Self Service Installation Guide for Windows RoamServer

VERSION 2.3 AUGUST 2014

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065 USA

www.ipass.com
+1 650-232-4100
+1 650-232-0227 fx

TABLE OF CONTENTS

TABLE OF CONTENTS

Introduction

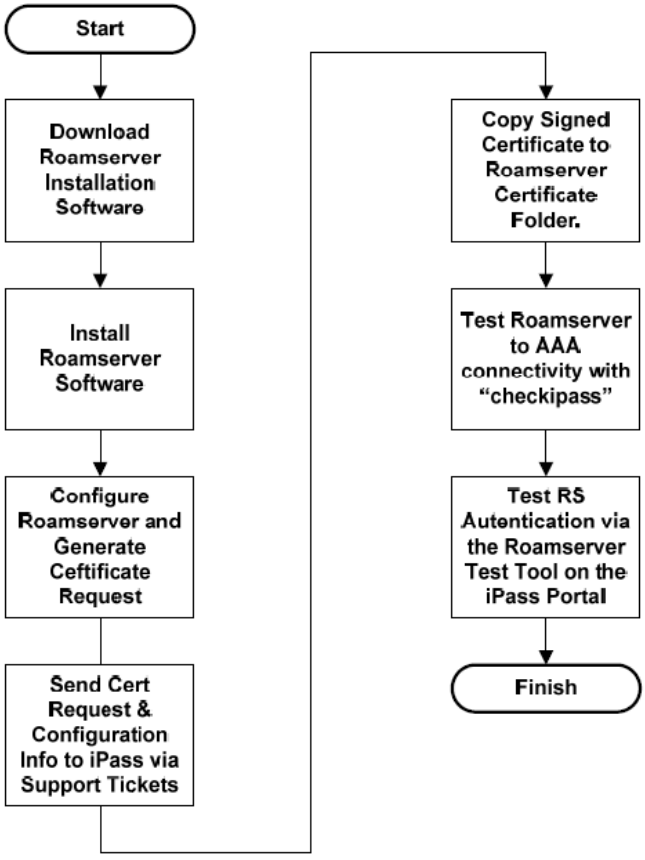
Overview

This document provides a Quick Start install procedure for iPass RoamServer for Windows to enable customers to quickly and independently install and configure a RoamServer in a self-service manner.

For additional detail concerning RoamServer features, settings, and configuration please refer to the RoamServer Administrator's Guide.

The below figure outlines the overall process flow and main steps necessary to successfully install and configure the RoamServer.

Fig 1. *Roamserver Installation Process Flow*



Redundancy

To ensure redundancy, the RoamServer must be installed on at least two separate physical host machines, preferably geographically diverse or at least on different subnets. No iPass service guarantees apply without at least one redundant RoamServer host (also named secondary RoamServer).

Prerequisites

Knowledge and Skills Requirements

The engineer installing RoamServer must have the following skills:

- Familiar with IP networking fundamentals
- Familiar with the relevant AAA protocols and AAA server administration
- Familiar with Windows server operating system
- Good understanding of the specific networking environment where the RoamServer will be installed.
- Good understanding of the specific configuration of the AAA to which the RoamServer will interface.

Preparation

Before installing RoamServer, you will need the following:

- Administrator rights on the RoamServer host server
- FTP client software
- The host should be fully up to date with the latest operating system patches and service pack releases.
- Ensure RoamServer is accessible from the Internet by iPass Transaction Center servers. Refer to the Appendix of this document for the list of Transaction Center server IP addresses.
- Access to the iPass Portal and Support Tickets.

In addition you will need to complete the following configuration checklist to successfully complete the RoamServer installation process.

RoamServer Installation Checklist:

Configuration Setting	Value
Your iPass Customer ID	
RoamServer Public IP address	
RoamServer Private IP address (if NAT'ed)	
TCP Port Number of RoamServer (port 577)*	
Host OS version and Service Pack Level	
Domain Name	
Company Name and Address (for Cert Req)	
Valid email Address (for Cert Req)	
AAA Server IP Address	
AAA Server Port Number	
AAA Shared Secret (for RADIUS, TACACS+)	

*** Port Number must be configured for 577. Port 577 is the standard port number for RoamServer IP communication.**

RoamServer Installation

I. Download the installation file.

1. With an ftp client connect to `ftp.ipass.com`. (Username is **roamserver** and password is **pass2roAm**).
2. On the ftp server, browse to the directory containing the appropriate software for your host platform and download the install file. (file mode for ftp transfer must be set to BIN before download)

II. Run the installation file.

1. Run the installation file, accept the license agreement, and select the location to install the RoamServer software.
2. Review the pre-installation summary information and make sure it is accurate.
3. Click **Install**.
4. When finished, click **DONE**.
5. If this is the first time you've installed RoamServer on this computer, you must install RoamServer as a Windows service by clicking **Add Service**. Then, you will automatically enter configuration mode.
6. If this is a re-install of the RoamServer software, you may skip the **Add Service** step by clicking **Configure**.

