feb 2015, 10:52:03	System

Page 1 of 1. Displaying 1 - 1 of 1.

Double-click on which ever item needs to be changed. In the example shown below, this item is **Announcement**. The following steps will show an Announcement being copied from one Communication Manager system to another.



The screenshot shows the 'Spotlight Configuration Management' interface. The top navigation bar includes 'DASHBOARD', 'CONFIGURATION' (highlighted), 'ROOT CAUSE ANALYSIS', 'REPORTING', 'OPTIONS', and 'ADMIN'. The left sidebar shows 'Browse Environments' with options like 'UAT', 'pre-prod', 'Search', and 'Last 100 Changes'. The main table lists configuration items. The 'Announcement' item is highlighted with a red box.

Item Name	Item Type	Version	Last Updated	Updated By
AAR Analysis	AAR Analysis Group	1	24 Feb 2015, 10:52:09	System
Abbreviated Dialing Enhanced	Abbreviated Dialing Enhanced Group	1	24 Feb 2015, 10:52:09	System
AE Services CTI Link	AE Services CTI Link Group	1	24 Feb 2015, 10:52:39	System
AE Services Link	AE Services Link Group	1	24 Feb 2015, 10:52:40	System
Agent Login ID	Agent Login ID Group	1	24 Feb 2015, 10:52:10	System
Agent Login Status	Agent Login Status Group	1	24 Feb 2015, 10:52:46	System
Announcement	Announcement Group	1	24 Feb 2015, 10:52:10	System
ARS Analysis	ARS Analysis Group	1	24 Feb 2015, 10:52:11	System
Cabinet Mapping	Cabinet Mapping Group	1	24 Feb 2015, 10:52:11	System
Capacity	Capacity Group	1	24 Feb 2015, 10:52:41	System

Page 1 of 3. Displaying 1 - 10 of 30.

A list of announcements is then shown that exist on the source Communication Manager.

The screenshot shows the Blackchair Spotlight Configuration Management interface. The top navigation bar includes 'DASHBOARD', 'CONFIGURATION' (highlighted), 'ROOT CAUSE ANALYSIS', 'REPORTING', 'OPTIONS', and 'ADMIN'. The left sidebar has 'Browse Environments' with options 'UAT', 'pre-prod', 'Search', and 'Last 100 Changes'. The main table lists announcements with columns: Item Name, Item Type, Version, Last Updated, and Updated By. The data rows are:

Item Name	Item Type	Version	Last Updated	Updated By
Extension 1099	Announcement	1	24 Feb 2015, 12:23:25	System
Extension 1234	Announcement	2	25 Feb 2015, 11:17:00	paul
Extension 2234	Announcement	1	25 Feb 2015, 11:17:00	paul
Extension 2688	Announcement	1	24 Feb 2015, 12:23:25	System

At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 4 of 4'. Below the table, there are tabs for 'General' and 'Options', and a message: 'There is no further information available for this object'.

Right-click on the announcement that is to be copied across to the target Communication Manager. In the example below, this is **Extension 1099**. Select **Add to Config Package**.

This screenshot is similar to the previous one, but a right-click context menu is open over the 'Extension 1099' row. The menu options are 'Edit Attachments', 'Add to Watch List', and 'Add to Config Package' (which is highlighted with a red box). The table data and interface elements are the same as in the previous screenshot.

Add a suitable name for the **Config Package**, in this case simply **announcement**. Click on **New**.

Item Name	Item Type	Version	Last Updated	Updated By
Extension 1099	Announcement	1	24 Feb 2015, 12:23:25	System
Extension 1234	Announcement	2	25 Feb 2015, 11:17:00	paul
Extension 2234	Announcement	1	25 Feb 2015, 11:17:00	paul
Extension 2688	Announcement	1	24 Feb 2015, 12:23:25	System

Add to Config Package X

Config Package:

Page 1 of 1 Back

Displaying 1 - 4

General Options

Version: Add this version to Config Package

Name: Extension 1099

Version: 1

The left pane shows the two environments, UAT represents the source Communication Manager and pre-prod represents the target Communication Manager. Right-click on the source environment, in this case **UAT**, and select **Manage Config Packages**.

