Avaya Solution & Interoperability Test Lab

Application Notes for MUG Enterprise Call Guard with Avaya Proactive Contact with CTI – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for MUG Enterprise Call Guard to interoperate with Avaya Proactive Contact with CTI. MUG Enterprise Call Guard is an application that marks call records on Avaya Proactive Contact to prevent future calls, when the associated call attempts are over the limit trigger.

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 for MUG Enterprise Call Guard to interoperate with Avaya Proactive Contact with CTI. MUG Enterprise Call Guard is an application that sets the STATUSFLAG parameter in call records on Avaya Proactive Contact to prevent future calls, when the associated COUNTER parameter value in the call record is over the limit trigger set by the customer.

The integration required two custom Linux shell scripts, MUGset and CALLGUARD, developed by MUG Enterprise and deployed to Avaya Proactive Contact. Two options were manually added to the Proactive Contact sysadm menu to associate with the scripts. The MUGset script sets the value for the limit trigger, and the CALLGUARD script processes call records in the specified calling lists to make updates to the STATUSFLAG parameter as needed to prevent future calls.

The CALLGUARD script can be invoked manually by the administrator, or run on a regular basis by scheduling a cron job. Cron job scheduling is outside the scope of these Application Notes and will not be described. The compliance testing used the manual method to run the script. When cron job scheduling is desired, the cron entry should be added to the non-supervisor section of the crontab file.

Call Guard can be customized for customers to password protect modification of the limit trigger value, to generate record activity files for exports, and to log modified call records. The compliance testing only covered the generic version of Call Guard without any customization. Note that any customized version of the application will require separate compliance testing.

This compliance test covered the Avaya Proactive Contact with CTI deployment option.

2. General Test Approach and Test Results

The feature test cases were performed manually. Multiple calling lists were prepared with manual script runs to verify proper update of call records.

The serviceability test cases were performed manually by disrupting the Proactive Contact server, such as a reboot.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following:

- Setting and updating of the limit trigger via the administrator menu.
- Invocation of CALLGUARD script via the administrator menu.
- Proper update of calling lists based on the limit trigger and associated call record values for COUNTER and STATUSFLAG parameters, including no match, partial match, and complete match conditions.
- Proper run of CALLGUARD script with updates to calling list during an active job.

The serviceability testing focused on verifying that Call Guard can run successfully after a disruption to the Proactive Contact server, such as a reboot.

2.2. Test Results

All test cases were executed and verified.

The one observation noted from the compliance testing is that the CALLGUARD script can run into frequent record lock contentions whenever the call record to be examined is active on an agent desktop and therefore locked by Proactive Contact. The lock on the call record is only released by Proactive Contact when the agent has finished work associated with the call. As such, the script can take a while to complete when there are active jobs utilizing the same calling lists.

2.3. Support

Technical support on Call Guard can be obtained through the following:

- **Phone:** 724-947-5453
- **Email:** info@mugenterprise.com
- **Web :** http://www.mugenterprise.com/connect.shtml

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

The detailed administration of basic connectivity between Communication Manager and Proactive Contact, and of contact center devices are not the focus of these Application Notes and will not be described.