III. Configure RoamServer and Generate the Certificate Request.

1. In the **iPass Code Entry** dialog box, enter your customer ID and click **Next**.
2. In the **Local Hostname** dialogue box, enter the host name of the server then click **Next**.
3. In the **IP Address** dialog box, enter the local IP address and then click **Next**.
4. At this point, you can optionally configure your Authentication and Accounting servers. Instructions for configuring your authentication and accounting servers using RADIUS, LDAP or TACACS+ can be found later in the document under Configuring AAA. You may configure authentication servers at any time by running the `ipassconf` utility, found in your `<RS_Home>\bin` folder.
5. Set log files and advanced options. On the **Logging Functionality Configuration** dialog box, select locations for your trace and log files, as well as the type of rotation you wish to use. Click **OK** when done. More information on this can be found in the appendix
6. Generate the certificate request. On the **Certificate Information** dialog box, enter your server IP address, domain name, the name of your company, city, state, and country. In the **Reply To field**, enter a valid e-mail address that will receive the certificate information. Click **Next**.

IV. Send Configuration Information and Certificate Request to iPass.

1. Identify the completed Certificate Request file. You will find this in `<RS_Home>\certs` folder.
2. The file is called `mail_cert_req.data`. Log into the iPass Portal (https://openmobile.ipass.com/moservices) and create and submit a new ticket request from Support Tickets. Request a signed certification and registration of the RoamServer by RoamServer Installation attaching the `mail_cert_req.data` file from step (i) above with the following information RoamServer configuration information:
    - RoamServer Server Name:
    - RoamServer external IP address:
    - RoamServer port address (def = 577):
    - RoamServer OS and Version:
    - Authentication Protocol:

V. Install Signed Certificate to RoamServer.

1. When you receive the signed certificate copy it to `<RS_Home>/certs` folder with filename isp_cert.pem. You can check the validity of the signed certificate by running `verify_certificate.cmd` in the `<RS_Home>/bin` folder.
2. Verify that the box labeled **Restart RoamServer on Update** is checked, and click **Update**. The RoamServer will automatically restart and the changes will take effect.

VI. Test RoamServer to AAA Server Connectivity.

1. The RoamServer to AAA server can be tested from the RoamServer by using the “checkipass” tool . Open a command windows and cd to the “test” folder under the RS install folder and type the following command:
    - `checkipass -u <username>`
    - `Alternatively you can type: checkipass -u <username>@<domain>`
2. Enter the appropriate password for this test user and the result will be either an Accept or a Reject. If you receive the `status=ack`, then the server is functional. If not, you will need to troubleshoot your RoamServer’s AAA configuration setting and connectivity to AAA server. For further information, refer to the RoamServer Administration Guide.

VII. Test Transaction Center to RoamServer Connectivity.

1. Log in to the iPass Portal (https://openmobile.ipass.com/moservices) and select **iPass RoamServer Test Tool** under **Support > Support Tools**.
2. Enter your iPass user name (with domain name), password, class of service and IP address and click **Submit**.
3. This test will display output. Scroll down to the bottom to look for an Accept or Reject response before viewing the rest of the results. An Accept result means that any user authorized to access your system can now roam on the iPass Network.

4. In addition to performing this test with a legitimate user name and password, you should also run the test with an invalid user name and password to ensure that the authorization attempt will be rejected. If this test fails but the previous `checkipass` test works it indicates a problem on the external Internet facing side for the RoamServer. Quite often this indicates that the customer firewall is not configured for the Transaction Center servers. See th Appendix for the list of Transaction Center server IP addresses.

