COMMUNICATION MANAGER TECHNICAL ONBOARDING GUIDE

<table>
<thead>
<tr>
<th>Purpose</th>
<th>The purpose of this document is to assist in understanding the registration process for Communication Manager for Main, ESS, and LSP installations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>A Technical Onboarding request in GRT 4.0 can perform several useful functions. Technical Onboarding should be performed to do any of the following:</td>
</tr>
<tr>
<td></td>
<td>- Creating SEIDS and Alarm IDs for newly installed devices. (Step A)</td>
</tr>
<tr>
<td></td>
<td>- Testing Connectivity and Alarming for newly created devices. (Step B)</td>
</tr>
<tr>
<td></td>
<td>- Modification of records for existing registered devices</td>
</tr>
<tr>
<td></td>
<td>- Connectivity and Alarm re-testing</td>
</tr>
<tr>
<td>Target Audience</td>
<td>Avaya Partners, Distributors, Avaya Associates</td>
</tr>
<tr>
<td>See Also</td>
<td>GRT Registration Process: <a href="https://support.avaya.com/helpcenter/getGenericDetails?detailId=C2009101293650506080">https://support.avaya.com/helpcenter/getGenericDetails?detailId=C2009101293650506080</a></td>
</tr>
<tr>
<td></td>
<td>SAL Migration: Migrating managed device from one SAL Gateway to another SAL</td>
</tr>
<tr>
<td></td>
<td><a href="https://support.avaya.com/ext/index?page=content&amp;id=SOLN322731">https://support.avaya.com/ext/index?page=content&amp;id=SOLN322731</a></td>
</tr>
<tr>
<td></td>
<td>Administer SEIDs into my SAL gateway</td>
</tr>
<tr>
<td></td>
<td><a href="https://support.avaya.com/ext/index?page=content&amp;id=FAQ105290">https://support.avaya.com/ext/index?page=content&amp;id=FAQ105290</a></td>
</tr>
<tr>
<td></td>
<td>GRT Enhancement KB Article: <a href="https://support.avaya.com/ext/index?page=content&amp;id=TRNG100448">https://support.avaya.com/ext/index?page=content&amp;id=TRNG100448</a></td>
</tr>
<tr>
<td>Tools</td>
<td>Global Registration Tool(GRT)</td>
</tr>
<tr>
<td>Acronyms Used</td>
<td>GRT - Global Registration Tool</td>
</tr>
<tr>
<td></td>
<td>SR - Service Request</td>
</tr>
<tr>
<td></td>
<td>CM - Communication Manager</td>
</tr>
<tr>
<td></td>
<td>SEID - Solution Element ID</td>
</tr>
<tr>
<td></td>
<td>RFA - Remote Feature Activation</td>
</tr>
<tr>
<td></td>
<td>SID - System Identifier</td>
</tr>
</tbody>
</table>
# CONTENTS

Glossary of Terms .......................................................................................................................... 3
New Main Communication Manager (Simplex and Duplex) ........................................................................ 3

   Technical Onboarding Step A: Creating SEIDs and Alarm IDs for the Installed Base ......................... 3
      Continuing a previously started End-To-End Registration request ...................................................... 3
      Starting a new “Technical Onboarding Only” request ........................................................................... 4
      Using the Technical On-Boarding (TOB) Dashboard / User Interface (UI) .............................................. 5
      Select a device associated with the Sold-To / Functional Location (FL) for registration ..................... 6
      Specifying Connectivity details for the device ...................................................................................... 8

New ESS or LSP .................................................................................................................................. 19

   Select a Device associated with the Sold-To / Functional Location (FL) for registration ....................... 19

Upgrading an Existing CM Main ESS or LSP .......................................................................................... 22

Technical Onboarding Step B: Testing Connectivity and Alarming for newly created devices. ................. 23

   Connectivity and Alarm testing ............................................................................................................. 25

Change History ...................................................................................................................................... 27
Glossary of Terms

**Remote Feature Activation** - RFA is a web-based application that is used to create and deliver license files for Avaya products. The license files are created using information from the customer and the SAP order.