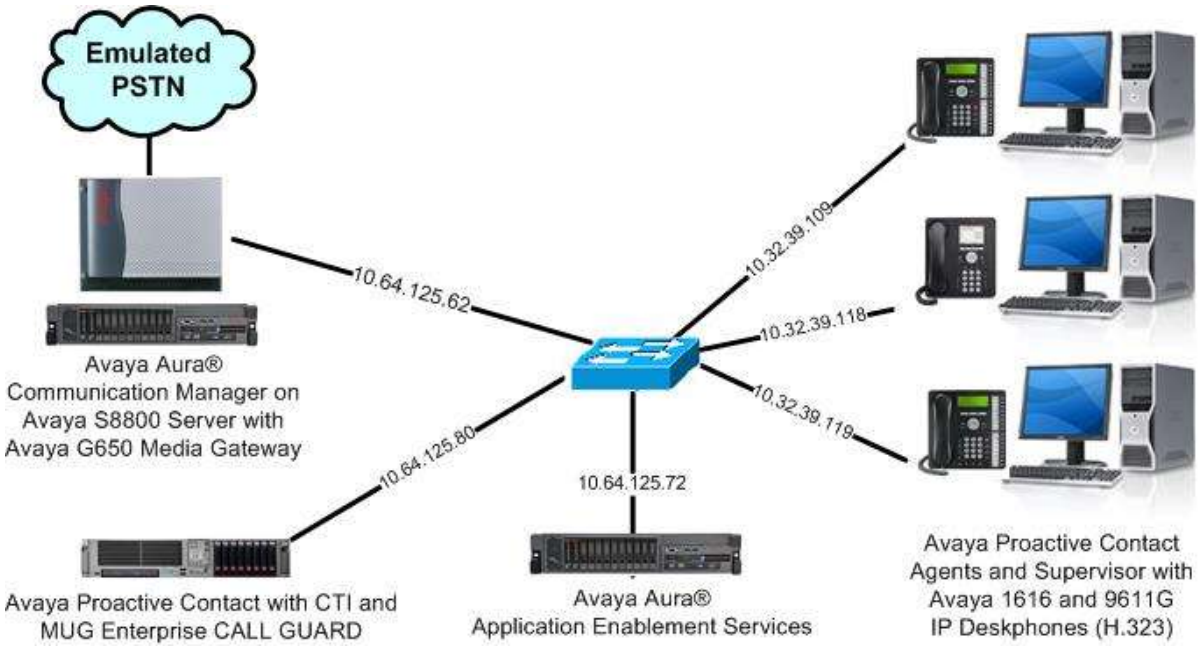


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.11.1 (R016x.03.0.124.0-22450)
Avaya Aura® Application Enablement Services	6.3.3 SP4 (6.3.3.4.10-0)
Avaya Proactive Contact with CTI • MUG Enterprise MUGset Script • MUG Enterprise CALLGUARD Script	5.1.1 1.1 2.6
Avaya Proactive Contact Agent	5.1.1
Avaya Proactive Contact Supervisor	5.1.1
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
Avaya 9650 IP Deskphone (H.323)	3.230A

5. Configure MUG Enterprise Call Guard

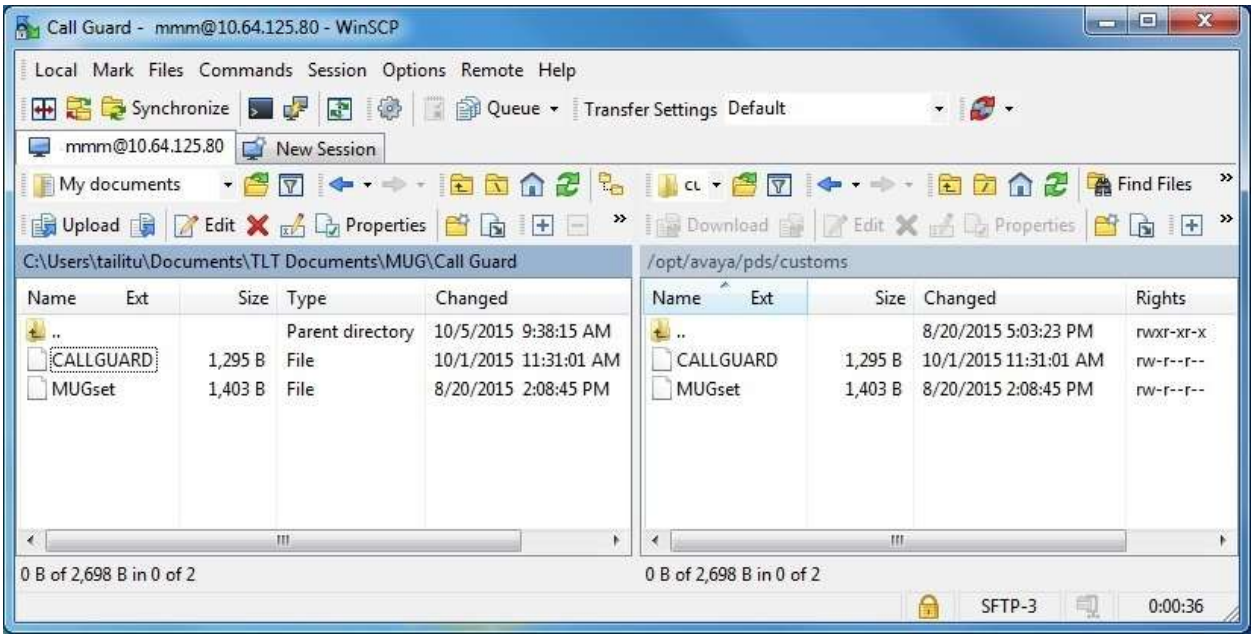
This section provides the procedures for installing and configuring Call Guard on Proactive Contact. The procedures include the following areas:

