Product Release Notes for Avaya Proactive Contact Dialer 4.0

COMPAS Document Number : 127858

Authorization	Name	Date
Current Issuer	*Kishor Mahajan*	18th Feb 2008
Technical Manager	*Girish Khilari*	18th Feb 2008

The author shall also add appropriate people to the COMPAS notification list at the first release.

Revision history

Issue	Date	Description
1	7th May 2007	Initial Release to System Verification.
2	21st May 2007	Release of 4.0.0.0.22 Build to SV
3	29th May 2007	Release of 4.0.0.0.23 Build to SV
4	12th June 2007	Release of 4.0.0.0.25 Build to SV
5	12th July 2007	Release of 4.0.0.0.30 Build to SV
6	1st Aug 2007	Release of 4.0.0.0.31 Build to SV
7	13th Aug 2007	Release of 4.0.0.0.32 Build to SV
8	1st Oct 2007	Release of 4.0.0.0.38 Build to SV
9	17th Oct 2007	Release of 4.0.0.0.39 Build to SV
10	26th Nov 2007	Release of Gold Master (4.0.0.0.39 repackaged with patches) Build to SV
11	18th Feb 2008	Release of Localized 4.0.0.64.39 (4.0.0.0.39 repackaged with language installation support) Build to SV

Table of Contents

1. Release Subject

This document is the release notes and installation notes for Avaya Proactive Contact Dialer 4.0.

1.1. Part Number / Version

Avaya Proactive Contact Dialer 4.0 Gold Master (4.0.0.64.39 repackaged with patches)

1.2. Context of the Release

This is a major new release for this product including language support.

1.3. Audience

System Verification

1.4. Supersedes

Avaya Proactive Contact Dialer 3.0 and Avaya Proactive Contact Dialer 3.0 Service Pack 1, Avaya Proactive Contact Dialer 4.0.0.0.39

1.5. Included Patches

None

1.6. Dependencies / Restrictions

None

1.7. References

Document Number	Document Name
117833	Requirements for Proactive Contact Security Compliance
121729	Kimaya Agent Keys Design
121703	Design Definition for Kimaya: Licensing
122351	Design document Scheduled Dialer Operations for Admin Manager
125022	Proactive contact HLD for Security
116965	Proactive Contact 4.0 Administration Requirements (Agent keys, Schedules, Staging)
118396	Proactive Contact 4.0 Calling List Management
105508	Licensing Feature Requirements Specification (FRS) for Kimaya
116963	Common Requirements for Proactive Contact 4.0 (Kimaya) (On Documentation)
118643	Proactive Contact Release 4.0 Product Requirements Document

2. Problem Definition / Reason for Release

This is a new release of Avaya Proactive Contact Dialer and supersedes the current 3.0, 3.0.1 and 4.0.0.0.39 releases.

2.1. Major Bug Fixes

None

2.2. Changes in Functionality

It Includes:

1) Localization installation support for all the supported languages.

3. Release Overview

3.1. Files Report

None

4. Release Details

4.1. Binaries Modified

All required binaries are modified to work on Linux

4.2. Binaries Added

Please refer to "PC4 0_AdditionsRemoval_ToBuild.xls" appended in Appendix B

4.3. Binaries Deleted

Please refer to "PC4 0_AdditionsRemoval_ToBuild.xls" appended in Appendix B

4.4. Directories Added

Please refer to "PC4 0_AdditionsRemoval_ToBuild.xls" appended in Appendix B

4.5. Directories Deleted

Please refer to "PC4 0_AdditionsRemoval_ToBuild.xls" appended in Appendix B

4.6. Files Modified

All required files are modified to work on Linux

4.7. Files Added

Please refer to "PC4 0_AdditionsRemoval_ToBuild.xls" appended in Appendix B

4.8. Files Deleted

Please refer to "PC4 0_AdditionsRemoval_ToBuild.xls" appended in Appendix B

4.9. Files Moved or Renamed

No files were renamed in this release.

4.10. Interfaces Modified

No interfaces were changed.

4.11. Interfaces Added

No interfaces were added.

4.12. Interfaces Deleted

No interfaces were deleted by this release.

4.13. Components Modified

No components modified

4.14. Components Added

No new components were added by this release.

4.15. Components Deleted

No components were deleted by this release.

5. Release Installation

This section describes how to install and uninstall this release.

5.1. Hardware Requirements

The following are the minimum hardware requirements to support this release of the Dialer and the associated mid-tier software components:

- HP Proliant DL 385G2 Rack Server / (1) Dual-Core AMD Opteron 2218 Processor (2.6 GHz, 95 Watts) / 2MB (2 x 1MB) Level 2 cache / Embedded Dual NC373i Multifunction Gigabit NICs / HP Smart Array P400/256MB Controller (RAID 0/1/5) / Hot Plug Fully Redundant Fans Standard
- 8 GB RAM
- 146 GB * 3 free disk space on hard drive regardless of its total size
- DVD RW
- Network capable

5.2. Installation Instructions

- Note: The OS and Dialer should be installed in the same time zone. Please refer to Info Dev documentation “AdminGuide.pdf” for setting dialer time zone as per local.

5.3. Pre-Installation Procedure

- Install RHEL OS Version PC4.0.0.0.13.iso
- In case you want to do dialer installation from RS-232 console, then login to the system with root privileges and then execute command “/sbin/lilo” and then reboot the system before stating installation of Dialer.

5.4. Upgrade Instructions

NA.

5.5. Installation Procedure

Note (For more information, refer to Appendix G for README and Appendix H for Distribution area).

1) Insert Dialer installation CD in the Linux Dialer system DVD-ROM.
2) Log in as sroot to the system and go to the path "/mnt"
3) Execute the command "mount cdrom"

4) Go to the path "/mnt/cdrom"

5) Execute the script "DialerInstaller".

After initial prompts all Dialer related RPM's are installed.

Then the MIDTIER packages are copied in the /tmp/midtier/ path of the Linux machine.

6) In case you want to install IVR also on the system, then again execute

“DialerInstaller” script and this time select IVR option in the initial prompts. And it will install IVR package on the dialer system.

7) Execute “eject” command and remove the DIALER CD from the Linux machine and insert the ORACLE CD in the CDROM.

8) Follow steps 2 and 3 to mount the ORACLE CD.

9) Go to the path "/mnt/cdrom" again and run script "OracleInstaller".

After initial prompts it will install ORACLE RPM's.

10) After installation of ORACLE, go to “/tmp/midtier/” path and run script "MidtierInstaller". After initial prompts all Midtier packages are installed.

5.6. Post-Installation Procedure

1) Install latest Dialer SP (4.0.1.003.018 or above) for localization support.

2) For configuring the Dialer using SFTP for hosttopds and pdstohost, please refer to Appendix C.

3) For configuring the Dialer for using LDAP support, please refer to Appendix F.

4) For configuring the Network printer on dialer please refer to Appendix E.