**New Main Communication Manager (Simplex and Duplex)**

The process outlined below start from the Technical Onboarding steps. It is assumed that the Install Base Creation has already been done and that you are ready to generate SEIDs. If assistance is needed in adding the Material Codes to the Install Base, please review the following document. [https://support.avaya.com/css/P8/documents/100162279](https://support.avaya.com/css/P8/documents/100162279)

**Note**: GRT requires that the user know the RFA SID for Communication Manager R5 or earlier.

**Technical Onboarding Step A: Creating SEIDs and Alarm IDs for the Installed Base**

**Continuing a previously started End-To-End Registration request**

1. **If continuing an End-To-End Registration request.**
   - From the GRT homepage, in the “Registration Management” section, click on “Update Existing Registration”
   - Using one of the various filters available, locate your existing End-To-End Registration request.
- Click on the RED hyperlink under the Technical Onboarding Status column.

**Proceed to Step 3**

**Starting a new “Technical Onboarding Only” request**

2. If starting from a new “Technical Onboarding Only” request...

- Enter the Sold-To/Functional Location details for the account. Select “Search”
  
  Note: End Customer ST / FL must be in the 10-digit format with leading zeros.

Avaya – Confidential & Proprietary. 
Use pursuant to your signed agreement or Avaya policy.
• Edit the Site Contact, Validation details if necessary, and click “Next”. Proceed to Step 3

Using the Technical On-Boarding (TOB) Dashboard / User Interface (UI)

3. Technical On-Boarding Dashboard is displayed.
Select a device associated with the Sold-To / Functional Location (FL) for registration

4. Expand the section “REGISTERABLE PRODUCTS LIST – READY FOR TECHNICAL ON-BOARDING”. This is a listing of the Installed Base of Material Codes which can be processed for SEID and Alarm ID creation on this account.

Locate the device to be technically Onboarded and click on “Select”.

5. Once the proper Installed Base has been located, make the proper selection under “Connectivity”.

- Choosing “Yes” will require connectivity details to be entered to continue.
- Choosing “No” will allow you to enter optional details expected to be used in the future if this is a staged installation
- Choosing “Later” will allow you to continue without providing any details. (Any SEIDS created with no connectivity details can be updated later via Update Registration.)
6. Choose the appropriate Access Type to be used for this device and click “Continue”

![Image of Access Type selection]

7. Product Configuration Data
   - For devices with multiple configuration possibilities, the “Group” dropdown will need to be properly selected.
   - The “SE Code Preview” will update to reflect what records will be created based on the selection in the Group dropdown.

![Image of Product Configuration Data]

Avaya – Confidential & Proprietary.
Use pursuant to your signed agreement or Avaya policy.
8. As this is for a Main CM installation, the “Is It a Main CM?” radio button should be set to “Yes”.

**Specifying Connectivity details for the device**

9. Connectivity Details must now be provided:

**SECURE ACCESS LINK (SAL) CONNECTED DEVICE**

i. Connectivity Access Type = SAL
   - SAL Gateway Configuration Details Section
     - For any device in which a “VSALGW” is listed in the SE Code Preview, and that embedded SAL will be used as the Primary access method, no selections need to be made in the “SAL GATEWAY CONFIGURATION DETAILS” section.
     - However, you must enter the Connectivity Details for at least ONE SE code in the group, otherwise you will get an error popup.
     - Fill in the “Device IP Address”, “Device Hostname”
     - For Gateway SEID selection, click on Select next to one of the records
       - When there is no SALGW in the configuration and no VSALGW records when clicking on the Hyperlink Select or if the proper record cannot be found, use the Add SoldTo ID or Gateway SEID, to add to the list. Click here for the process.
• SAL Gateway is associated to the SoldTO (YES)
  o Popup appears with the list of Gateways SEIDs. User can select ONLY an Active gateway. For the Inactive gateway/s when clicking on icon “I”, a popup appears with the details

For a Gateway not listed, users can enter the SoldTo or Gateway SEID and click on Add button.  
**Note:** User must be authorized for the Sold To

  o To proceed Select the Active device and click on “Save”
• If there are no SAL Gateways available at the Sold To you will see this pop up
  
  o Select “Enter Different Sold To”

  ![Pop-up Image]

  o Enter the “SoldTo” or “Gateway SEID”. Click on “Add”.

  ![Gateway SEID Entry Image]

  o Select the proper Primary SAL Gateway to be used for remote access of this device. Click “Save”

  ![Primary SAL Gateway Image]
All three (3) fields (Device IP Address, Device Hostname, Gateway SEID) must be completed for at least one (1) record of the configuration before proceeding. When one or more records are completed, click “Add”.