spotlight

Browse Environments

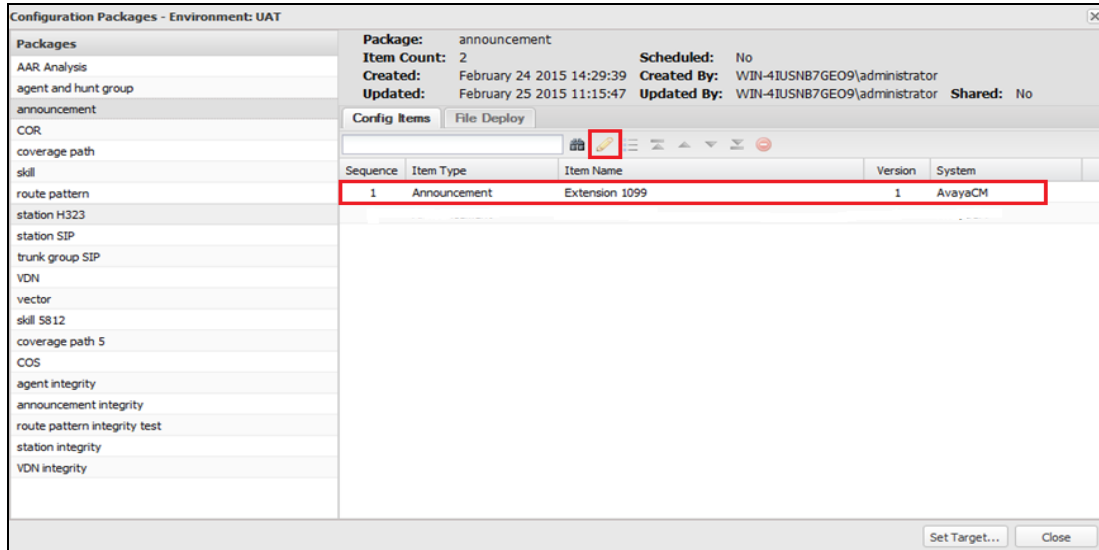
- UAT
- pre-prod
- Search
- Last 1

- Watch List
- Edit Attachments
- Manage Config Packages

Item Name	Item Type	Version	Last Updated
Extension 1099	Announcement	1	24 Feb 2015, 12:23:25
Extension 1234	Announcement	2	25 Feb 2015, 11:17:00
Extension 2234	Announcement	1	25 Feb 2015, 11:17:00
Extension 2688	Announcement	1	24 Feb 2015, 12:23:25

Page 1 of 1 Back

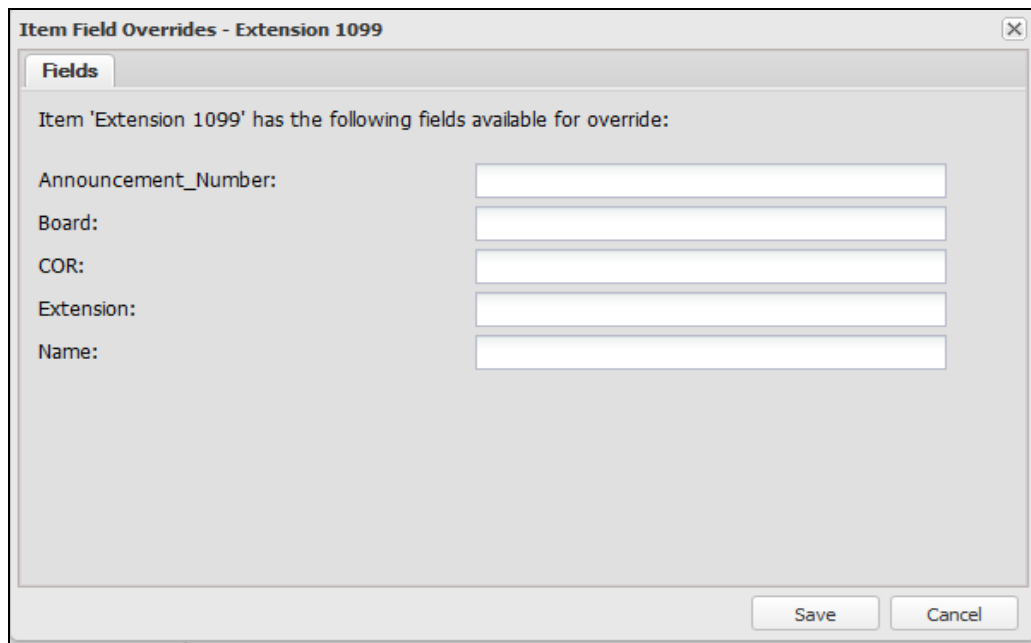
Highlight the announcement and click on the **edit icon** in the toolbar as highlighted below.