- Transfer custom scripts
- Change scripts permissions
- Add menu options
- Specify calling lists

The installation and configuration of Call Guard is performed by MUG Enterprise analysts. The procedural steps are presented in these Application Notes for informational purposes.

5.1. Transfer Custom Scripts

Use a tool such as WinSCP to transfer custom scripts MUGset and CALLGUARD to Proactive Contact. Place the two scripts under the **/opt/avaya/pds/customs** directory, as shown below.



5.2. Change Scripts Permissions

Log in to the Linux shell of the Proactive Contact server, and navigate to the **/opt/avaya/pds/customs** directory. Enter the command "chmod 775 MUGset", followed by "chmod 775 CALLGUARD" to change the access permissions. The screenshot below shows the resultant access permissions for the two scripts.

```
$ cd /opt/avaya/pds/customs
LZPDS4(xxxxx)@/opt/avaya/pds/customs [1006]

$ chmod 775 MUGset
LZPDS4(xxxxx)@/opt/avaya/pds/customs [1007]

$ chmod 775 CALLGUARD
LZPDS4(xxxxx)@/opt/avaya/pds/customs [1008]

$ ls -l
-rwxrwxr-x 1 xxxxx pds_system 1295 Oct  1 11:31 CALLGUARD
-rwxrwxr-x 1 xxxxx pds_system 1403 Aug 20 14:08 MUGset
LZPDS4(xxxxx)@/opt/avaya/pds/customs [1009]
$
```

5.3. Add Menu Options

Navigate to the **/opt/avaya/pds/menus** directory, and edit the **sysadm.menu** file. Insert the two lines shown below to add options for Call Guard.

```
WELCOME:@W10010
HELPNAME:sysadm
MENU:@P10900::::1:0:cmd:sysadm
MENU:@P10901::::1:0:menu:backup
MENU:@P10903::::0:0:config_backup
MENU:@P10904:YES:::1:0:cmd:inbnd
MENU:@P10905:YES:::1:0:noapp_winmsg:ivr
MENU:@P10906::::1:0:cmd:transfer
MENU:@P10908:YES:::1:0:cmd:mplay
MENU:@P10909::::1:0:%modifydbusers
MENU:@P10910:YES:::1:0:/bin/cat:$VOICEDIR/help/ssa.hlp
MENU:@P10911:YES:::1:0:/bin/cat:$VOICEDIR/help/csi.hlp
MENU:CALLGUARD Call Limit Manager::::1:0:MUGset
MENU:CALLGUARD::::1:0:CALLGUARD
~
~
```

5.4. Specify Calling Lists

Navigate to the **/opt/avaya/pds/customs** directory, and open the **CALLGUARD** script. Scroll to the bottom of the file, and add a **set_field** command line for every existing calling list to be processed by Call Guard, where "list1" is the name of the desired calling list in the first example shown below.