5) For verifying build version log in to the dialer with admin user and open file /var/log/Dialer-4.0.0.0.x-Install.log and check for “Dialer SCM released version” info in it.

5.7. Uninstall Procedure

N A.

6. Special Testing Requirements

None.

7. Install Verification

Check all newly added files are available after installation.

Please refer to “PC4 0_AdditionsRemoval_ToBuild.xls” appended in Appendix B

8. Known Issues

Please refer to “KnownIssues.xls from Appendix A, for detail listing and workaround of the open issues.

9. Patches included in this release

The patches merged in the build were treated as a work item and details of the same are available in the work item resolution listing. Refer to Clear Quest for details.

10. File Listing

NA

11. Build ID of CQ

APC:Dialer	=>	wi00048714
APC:DBOra	=>	wi00045042

Appendix A Known Issues

Please refer to Dialer Service Pack 4.0.1 Release note (CID 133407) for Know issue list.

Appendix B PC4 0_AdditionsRemoval_ToBuild.xls

D:\PC4
0_AdditionsRemoval_

Appendix C SFTP Configuration without Password

Purpose

As we migrate to more secure systems, convenient utilities such as FTP and TELNET will be replaced with more secure systems. Secure Shell (ssh) and Secure Copy (scp) are the standard replacements for these. Here **machine B** is the name of server to which you want to connect and **machine A** is the client. The server will not prompt for the password. The secure connection will be established between the server and the client.

Setting up the keys

1. Login as **user1** (e.g admin) on **machine A** (e.g 135.27.151.17) and generate a pair of Authentication keys. On the terminal session, type **ssh-keygen -t rsa**. Press <ENTER> for the next 3 questions. The above command will create the **.ssh** directory under the users' home directory.

   Run command # ssh-keygen –t rsa

   To ensure that the permissions of the home directory of the client, the $HOME/.ssh directories, and all files under the $HOME/.ssh directory match the permissions listed below.

   Run the following commands:

   #ll -d $HOME
   #ll -d $HOME/.ssh
   #ll $HOME/.ssh/
   Below are the specific permissions for these files and directories. Make sure that you have these permissions set.

$HOME (home directory)	**drwx------ OR drwxr--r--**
$HOME/.ssh	**drwx------ OR drwxr--r--**

$HOME/.ssh/id_rsa and id_dsa	**-rw-r--r—- OR -rw------**
$HOME/.ssh/id_rsa.pub and id_dsa.pub	**-rw-r--r-- OR -rw------**
$HOME/.ssh/config	**-rwx------**

2. Now use ssh to create a .ssh directory as **user2 i.e. craft** on **machineB**(135.27.151.16) (many Linux distributions create this folder by default. No problem with that.). You still need the password for now....

   Run command #ssh –l craft 135.27.151.16 mkdir –p .ssh

```
PUDSLX15(admin)@/opt/avaya/pds [3]
$ ssh -l craft 135.27.151.16 mkdir -p .ssh
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

                              ***  WARNING NOTICE  ***

This system is restricted solely to Avaya authorized users for legitimate
business purposes only. The actual or attempted unauthorized access, use,
or modification of this system is strictly prohibited by Avaya. Unauthorized
users are subject to Company disciplinary proceedings 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 is advised that if monitoring reveals possible
```

   Set the directory and file permissions on the server (MachineB) as :

$HOME (home directory)	**drwx------ OR drwxr--r--**
$HOME/.ssh	**drwx------ OR drwxr--r--**
$HOME/.ssh/authorized_keys	**-rw-r--r—OR -rw----**

3. Copy the **user1 (admin)** public key to **user2 (craft)** user2@machineB .ssh folder into authentication_hosts file. And, type the password again for the last time, hopefully...

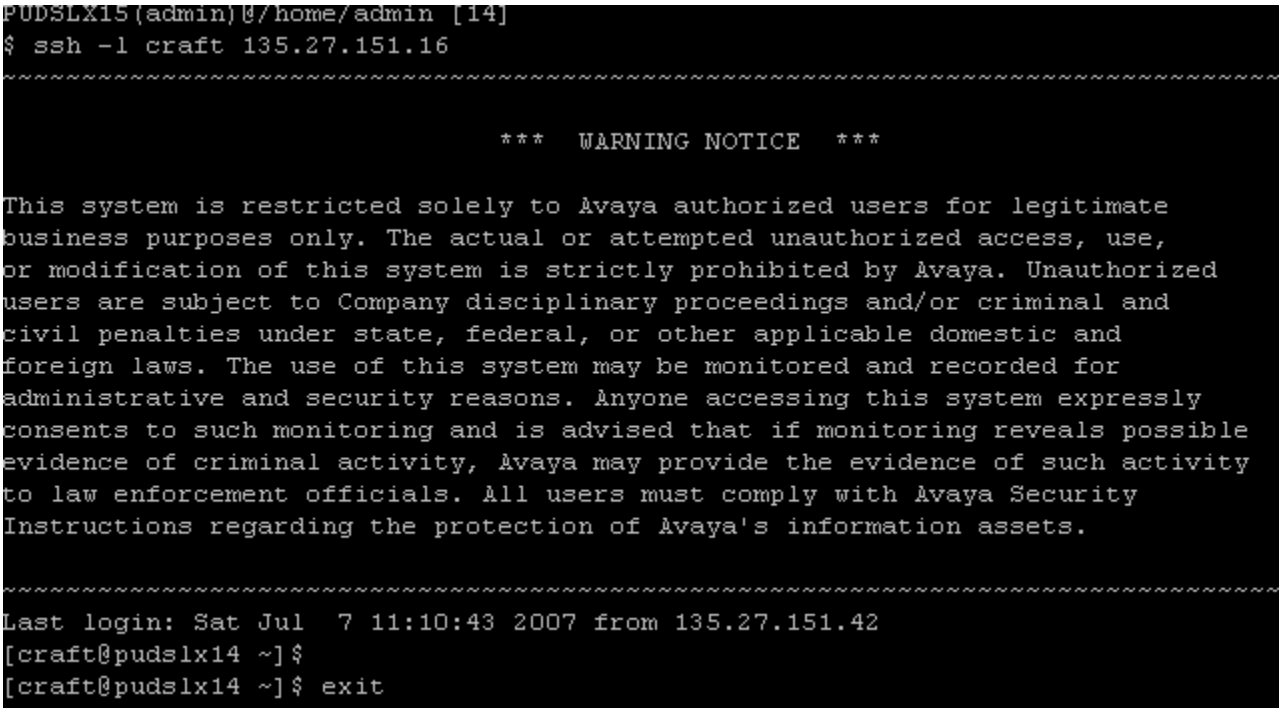
   Make sure that you are in $HOME directory.
   cd $HOME
   #cat $HOME/.ssh/id_dsa.pub ssh –l admin 135.27.151.16 'cat >> $HOME/.ssh/authorized_keys'

```
$
PUDSLX15(admin)@/home/admin [13]
$ cat .ssh/id_rsa.pub | ssh -l craft 135.27.151.16 'cat >> .ssh/authorized_keys'
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

                              ***  WARNING NOTICE  ***

This system is restricted solely to Avaya authorized users for legitimate
business purposes only. The actual or attempted unauthorized access, use,
or modification of this system is strictly prohibited by Avaya. Unauthorized
users are subject to Company disciplinary proceedings 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 is advised that if monitoring reveals possible
evidence of criminal activity, Avaya may provide the evidence of such activity
to law enforcement officials. All users must comply with Avaya Security
Instructions regarding the protection of Avaya's information assets.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Password:
PUDSLX15(admin)@/home/admin [14]
$ ssh -l craft 135.27.151.16
```