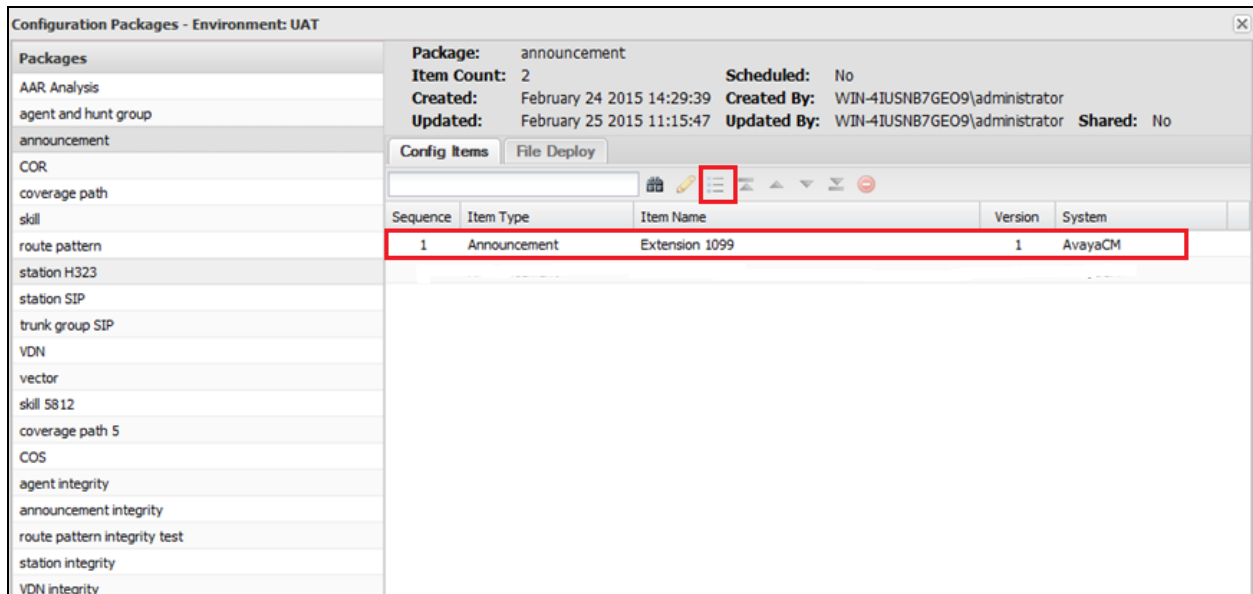
The following fields can be altered before the package is then sent to the target Communication Manager.

- **Announcement_Number**
- **Board**
- **COR**
- **Extension**
- **Name**

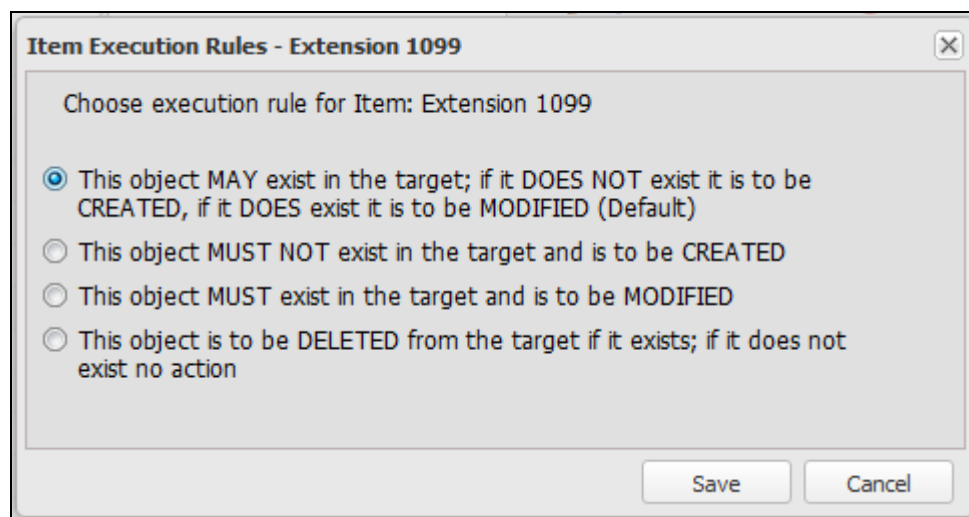
Click on **Save** at the bottom of the screen.



The package contents screen is again shown. Click on the **execution rules** button highlighted.



This brings up the execution rules window. Select the necessary rule that applies to this system, typically the following rule is selected, so as the specified announcement is created if it does not exist on the target system. Click on **Save** to continue.



Click on **Set Target** at the bottom of the screen as shown below.

Sequence	Item Type	Item Name	Version	System
1	Announcement	Extension 1099	1	AvayaCM

Enter the correct information for the target system, including the target system in our **case pre-prod** and the correct **CM Username** and **CM Password**. The other fields can be left blank but are used to keep records of the changes that are made by sending an email to a specified address. This package can be executed immediately, scheduled or tested prior to any execution. In the example below this was tested first, click on **Test**.