In the compliance testing, three calling lists were configured to be processed. Note that the name of the calling lists may vary.

```
########################################
#

#  Change the STATUSFLAG field of any record having a COUNTER value = or >  #
#  then the value stored in the MUGcount user setting                        #
#
########################################################
#
# Insert the lists that will be scrubed below
set_field list1 STATUSFLAG Z -s"COUNTER:>=$var2;STATUSFLAG:=$var3"
set_field list2 STATUSFLAG Z -s"COUNTER:>=$var2;STATUSFLAG:=$var3"
set_field list3 STATUSFLAG Z -s"COUNTER:>=$var2;STATUSFLAG:=$var3"
# set_field list25 STATUSFLAG Z -s"COUNTER:>=$var2"
#
print $var2 > test111
#read a
> dptest
exit
```

6. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Call Guard.

Log into the Linux shell of the Proactive Contact server, and enter "menu sysadm" to display the **ADMINISTRATOR MAIN MENU** screen. Verify that two new options associated with CALLGUARD are displayed, as shown below. Enter "12" for **CALLGUARD Call Limit Manager**.

```
                          ADMINISTRATOR MAIN MENU

   0. Exit
   1. Display help

   2. Administrative tasks
   3. Back up, restore and verify
   4. Manage backup configuration file
   5. Inbound calling lists
   6. IVR administration
   7. Transfer and process records
   8. Voice messages
   9. Manage database accounts
  10. View customer support information
  11. View APS information
  12. CALLGUARD Call Limit Manager
  13. CALLGUARD

  Enter Command Number: 12
```

The screen below is displayed next. The warning at the top of the screen is displayed upon initial invocation, and can be ignored as the **MUGcount** parameter will be set subsequently. Enter a desired triggering value, such as "6".

```
/opt/avaya/pds/customs/MUGset: line 9: /opt/avaya/pds/customs/MUGcount: No such file
or directory



          MUG ENTERPRISE CALL LIMIT MANAGEMENT APPLICATION

          The Current Call Count setting is



          Enter the call count setting, a number between 1-9

          Input the desired setting here 6
```

The screen is updated with additional line toward the bottom, showing the limit trigger has been set.

```
/opt/avaya/pds/customs/MUGset: line 9: /opt/avaya/pds/customs/MUGcount: No such file
or directory



          MUG ENTERPRISE CALL LIMIT MANAGEMENT APPLICATION

          The Current Call Count setting is



          Enter the call count setting, a number between 1-9

          Input the desired setting here 6



          The number is valid and will be the limit trigger


                 HIT ENTER TO CONTINUE
```

Press the **Enter** key, and the **ADMINISTRATOR MAIN MENU** is displayed next. Enter "13" for **CALLGUARD**. Verify that the **ADMINISTRATION MAIN MENU** screen is shown again at the end of successful script run.

```
                          ADMINISTRATOR MAIN MENU

   0. Exit
   1. Display help

   2. Administrative tasks
   3. Back up, restore and verify
   4. Manage backup configuration file
   5. Inbound calling lists
   6. IVR administration
   7. Transfer and process records
   8. Voice messages
   9. Manage database accounts
  10. View customer support information
  11. View APS information
  12. CALLGUARD Call Limit Manager
  13. CALLGUARD

  Enter Command Number: 13
```

7. Conclusion

These Application Notes describe the configuration steps required for MUG Enterprise Call Guard to successfully interoperate with Avaya Proactive Contact with CTI. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

8. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at http://support.avaya.com.

3. *Administering Avaya Proactive Contact*, Release 5.1, April 2013, available at http://support.avaya.com.

4. *Call Guard Installation Notes*, Rev 2.2, 8/18/15, available upon request to MUG Enterprise Support.

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.