To enable public-key authentication, set the following directive in the server configuration file /opt/ssh/etc/sshd_config:
PubkeyAuthentication **yes**

Note: For machine other then dialer you need to set this value. For dialer it's already set to YES.

4 If all things are OK, you don't need the password.
Run #ssh –l craft 135.27.151.16
The server does not prompt for the password. The secure connection is established between the server and the client


PUDSLX15(admin)@/home/admin [14]
$ ssh -l craft 135.27.151.16
*** WARNING NOTICE ***
This system is restricted solely to Avaya authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited by Avaya. Unauthorized users are subject to Company disciplinary proceedings 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 is advised that if monitoring reveals possible evidence of criminal activity, Avaya may provide the evidence of such activity to law enforcement officials. All users must comply with Avaya Security Instructions regarding the protection of Avaya's information assets.
Last login: Sat Jul 7 11:10:43 2007 from 135.27.151.42
[craft@pudslx14 ~]$
[craft@pudslx14 ~]$ exit

Appendix D FTP and Telnet configuration

A) FTP Configuration

To enable FTP service

1. Login as sroot uncomments following line in /etc/firewall/conf/cs-rules.sh.
   #$IPTABLES -A INPUT -p tcp --dport 21 -j ACCEPT

2. Find the service name
   #chkconfig --list|grep ftp
   gssftp.orig: off
   gssftp: off

3. Turn on the service using the command #chkconfig gssftp on

4. Configuration
   Change the server_args = -l –a parameter from the /etc/xinetd.d/gssftp file to the server_args = -l

5. Restart the system using command
   "/sbin/shutdown –r now"

** NOTE: ftp using anonymous user cannot be configured using gssftp.

B) Telnet Configuration

To enable telnet service

1. Login as sroot add these lines in /etc/firewall/conf/cs-rules.sh.

   $IPTABLES -A INPUT -p tcp --dport 23 -j ACCEPT
   $IPTABLES -A INPUT -p udp --dport 23 -j ACCEPT

   Add these lines after
   # ftp
   #$IPTABLES -A INPUT -p tcp --dport 21 -j ACCEPT

2. Find the service name
   #chkconfig --list|grep telnet
   krb5-telnet: off

3. Turn on the service using the command #chkconfig krb5-telnet on.

4. Restart the system using command
   "/sbin/shutdown –r now"

Appendix E Network Printer Configuration

For Configuring Network printer

1) Login to the dialer as sroot user
2) Go to path /usr/share/cups/model/
3) Unzip the tar file of printer as per available network or desktop printer using command "gunzip" (do not use tar -xzvf ...)
4) Go to path /usr/sbin/
5) Execute command

./lpadmin -p LaserJet -E -v socket:**"//135.27.156.46/avpun-HP4350-7"** -m laserjet.ppd

Where

1. "//135.27.156.46/avpun-HP4350-7" is the IP of the network printer
2. "laserjet.ppd" is the name of file unzipped in "/usr/share/cups/model/"

For more information, read the help of lpadmin for other printer configurations like desktop printers

For printing use the command

lp " file name"

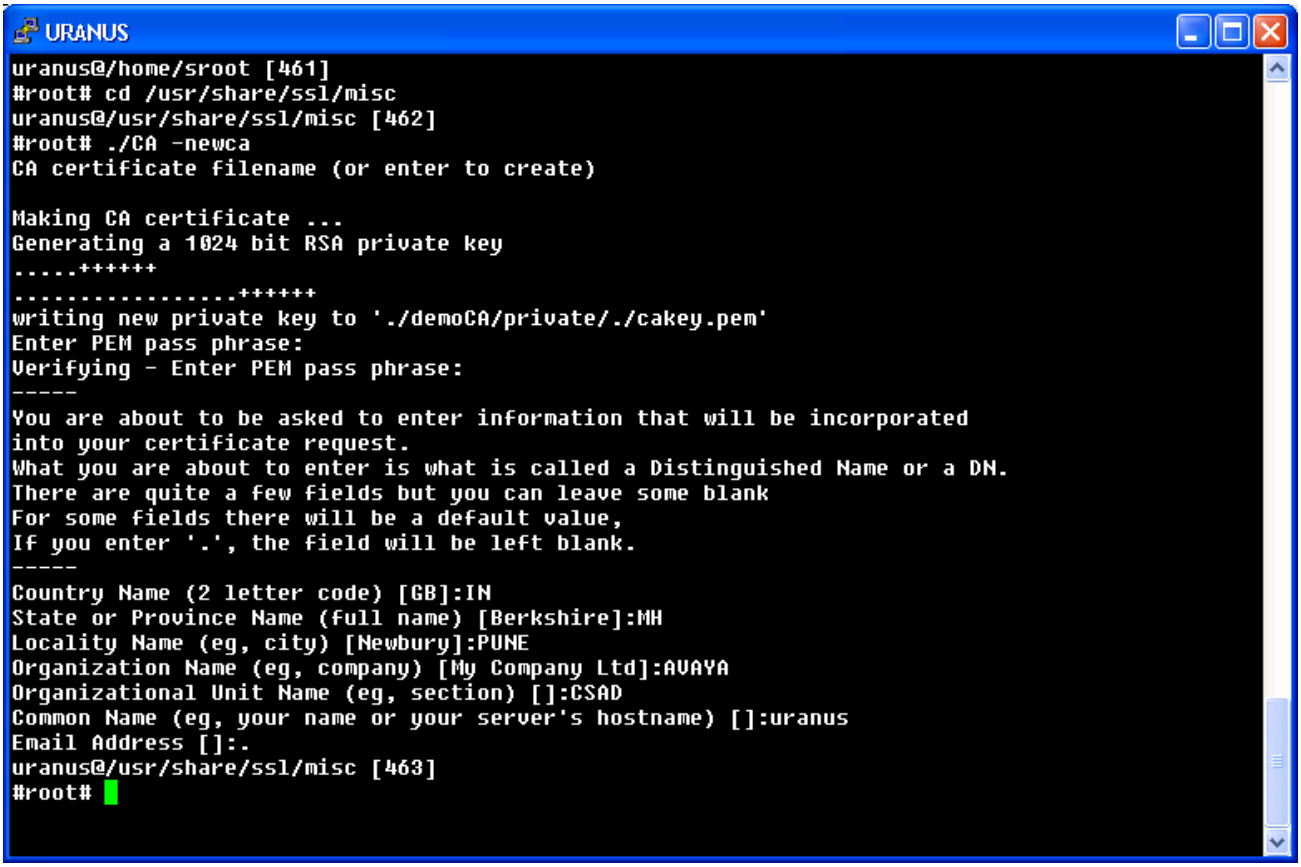
For checking printer queue use the command