Environment: pre-prod

Avaya CM

Avaya CM Username: xxxxxxxx

Avaya CM Password:

Reviewer: R. Hughes

Reference: CR4434

Notification Email: support@rai.com

Terminate on Error?: ☒

Schedule?: ☐ Store for Execution?: ☐

Start Time: Thu, 26 February 2015 13:06 UTC

Test Execute Now Cancel

When the package is tested for errors and none are present the following window is displayed with a green tick on the right-hand side as shown below.

Test Package Report - announcement - Target Environment: pre-prod								
Sequence	Item Type	Item Name	System	Exists In Spotlight?	Exists In Target?	Execution Rule	Uses A Preceding Item?	Issues
1	Announcement	Extension 1099	AvayaCM	Yes	No	Delete	No	

Once the test has completed successfully and the previous screen is closed, click on **Execute Now** at the bottom of the screen shown below to initiate the change to be made on pre-prod.

Execute or Schedule Config Package

Select the Execution details for Config Package 'announcement'

Environment:

pre-prod

Avaya CM

Avaya CM Username:

xxxxxxxxxxxx

Avaya CM Password:

●●●●●●●●

Reviewer:

R. Hughes

Reference:

CR4434

Notification Email:

support@rai.com

Terminate on Error?:

☒

Schedule?:

☐

Store for Execution?:

☐

Start Time:

Thu, 26 February 2015

13 : 06

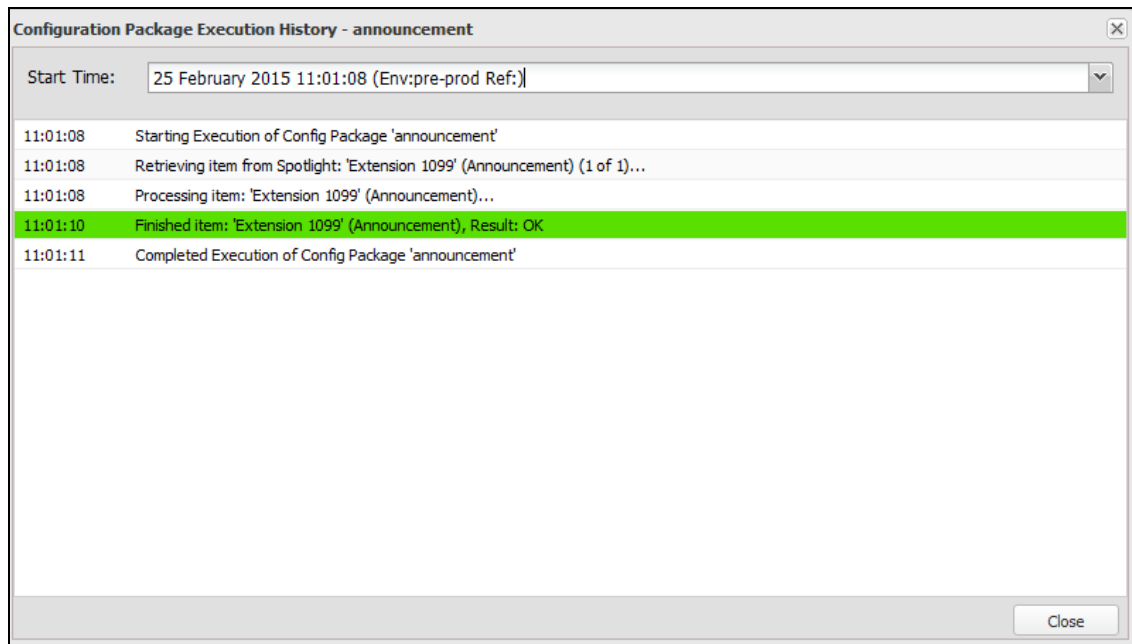
Thu, 26 February 2015 13:06 (UTC)