- A popup will display as below if one of the 3 fields is not completed. Choose an option and proceed.

Go to Step 10
RASIP Connected Device

ii. Connectivity Access Type = RASIP

- Ignore the SAL GATEWAY CONFIGURATION DETAILS section
- Provide the device IP Address in the “IP Address” field. Select Add

Modem Connected Device

iii. Connectivity Access Type = Modem

- If the customers end device must use an outbound prefix (*9 for example) provide this information in the “Outbound Prefix” field (to be used for alarming configurations).
- Enter the modem telephone number in the “Dial-In Number” field. Select Add
10. Select the most accurate details in the “PRODUCT CONFIGURATION DETAILS”. The SID and MID must be provided based RFA license details in the case of CM R5 or earlier. Click “VALIDATE SID/MID” to verify proper settings. For CM R6+ these fields will not be available as new details are created automatically for all Main servers.

NOTE: If SID/MID combination is already being used by other Active records within Avaya, an error will be presented.

11. Click on “Proceed”.

12. CM details will now be listed in the “REGISTERABLE PRODUCTS – READY TO PROCESS”.
13. To create additional SEIDs or Alarm IDs for other Installed Base device, repeat the steps 4 -12.

14. Once all necessary devices have been added and are ready to process, click the “Submit” button at the bottom of the page.

15. Click on OK to confirm.

16. SAL On-Boarding Summary displays details of the request.
**Note:** At this point SEIDs and Alarm ID are being created for the requested devices. Please monitor Email activity. Notification emails will alert to changes in status as well as to provide SEID and Alarm ID details that have successfully created. In many cases, it’s expected that more than one email will be generated per request.

There are new notifications for SAL TOB material code and four notifications as it stepped thru the process via SAL Admin.

Examples below:

<table>
<thead>
<tr>
<th>GRT Registration ID</th>
<th>GRT Registration ID</th>
<th>GRT Registration ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>8257532</td>
<td>Technical</td>
<td>8257532</td>
</tr>
<tr>
<td>Technical</td>
<td>SAL Admin</td>
<td></td>
</tr>
</tbody>
</table>

17. Once the SEID/Alarm ID creation is complete, SEID Creation status changes to Completed.

Next step is SAL Administration and SAL Administration Result is set to IN PROGRESS

If you click on **In Progress hyperlink**, Sal Administration details are displayed.
18. Once the SAL Administration step is completed, there are one of the two scenarios that can come into effect:

i) SAL Administration Result is **Success with TOB Step B** - In this case GRT has automatically initiated Connectivity and Alarm testing i.e. TOB Step B is initiated.

- SAL Administration Result Success with TOB Step B links to the message:
- Email notification will notify user that step B has been automatically submitted

- Once the Automatic Connectivity and Alarming testing is complete, Connectivity/Alarming status set to Completed.

Avaya – Confidential & Proprietary.
Use pursuant to your signed agreement or Avaya policy.
• User will receive an email notification confirming Connectivity/Alarm testing is complete.

Note: Similar notification is sent when TOB step B is completed manually or automatically.

Goto TOB Step B to manually initiate Connectivity and Alarm testing.
New ESS or LSP

The process outlined below start from the Technical Onboarding steps. It is assumed that the Install Base Creation has already been done and that we are ready to generate our SEIDs. If assistance is needed in adding the Material Codes to the install base, please review the following. [https://support.avaya.com/css/P8/documents/100162279](https://support.avaya.com/css/P8/documents/100162279)

If the Communication Manager server that is being registered is an SAP or an ESS, GRT requires that the user know the SEID of the Main Communication Manager with the MID of “1”. GRT will link the new CM being registered with the main server through the Avaya tools.

If the SEID of the main is not known, please use the SEID Record Building Report to gather these details from the customers main Sold-To. For Duplex Main CM configurations, only 1 of the SEIDs will be needed. [https://downloads.avaya.com/css/P8/documents/10018290](https://downloads.avaya.com/css/P8/documents/10018290)

Select a Device associated with the Sold-To / Functional Location (FL) for registration

1. Expand the section “REGISTERABLE PRODUCTS LIST – READY FOR TECHNICAL ON-BOARDING”. This is a listing of the Installed Base of Material Codes which can be processed for SEID and Alarm ID creation on this account.

Locate the Device to be technically Onboarded and click on “Select”.