lpq

Appendix F LDAP Configuration

LDAP Server Installation and Configuration Guide

1) Generate the certificates using OpenSSL
   - Login as sroot.
   - Go to /usr/share/ssl/misc
   - Type ./CA –newca
     This will create your ca certificate.
   - Press Enter, when prompted for "CA certificate filename (or enter to create)"
   - Enter a pass phrase (minimum 4 chars), when prompted for "Enter PEM pass phrase:"
   - Re-enter the pass phrase, when prompted for "Verifying - Enter PEM pass phrase:"
   - Enter the following information as appropriate:
     Country Name (2 letter code) [GB]:
     State or Province Name (full name) [Berkshire]:
     Locality Name (eg, city) [Newbury]:
     Organization Name (eg, company) [My Company Ltd]:
     Organizational Unit Name (eg, section) []:
     Common Name (eg, your name or your server's hostname) []: Provide the hostname of the LDAP server)
     Email Address []:.



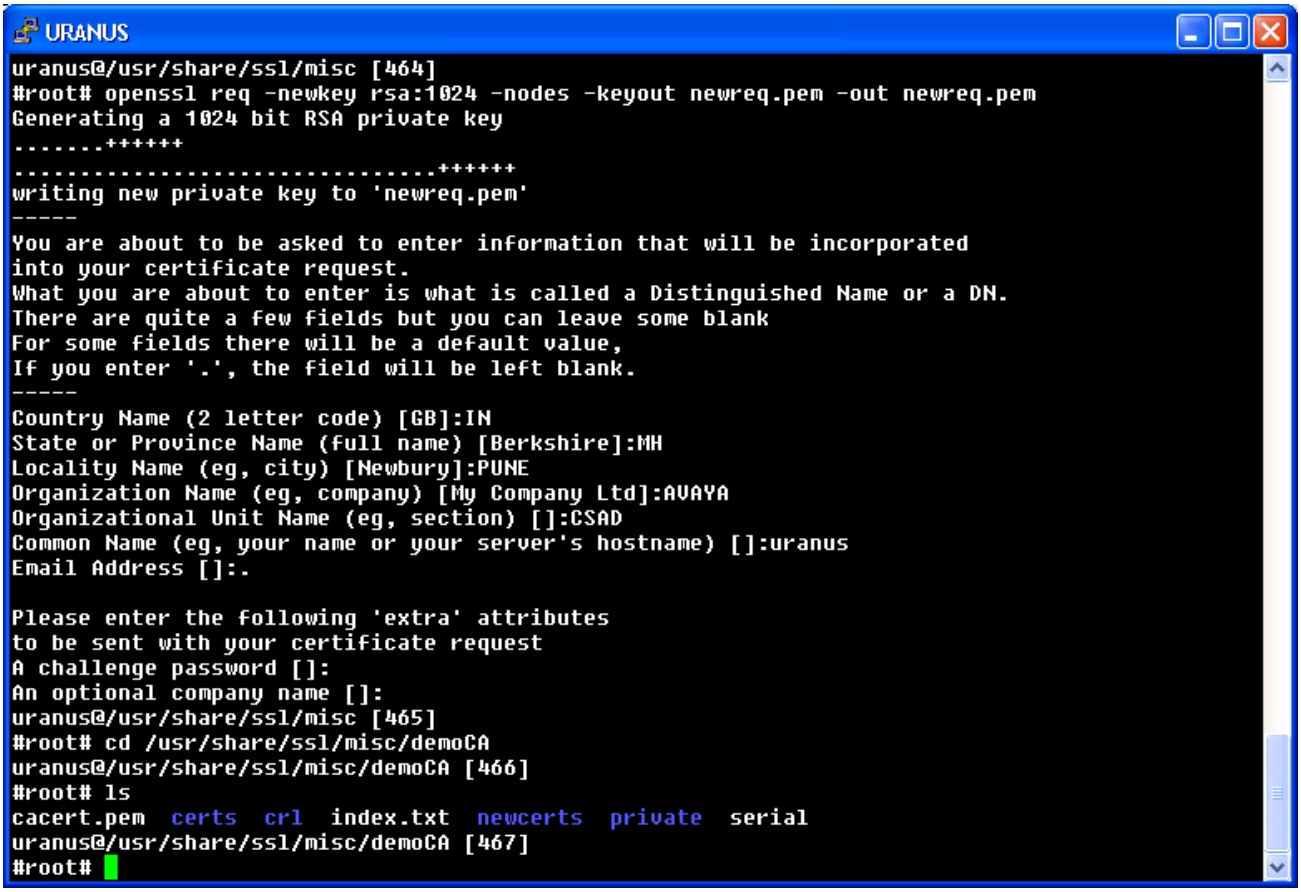
2) Make your server certificate signing request (CSR):

- Execute the following:
  openssl req -newkey rsa:1024 -nodes -keyout newreq.pem -out newreq.pem

- Enter the following information. It should match the information provided in section 1.1 :
  Country Name (2 letter code) [GB]:
  State or Province Name (full name) [Berkshire]:
  Locality Name (eg, city) [Newbury]:
  Organization Name (eg, company) [My Company Ltd]:
  Organizational Unit Name (eg, section) []:
  Common Name (eg, your name or your server's hostname) []:
  Email Address []:

- Please enter the following 'extra' attributes to be sent with your certificate request
  A challenge password []: (leave this field blank)
  An optional company name []: (leave this field blank)

- This will create cacert.pem on following location
  /usr/share/ssl/misc/demoCA/cacert.pem
  This is your ca's certificate



3) CA sign the CSR:

- Make sure you are at the location /usr/share/ssl/misc

- Execute the following:
  /usr/share/ssl/misc/CA –sign

- Enter the pass phrase provided during "section 1.1", when prompted for "Enter pass phrase for ./demoCA/private/cakey.pem:"

- Enter 'y' when prompted for the following:
  Certificate is to be certified until Dec 12 22:13:19 2008 GMT (365 days)
  Sign the certificate? [y/n]:

- Enter 'y' when prompted for the following:
  1 out of 1 certificate requests certified, commit? [y/n]

4) Create dir cacerts in /etc/openldap with the following permissions, if not already present.
drwxr-xr-x 2 root root 4096 Nov 22 23:42 cacerts