Test

Execute Now

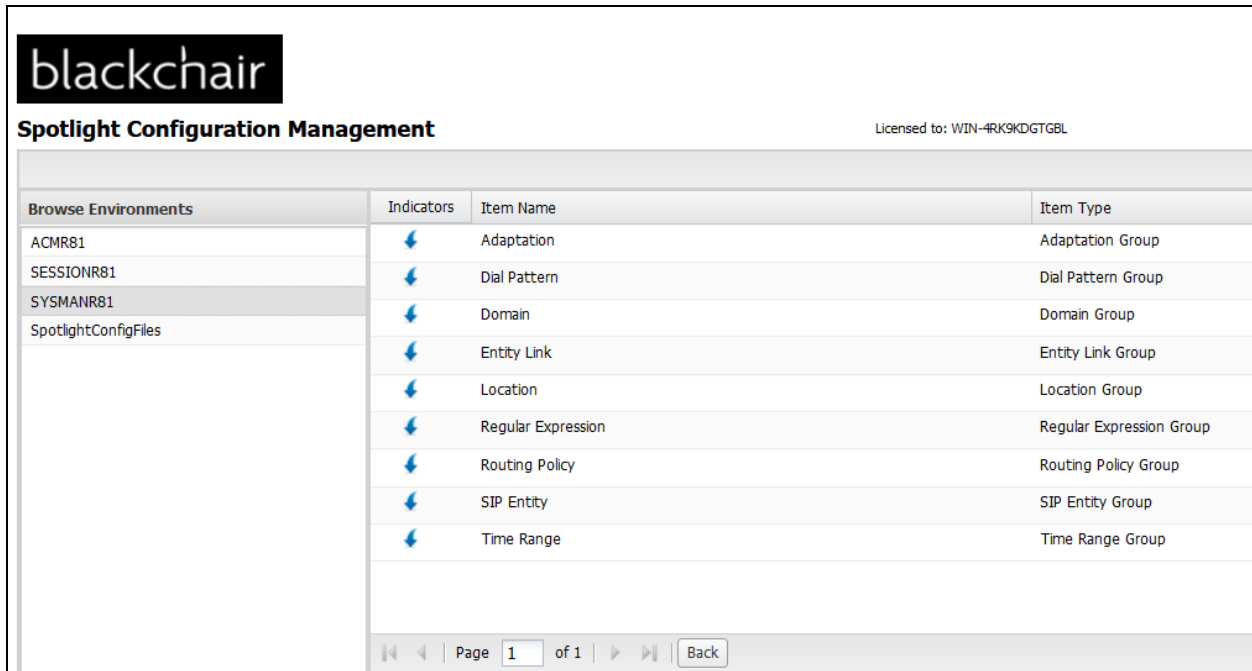
Cancel

The following screen then appears showing the changes that are being made. This change can then be viewed on the target system using a program such as SAT to display the new announcement.



9.5. Verify Spotlight Connection to Avaya Aura® System Manager

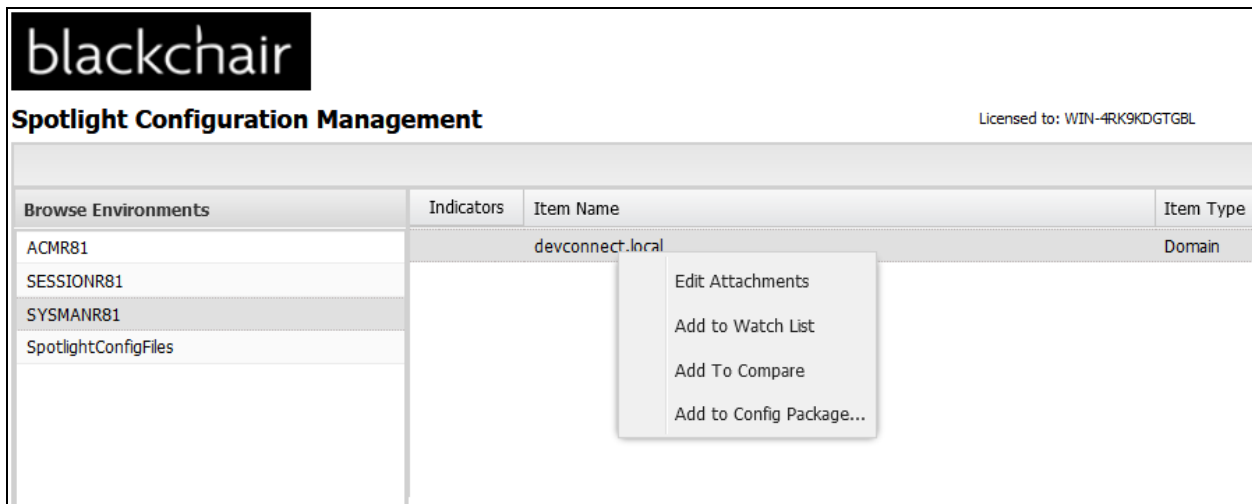
In the example below, changes to the **Domain** are being made. This domain will be copied, and an additional domain called Blackchair.com will be created. Click on Domain below, this will show the existing domains configured on System Manager.