2. Once the proper Installed Base has been located, make the proper selection under “Connectivity”.
   - Choosing “Yes” will require connectivity details to be entered to continue.
   - Choosing “No” will allow you to enter optional details expected to be used in the future if this is a staged installation
   - Choosing “Later” will allow you to continue without providing any details. (Any SEIDS created with no connectivity details can be updated later via Update Registration.)
3. Choose the appropriate Access Type to be used for this device and click “Continue”.

![Selection screen](image)
4. Product Configuration Data
   - For devices with multiple configuration possibilities, the “Group” dropdown will need to be properly selected.
   - The “SE Code Preview” will update to reflect what records will be created based on the selection in the Group dropdown.

5. Since this is for an ESS or LSP installation, the “Is It a Main CM?” radio button should be set to “No”, and GRT will present a field for “Enter Main SEID”. Enter the SEID of the Main CM and then click “VALIDATE”. GRT will present details of the Main CM selected for reference.

   **NOTE:** Remote Communication Manager servers must be at an equal or greater release than the Main CM. If the details entered do not reflect this, GRT will present an error. If encountered, please review the document linked in the error message for information on how to resolve.
6. Continue with the steps listed in the above section.

Upgrading an Existing CM Main ESS or LSP

For Main CM installations that are being upgraded from r.5 to CM r.6, the existing RFA SID should not be retained. When creating a new Main CM server that is r.6+, GRT will automatically create a new SID for these records. This SID must be manually entered in the Main CM servers as well as any ESS servers. LSP server will receive these details automatically. For more information please review the following guide.

https://support.avaya.com/public/index?page=content&id=FAQ106063

For ESS or LSP servers that will be using the same SID/MID combination as the old server, it will be necessary to free up the SID/MID combination for use with the new servers. To accomplish this, an Equipment Removal request must be completed on the old servers before Technical Onboarding is started for the new servers. For more information on how to process an Equipment Removal request, please review the following guide.

https://downloads.avaya.com/css/P8/documents/100175936

Once these considerations have been resolved, follow the appropriate sections above
Technical Onboarding Step B: Testing Connectivity and Alarming for newly created devices.

1. Once the SEIDs and Alarm ID are created for the requested devices, next step is to test Connectivity and Alarming for the new devices.
   From the GRT homepage, in the “Registration Management” section, click on “Update Existing Registration”

2. Using the various available filters, locate your existing End-To-End Registration request, and click on the red hyperlink under the Technical Onboarding Status column.

3. Listed will be the devices that had SEIDs and Alarm IDs created in TOB Step A on this request. Using the “Select” check boxes on the left, check any devices that have had its SEIDs added to the SAL Gateway/s for remote access.
4. Once the devices that are ready for connectivity and alarm testing have been selected. Click the “SAL ALARM & CONNECTIVITY” button at the bottom of the page. Note: Any devices not selected will still be available for Connectivity and Alarm testing on this GRT request, and may be submitted later without the need to create a new request.

5. Click on Ok to confirm.
Connectivity and Alarm testing

6. Listed here are all the SEIDs that were created for this device. Use the “Select for Remote Access?” and “Select for Alarming?” checkboxes to indicate the level of testing required. NOTE: Alarm checkboxes will only be enabled for alarming capable devices with active alarming entitlements.
7. Once all selections have been made and the necessary remote access and alarming checkboxes have been populated, click the “SUBMIT” button at the bottom of the page.

8. Click Ok

9. Confirmation Popup
10. Connectivity/Alarming Status is set to In Process

At this point GRT will perform automated connectivity and alarm testing for supported devices based on the details submitted. Not all devices are supported for automated testing. Any devices not supported for automated testing, as well as any devices that may have failed any portion of the automated testing process, will be managed manually via a registration engineer.

Change History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Change Detail</th>
<th>Changed By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>New Document Release for GRT 4.0</td>
<td>Adam Chovan</td>
<td>8/24/2015</td>
</tr>
<tr>
<td>2</td>
<td>Updated Technical Onboarding Process – automated process</td>
<td>Mary Bora</td>
<td>05/08/2018</td>
</tr>
<tr>
<td>3</td>
<td>Updates on Automatic Remote connectivity and Alarm Testing (TOB Step B)</td>
<td>Mary Bora</td>
<td>22/08/2018</td>
</tr>
</tbody>
</table>