5) Create dir certs in /etc/openldap with the following permissions
drwxr-xr-x 2 root root 4096 Nov 21 08:18 certs

6) Copy all the certs

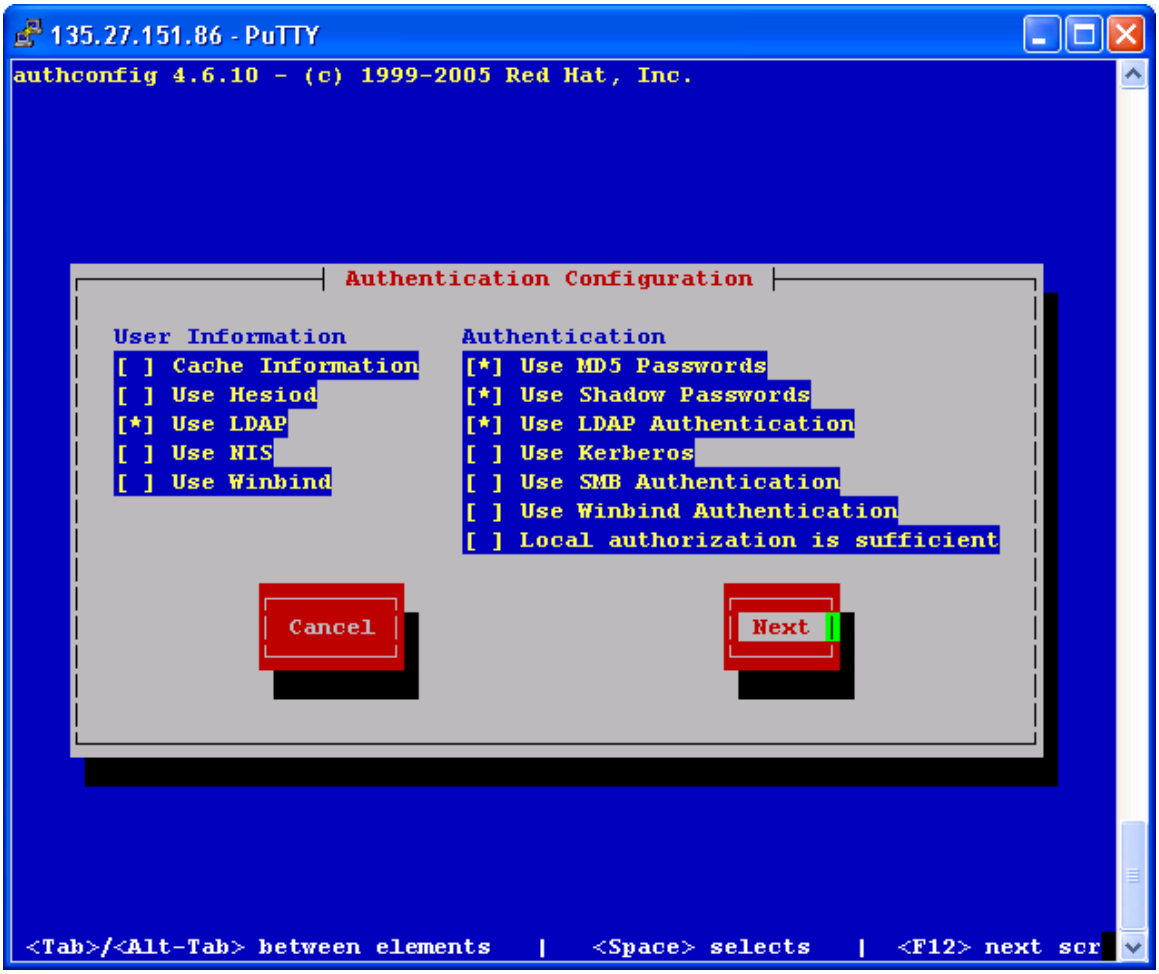
- Go to /usr/share/ssl/misc
  cp demoCA/cacert.pem /etc/openldap/cacerts/cacert.pem
  cp newcert.pem /etc/openldap/certs/servercrt.pem
  cp newreq.pem /etc/openldap/certs/serverkey.pem

7) Edit slapd.conf and add following entries to it

Location:- /opt/avaya/pds/tools/ldap/slapd.conf

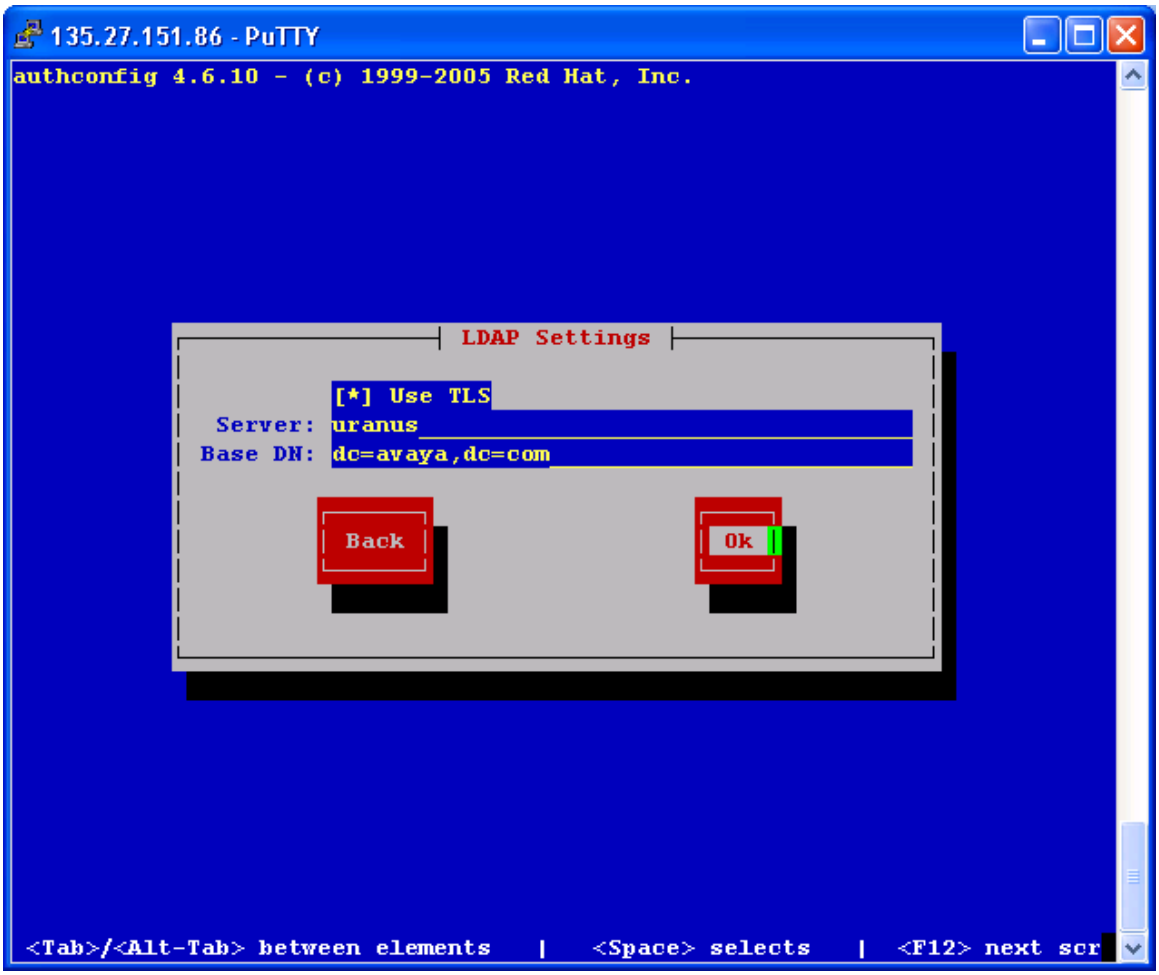
Entries:-
TLSCACertificateFile /etc/openldap/cacerts/cacert.pem
TLSCertificateFile /etc/openldap/certs/servercrt.pem
TLSCertificateKeyFile /etc/openldap/certs/serverkey.pem
TLSVerifyClient never