The screenshot shows the Blackchair Spotlight Configuration Management interface. The header includes the Blackchair logo, the title "Spotlight Configuration Management", and the license "Licensed to: WIN-4RK9KDG TGBL". The main content area is a table with the following columns: "Browse Environments", "Indicators", "Item Name", and "Item Type". The "Browse Environments" column lists "ACMR81", "SESSIONR81", "SYSMANR81", and "SpotlightConfigFiles". The "Indicators" column contains blue arrows pointing right. The "Item Name" column lists "Adaptation", "Dial Pattern", "Domain", "Entity Link", "Location", "Regular Expression", "Routing Policy", "SIP Entity", and "Time Range". The "Item Type" column lists "Adaptation Group", "Dial Pattern Group", "Domain Group", "Entity Link Group", "Location Group", "Regular Expression Group", "Routing Policy Group", "SIP Entity Group", and "Time Range Group". At the bottom of the table, there is a pagination bar showing "Page 1 of 1" and a "Back" button.

Browse Environments	Indicators	Item Name	Item Type
ACMR81	➡	Adaptation	Adaptation Group
SESSIONR81	➡	Dial Pattern	Dial Pattern Group
SYSMANR81	➡	Domain	Domain Group
SpotlightConfigFiles	➡	Entity Link	Entity Link Group
	➡	Location	Location Group
	➡	Regular Expression	Regular Expression Group
	➡	Routing Policy	Routing Policy Group
	➡	SIP Entity	SIP Entity Group
	➡	Time Range	Time Range Group

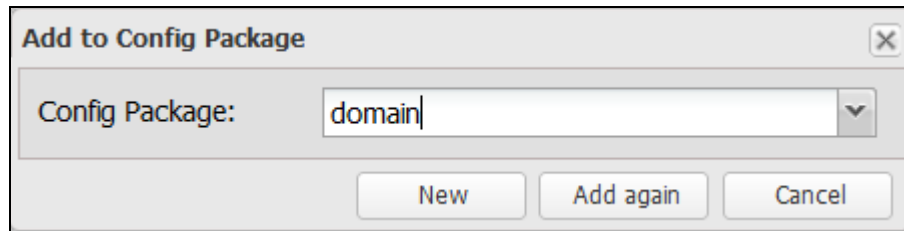
Right-click on the domain to be copied and select **Add to Config Package....**



The screenshot shows the Blackchair Spotlight Configuration Management interface with a right-click context menu open over the "Domain" item. The menu options are "Edit Attachments", "Add to Watch List", "Add To Compare", and "Add to Config Package...". The "Domain" item in the table has the value "devconnect.local" in the "Item Name" column.

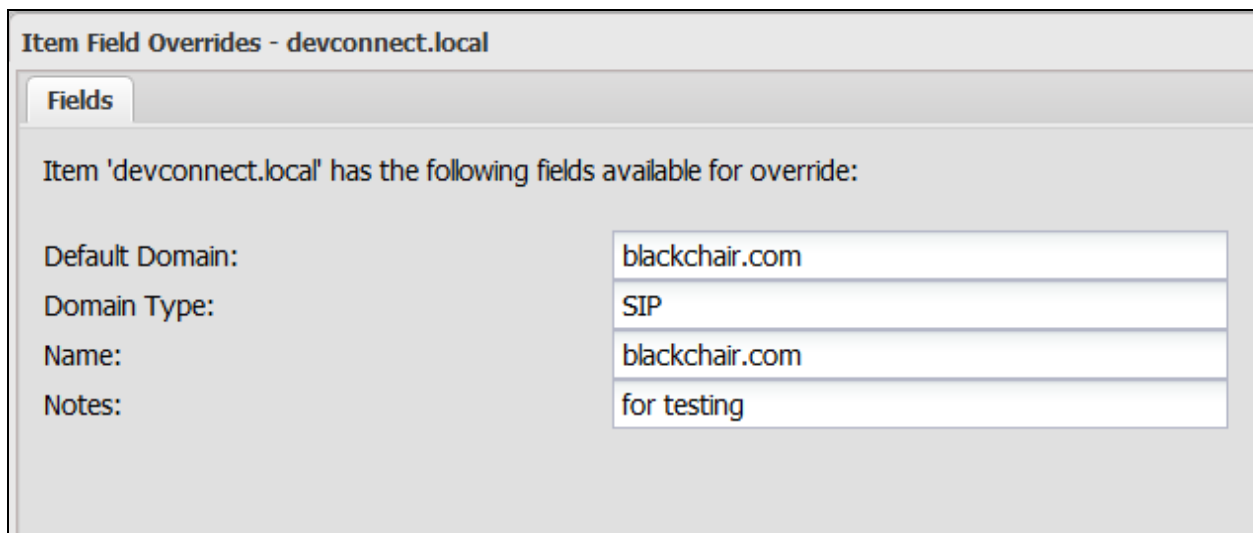
Browse Environments	Indicators	Item Name	Item Type
ACMR81		devconnect.local	Domain
SESSIONR81			
SYSMANR81			
SpotlightConfigFiles			

Give a name to the **Config Package** and click on **New**.