8) As root run “authconfig” command
On the Authentication Configuration Screen:
Mark the option "Use LDAP" under "User Information".
Mark the option "Use LDAP Authentication" under "Authentication".



- On the "LDAP Settings" screen:
  Mark the option "Use TLS"

Provide the hostname of the LDAP server for "Server:"
Provide the "Base DN:" as appropriate.



9) Edit /etc/ldap.conf add following entries in it

ssl yes
port 636
TLS_REQCERT never

Your file will look like this:

```
ssl start_tls
ssl yes
TLS_REQCERT never
pam_password md5
host uranus
base dc=avaya,dc=com
port 636
tls_cacertdir /etc/openldap/cacerts
```

10) Check localhost entry in /etc/hosts file as.

127.0.0.1 localhost

If the entry is not present then add the entry

11) Add following entry in /etc/hosts.allow file
slapd = machine's IP addr

Note: There is a white space after and before "=" sign.

12) Set LDAP flag to YES in master.cfg as below
LDAP:YES

13) Login as a sroot user and execute following script
LdapServerInstaller.sh -D {"your domain name"}

For example: LdapServerInstaller.sh -D avaya

14) Run "ldconfig" command

15) To verify all the entries in the LDAP run following command
ldapsearch -x -b 'dc={domain name},dc=com' '(objectclass=*)'

For example: ldapsearch -x -b 'dc=avaya,dc=com' '(objectclass=*)'

Troubleshooting Tips:-
If client is not able to connect to server check that ssl yes entry is present in /etc/ldap.conf

LDAP Client Installation and Configuration Guide

Configuring/Starting LDAP/DB

Refer LDAP server installation README

1) Follow these commands for secondary dialer (LDAP client)

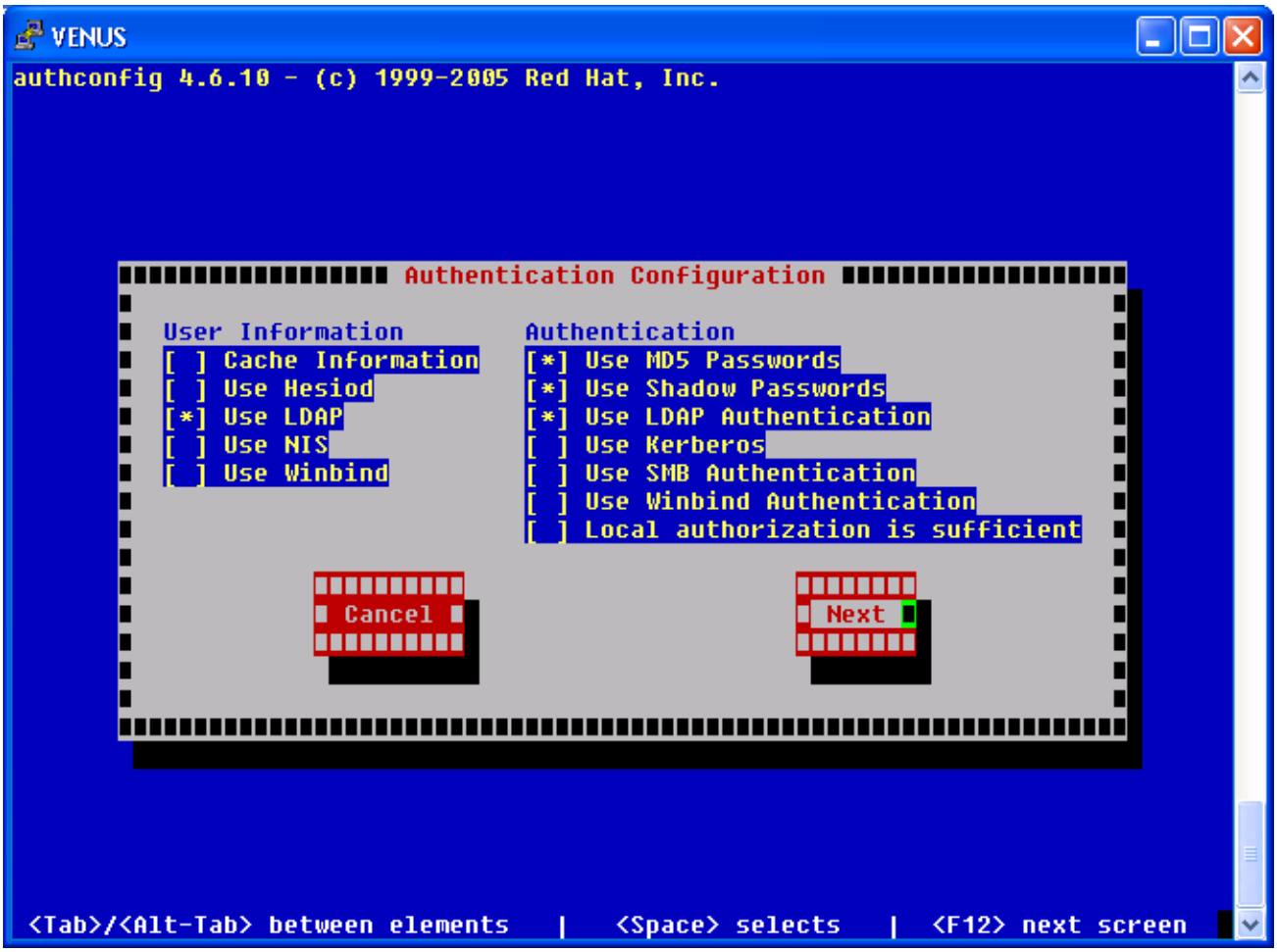
   1: Set LDAP flag to YES in master.cfg as follows:
   LDAP:YES