A dialog box titled "Add to Config Package" with a close button (X) in the top right corner. It contains a text input field labeled "Config Package:" with the text "domain" entered. Below the input field are three buttons: "New", "Add again", and "Cancel".

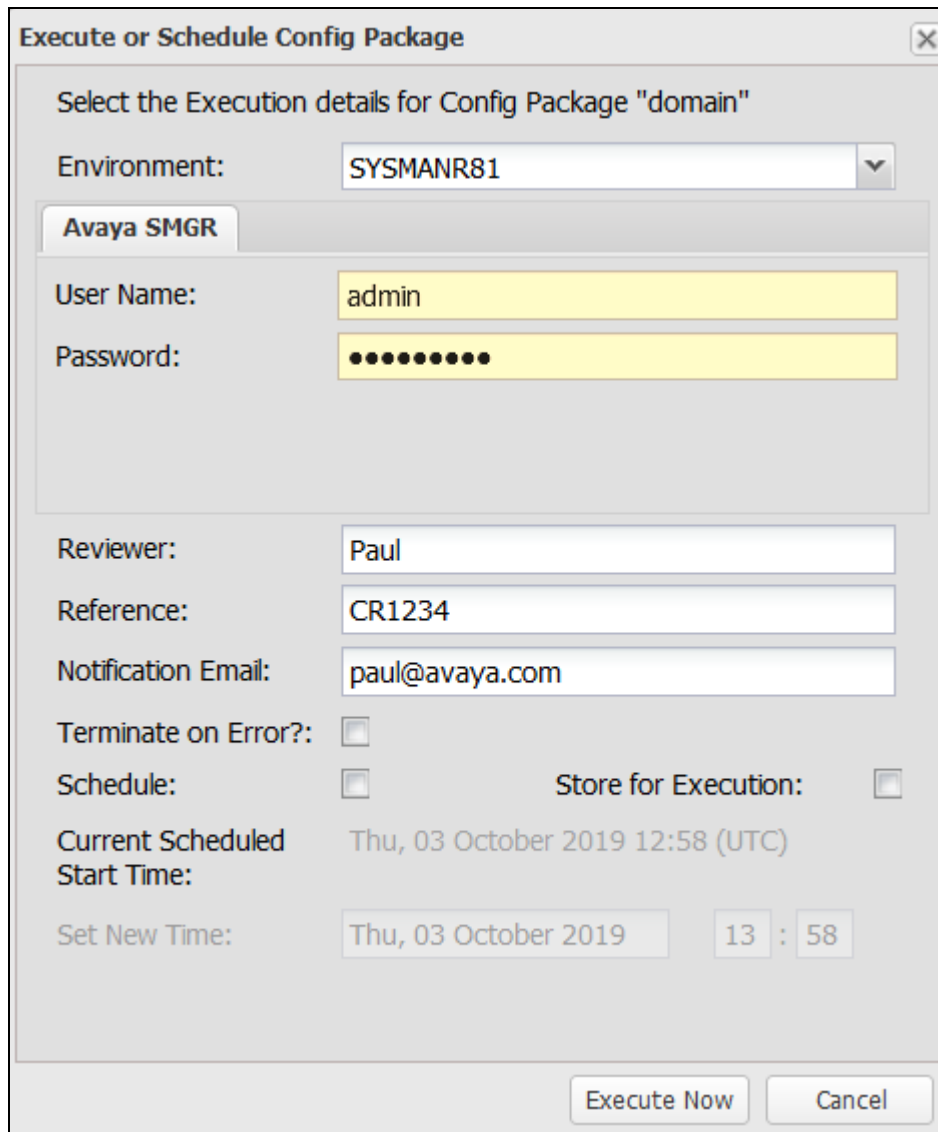
The following **Fields** can be changed. Leaving a field blank will simply copy the equivalent field from the existing domain. The new domain will be called **Blackchair.com** with new **Notes** labelled **for testing**. Once the fields are entered, click on **Save** at the bottom right of the screen (not shown below).



A dialog box titled "Item Field Overrides - devconnect.local" with a "Fields" tab selected. The text inside reads: "Item 'devconnect.local' has the following fields available for override:". Below this text are four rows of labels and input fields:

Default Domain:	blackchair.com
Domain Type:	SIP
Name:	blackchair.com
Notes:	for testing

The following window appears where the **User Name** and **Password** for System Manager are added and some information on who is making the changes. Click on **Execute Now** to initiate the changes.