   2: As sroot user run the following script
   LdapClientInstaller.sh

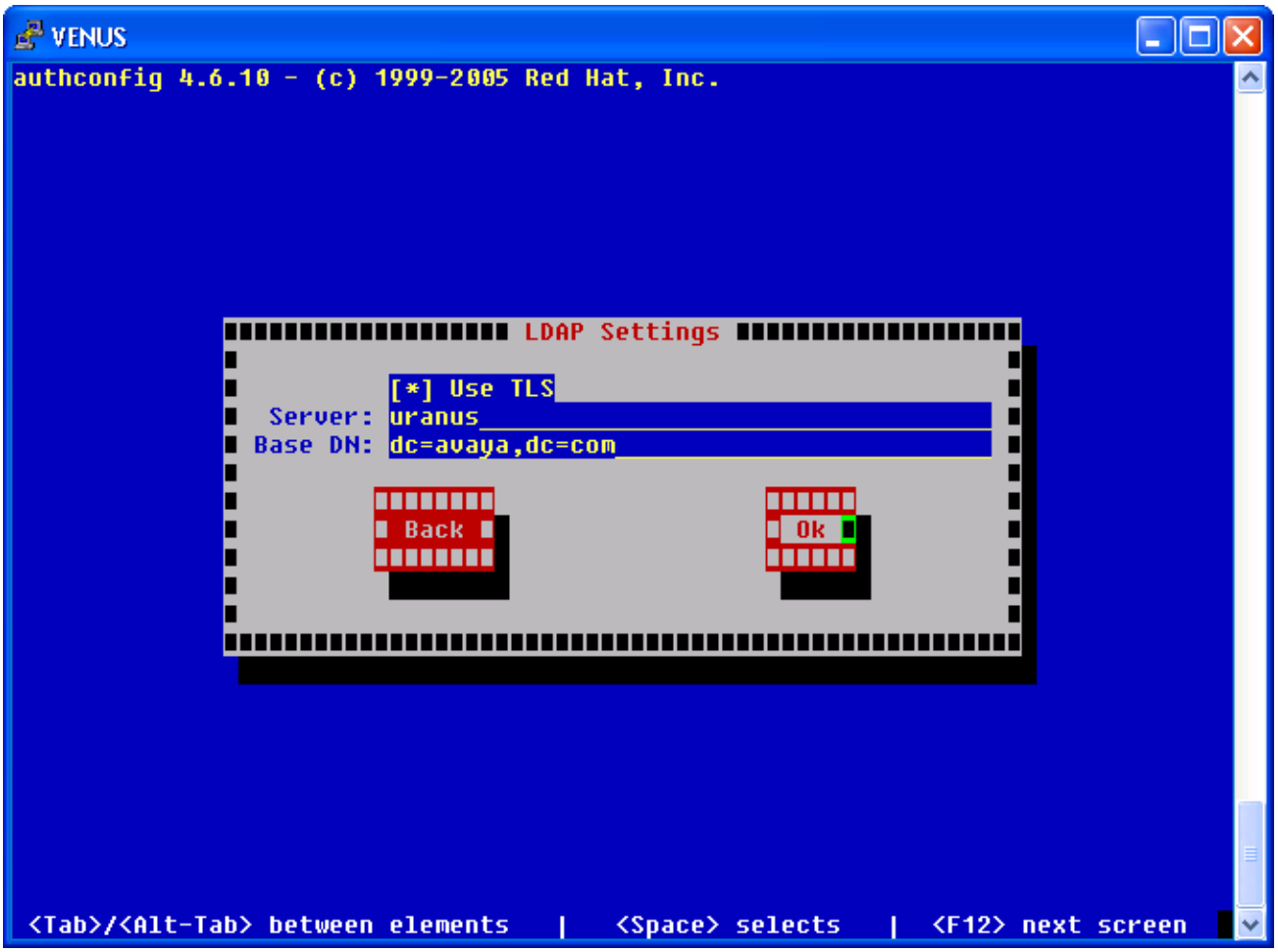
2) Create dir cacerts in /etc/openldap with the following permissions
   drwxr-xr-x 2 root root 4096 Nov 22 23:42 cacerts

3) FTP /etc/openldap/cacerts/cacert.pem from your server machine to client machine
   Copy it to /etc/openldap/cacerts/cacert.pem

4) Run “authconfig” command
   On the Authentication Configuration Screen:
   Mark the option "Use LDAP" under "User Information".
   Mark the option "Use LDAP Authentication" under "Authentication".



On the "LDAP Settings" screen:
Mark the option "Use TLS"
Provide the hostname of the LDAP server for "Server:"
Provide the "Base DN:" as appropriate.



5) Edit /etc/ldap.conf add following entries in it

ssl yes

port 636

Troubleshooting Tips:-

If client is not able to connect to server check that ssl yes entry is present in /etc/ldap.conf

Appendix G Readme

This is a preliminary release of the Linux version of the Dialer. The files distributed by this release are as follows:

Dialer Installation CD
- Proactive_Contact_ADMIN-4.0.0.x-1.i386.rpm
- Proactive_Contact_BLEND-4.0.0.x-1.i386.rpm
- Proactive_Contact_BLENDBASE-4.0.0.x-1.i386.rpm
- Proactive_Contact_CHINESE_SIMPLIFIED-4.0.0.x-1.i386.rpm
- Proactive_Contact_DIALER-4.0.0.x-1.i386.rpm
- Proactive_Contact_DIALERBASE-4.0.0.x-1.i386.rpm
- Proactive_Contact_ENGLISH-4.0.0.x-1.i386.rpm
- Proactive_Contact_FRENCH_FRANCE-4.0.0.x-1.i386.rpm
- Proactive_Contact_GERMAN-4.0.0.x-1.i386.rpm
- Proactive_Contact_ITALIAN-4.0.0.x-1.i386.rpm
- Proactive_Contact_IVR-4.0.0.x-1.i386.rpm
- Proactive_Contact_JAPANESE-4.0.0.x-1.i386.rpm
- Proactive_Contact_KOREAN-4.0.0.x-1.i386.rpm
- Proactive_Contact_MANBASE-4.0.0.x-1.i386.rpm
- Proactive_Contact_MIDTIER-4.0.0.x-1.i386.rpm
- Proactive_Contact_MTBASE-4.0.0.x-1.i386.rpm
- Proactive_Contact_MTDBASE-4.0.0.x-1.i386.rpm
- Proactive_Contact_PORTUGUESE_BRAZIL-4.0.0.x-1.i386.rpm
- Proactive_Contact_RUSSIAN-4.0.0.x-1.i386.rpm
- Proactive_Contact_SPANISH_INTL-4.0.0.x-1.i386.rpm
- Proactive_Contact_TZONEBASE-4.0.0.x-1.i386.rpm
- DialerInstaller
- DialerUninstaller
- MidtierInstaller
- MidtierUninstaller
- README

Oracle Installation CD
- Proactive_Contact_ORACLE-4.0.0.0.x-1.i386.rpm
- add.swap
- OracleInstaller
- OracleUninstaller

(Where ".x" is the version number for ex. 4.0.0.0.26 etc)

##

Prior to installing this release, log in as sroot and verify the following information:

1. The file /etc/resolv.conf contains an entry for a domain.
   For example,

   domain rnd.avaya.com

   Use the domain name which is appropriate for the system being installed.