The dialog box is titled "Execute or Schedule Config Package" and contains the following fields and controls:

- Select the Execution details for Config Package "domain"**
- Environment:** A dropdown menu showing "SYSMANR81".
- Avaya SMGR** (tabbed section)
- User Name:** A text field containing "admin".
- Password:** A text field containing 10 dots.
- Reviewer:** A text field containing "Paul".
- Reference:** A text field containing "CR1234".
- Notification Email:** A text field containing "paul@avaya.com".
- Terminate on Error?:** A checkbox.
- Schedule:** A checkbox.
- Store for Execution:** A checkbox.
- Current Scheduled Start Time:** A label with the text "Thu, 03 October 2019 12:58 (UTC)".
- Set New Time:** A text field containing "Thu, 03 October 2019" and a time selector showing "13 : 58".
- Execute Now** and **Cancel** buttons at the bottom right.

The following screen shows the changes have been made correctly as the **Result** is shown as **OK** and is in green.

Configuration Package Execution Log	
Timestamp	Message
13:59:10	Starting Execution of Config Package 'domain'
13:59:10	Analysing target location for Config Package 'domain'
13:59:10	Retrieving item from Spotlight: 'devconnect.local' (Domain) (1 of 1)...
13:59:10	Processing item: 'devconnect.local' (Domain) with action Create or Modify...
13:59:12	Finished item: 'devconnect.local' (Domain), Result: OK
13:59:13	Completed Execution of Config Package 'domain'

10. Conclusion

These Application Notes describe the configuration steps required to integrate Blackchair Spotlight Audit and Release Management with Avaya Aura® Communication Manager, using the SMS connection on Avaya Aura® Application Enablement Services, and Avaya Aura® System Manager. Please refer to **Section 2.2** to see the compliance test results and observations.

11. Additional References

The following documents are available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1, Issue 3, August 2019
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1
- [3] *Administering and Maintaining Avaya Aura® Application Enablement Services* Release 8.1
- [4] *Routing Web Service API Programming Reference* Release 8.0.1 Issue 2 December 2018

Information on the Avaya Aura® Application Enablement Services SMS SDK can be found by navigating to this link <https://www.devconnectprogram.com/>

The AE Services System Management Service Fact Sheet can be found by searching for the following file **LB3873.pdf** on the DevConnect website, <https://www.devconnectprogram.com/>.

Product information on Blackchair Spotlight can be found at <http://www.thebackchair.com>.

12. Appendix

The Appendix contains information on the objects and operations that are supported for Communication Manager, System Manager and Session Manager.

12.1. Communication Manager

The following objects and operations are supported for Communication Manager:

Object	Audit	Create	Amend	Delete
AAR Analysis	X		X	
AAR Digit Conversion	X			
Abbreviated Dialling Enhanced	X	X		X
Abbreviated Dialling Group	X	X	X	X
Agent Login	X	X	X	X
Announcement	X	X	X	X
ARS Analysis	X			
ARS Digit Conversion	X			
Audio Group	X	X	X	X
Authorisation Code	X	X	X	X
Cabinet Mapping	X			
COR	X		X	
COS	X		X	
Coverage Answer Group	X	X	X	X
Coverage Path	X	X	X	X
Coverage Time of Day	X	X		X
CTI Link	X	X	X	X
Customer Options	X			
Dial Plan	X			
Dial Plan Parameters	X			
Feature Access Codes	X			
Holiday Table	X		X	
Hunt Group	X	X	X	X
Intercom Group	X	X	X	X
IP Interface	X			
IP Services	X			
Locations	X			
Media Gateway	X	X	X	X
Off PBX Feature Name Extension	X			
Off PBX Station	X			

Pick Up Group	X	X	X	X
Public Unknown Numbering	X			
Reason Code	X			
Remote Access	X			
Remote Call Coverage	X			
Route Pattern	X	X	X	
Signaling Group	X			
Site Data	X			
Station	X	X	X	X
Terminating Extension Group	X		X	
Trunk Group	X		X	
Uniform Dialplan	X			
VDN	X	X	X	X
Vector	X	X	X	
Vector Variables	X			
VRT	X			

12.2. System Manager

The following objects and operations are supported for System Manager:

Object	Audit	Create	Amend	Delete
Adaptation	X	X	X	X
Dial Pattern	X			
Domain	X	X	X	X
Entity Link	X		X	X
Location	X	X		X
Regular Expression	X	X	X	X
Routing Policy	X	X	X	X
SIP Entity	X	X	X	X
Time Range	X	X	X	X

12.3. Session Manager

The following objects and operations are supported for Session Manager:

Object	Audit	Create	Amend	Delete
Address Mapping Group	X			
App Set	X			
Application	X			
ASM Instance	X			
ASM Terminal Group Parameters	X			
Factory Set	X			
Failover Group	X			
Hostname Resolution IP	X			
Initiation	X			
Pattern to App Set	X			

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.