2. The file /etc/hosts has an entry containing the IP address of the machine on which this software is being installed. The order in that entry should be IP address followed by machine name followed by machinename.domainname.
For example,

135.27.151.15 pudslx13 pudslx13.rnd.avaya.com

3. The HOSTNAME entry in the file /etc/sysconfig/network matches the machine name specified in the file /etc/hosts.

4. If you want to install the dialer from console (through RS-232 communication) execute command:

/sbin/lilo

After executing the above command, restart the Dialer by executing the command:

/sbin/shutdown -r now

##

To install this release, insert the Dialer installation cd in the system, log in to the system as sroot and execute the following commands:

```
cd /mnt
mount cdrom
cd cdrom
./DialerInstaller
```

You will see the following prompt:

```
[
Installing Proactive Contact 4.0.0.0.x Dialer packages

Note: This installation requires that the Dialer and the IVR be installed separately i.e. first the Dialer and
then the IVR.

Please select a product to install:
  1: Dialer
  2: IVR      {Note: Dialer must be installed before installing IVR.}
  q: Quit installer
]
```

At the prompt select 'Dialer' and you will get the following prompt:

```
[
Please select a language to install:
  1: English
  2: Simplified Chinese
  3: French for France
  4: German
  5: Italian
  6: Japanese
  7: Korean
  8: Portuguese for Brazil
  9: Russian
 10: International Spanish
```

```
  q: Quit installer
]
```

At the prompt select required Language to be installed and you will get the next prompt:

```
[
Please select the packages to be installed:
  1: Dialer
  2: Blend (Note: Dialer must be installed before installing Blend)
  3: Dialer and Blend
]
```

At the prompt select appropriate installation packages. This will start installing packages on the system. It will install the following packages:

'LANGUAGE PACK'
ADMIN
DIALERBASE
DIALER
TZONEBASE
MANBASE
BLENDBASE (If selected)
BLEND (If selected)

After installing all the packages, check if you are able to log in to the system as 'sroot'. Check whether the "/tmp/midtier" folder is created on Linux Dialer machine and it contains the following set of files:

MidtierInstaller
MidtierUninstaller
Proactive_Contact_MIDTIER-4.0.0.0.x-1.i386.rpm
Proactive_Contact_MTDBASE-4.0.0.0.x-1.i386.rpm
Proactive_Contact_MTBASE-4.0.0.0.x-1.i386.rpm
README

##

Remove the Dialer Installation CD, insert the Oracle Installation CD, and execute the following commands:

```
cd /mnt
mount cdrom
cd cdrom
./OracleInstaller
```

You will get the following prompt

```
[
  Installing Proactive Contact 4.0.0.0.x Oracle package

  Note: This installation requires the Dialer packages.  If the Dialer has not been installed, install the Dialer before installing Oracle.

  Have you installed the Dialer packages? (Y or N)
]
```

At the prompt press 'Y' on the keyboard. The system will start installing Oracle.

Note: Based on the system performance, it will take approximately 75 minutes to install the complete Oracle package.

It will install the following package:

ORACLE

##

After the Oracle is installed, check if you are logged in to the system as a 'sroot' user, if not, then please relogin as "sroot". After logging in as 'sroot' go to "/tmp/midtier" path and execute the following command:

./MidtierInstaller

You will get the following prompt:

[
Installing Proactive Contact 4.0.0.0.x Mid-Tier Package

Note: This installation requires the Dialer and Oracle to be installed. If the Dialer and Oracle has not been installed, then install the Dialer and Oracle before installing Mid-Tier.

Have you installed the Dialer and Oracle Package? (Y or N)
]

At the prompt press 'Y' on the keyboard. The system will start installing Mid-Tier. It will install the following packages:

MTBASE
MIDTIER
MTDBASE

##

After the installation has finished, log off, and then log in as admin.
After logging in as admin, execute the following steps:

1. Execute the command:
   stop_db

2. Edit master.cfg to set the following parameters:
   DBSERVERIP: IP address of Dialer
   DIALERID: ID number desired
   NAMESERVICEHOST: machine name from /etc/hosts
   PRIMARY: YES
   WEBLMURL: WEBLM URL (eg. http,//135.27.151.44,8080/WebLM/LicenseServer:)

3. Execute command:
   manage_corba_users -D <DIALERID> -A
   (eg. "manage_corba_users -D 10 -A")

4. Configure the Mid-Tier software by running the following commands:
   start_db
   gennis

StartThinAgent (This command may give Oracle certificate validation error, Please ignores it as it will get taken care once Dialer SP1 (4.0.1.003.018 or above) version is installed.)
mtsconfigure
start_mts
heck_mts
heck_db

5. Configure the Dialer software by running the following commands:

pdsconfigure
start_pds
check_pds
check_mts
check_db

At this point, the Dialer, Mid-Tier, and the Database should all be ready to use.

Appendix H Distribution Area Details

OS Distribution

Machine IP	148.147.165.26
User ID / Password	rohit / rohit
Path	/var/ftp/pub/LinuxOSImage/4.0.0.0.13
Image Name	PC4.0.0.0.13.iso

Linux Dialer Distribution

Machine Name	puscmdist1
Path	\\135.27.161.35\puscm_dist01\builds\v_dialer\Formal\4.0.0.64.39
TAR Name	outputtar\Dialer_4.0.0.0.39.tar
ISO Name	outputiso\Dialer_4.0.0.0.39.iso

Linux Oracle Distribution

Machine Name	puscmdist1
Path	\\135.27.161.35\puscm_dist01\builds\v_dialerdb\Formal\4.0.0.51.39
TAR Name	outputtar\Oracle_4.0.0.0.39.tar
ISO Name	outputiso\Oracle_4.0.0.0.39.iso

To Install Dialer and Oracle package

1) You can directly cut ISO image on CD and use it or
2) You can mount the distribution on your dialer and use the same.
3) Follow this step to mount the distribution server on the dialer system

```
mount 135.27.161.35:/vol/puscm_dist01 /mnt
cd /mnt/builds/v_dialer/Formal/4.0.0.64.39
cp * /tmp
```

Note: - After downloading TAR from distribution area to Dialer user can verify integrity of tar file by executing command “md5sum Dialer_4.0.0.0.39.tar” and comparing checksum with file CHECKSUM.txt in distribution path