RoamServer AAA Integration

LDAP Authentication

To configure RoamServer for LDAP authentication:

1. Click **Start > iPass RoamServer > Configure RoamServer**. The iPass Configuration dialog is displayed.
2. Under **Authentication Servers**, click **Add**.
3. On the **Authentication Servers** dialog box, under **Protocol**, select **LDAP** from the drop-down list.
4. In the **Auth. Server** field, enter the IP address of your LDAP server. If LDAP is installed on the same server, use the server's lan ip address, not 127.0.01
5. In the **Auth. Server Port** field, enter the port number that the RoamServer will send requests on (usually 389).
6. In **LDAP Config. File**, enter the path to the LDAP configuration file.
7. In **Enable SSL**, check the box if SSL will be enabled over LDAP connections. (See Secure LDAP in RoamServer Adminstator's Guide.)
8. In **Timeout**, enter the duration in milliseconds that RoamServer should wait for a response from the LDAP server. (Valid range is between 2000 and 15000 inclusive with 10000 as the default.)
9. In **Server Priority**, set the priority of this server for failover. (If this is the only server of its kind, enter **1**. See **Setting Secondary Servers for Failover**).
10. Customize the LDAP configuration file to conform with your LDAP server configuration by clicking **Edit**. Sample ipassLDAP.properties file for Active Directory (See the RoamServer Administrator's Guide for detail):

```
LdapBaseDn1 = cn=Users,dc=company_name,dc=com
LdapSearchFilter = sAMAccountName=$USERID
LdapSearchScope = 2
LdapBindDn = cn=ad_lookup_user, cn=Users,dc=company_name,dc=com
LdapBindPassword = ad_lookup_user_password
```

11. Click **OK**.
12. On the **iPass Configuration** dialog box, select **Restart RoamServers on Update**. Then click **Update**. The RoamServer will restart and the changes will take effect.

RADIUS Authentication

To configure RoamServer for RADIUS authentication:

1. Add the RoamServer as a client of your RADIUS server. This is done differently for each flavor of RADIUS, but in most situations, you will need to add the IP address and a shared secret to a clients file or through a GUI. **Note:** A shared secret cannot contain the comma (,) or equals sign (=) characters.
2. Click **Start > iPass RoamServer > Configure RoamServer**. The iPass Configuration dialog is displayed.

3. Under **Authentication Servers**, click **Add**.
4. On the **Authentication Servers** dialog box, under **Protocol**, select **RADIUS** from the drop-down list.
5. In **Auth. Server IP**, enter the IP address of your RADIUS server.
6. In the **Auth. Server Port** field, enter the port number that the RoamServer will send requests on (usually 1812 or 1645). If the Radius server is on the same server, use the lan ip address of the server, not 127.0.0.1
7. In **Shared Secret**, enter the same shared secret that you entered into your RADIUS clients file in **step 1**. (This entry will be used to create a local clients file in `<RS_Home>\clients`.)
8. In **Attempts**, enter the number of attempts the RoamServer should make to connect with the RADIUS server. (Valid range is between 1 and 3 inclusive, with 3 as the default.)
9. In **Timeout**, enter the duration in milliseconds that RoamServer should wait for a response from the RADIUS server. (Valid range is between 2000 and 15000 inclusive, with 5000 as the default.)
10. If the RoamServer should pass on prefix information to the RADIUS server, select the **Include Prefix** checkbox.
11. If the RoamServer should pass on domain information to the RADIUS server, select the **Include Domain** checkbox.
12. In **Server Priority**, set the priority of this server for failover. (If this is the only server of its kind, enter 1)
13. Click **OK**.
14. Optionally, to add your RADIUS server as an accounting server, under Accounting Servers, click **Add**. On the Accounting Servers dialog box, enter all the information you entered for the RADIUS Authentication Server. Click **OK**.
15. On the **iPass Configuration** dialog box, select **Restart RoamServers on Update**. Then click **Update**.
16. The RoamServer will restart and the changes will take effect

TACACS+ Authentication

To configure the RoamServer for TACACS+ authentication:

1. Retrieve and copy the TACACS+ key from the configuration file of your TACACS+ Authentication server.
2. Click **Start > iPass RoamServer > Configure RoamServer**. The **iPass Configuration** dialog box is displayed.
3. Under **Authentication Servers**, click **Add**.
4. On the **Authentication Servers** dialog box, under **Protocol**, select **TACACS+** from the drop-down list.
5. In the **Auth. Server** field, enter the IP address of your TACACS+ server. If the TACACS+ is installed on the same machine as the RoamServer, do not use the loopback address (127.0.0.1); instead, provide the machine's routable IP just as you would if they were installed in different locations.
6. In **Auth. Server Port**, enter the port number that the RoamServer will send requests on (usually 49).
7. In **Shared Secret**, enter the key that you copied from your TACACS+ configuration file in **step 1**.

8. In **Timeout**, enter the duration in milliseconds that RoamServer should wait for a response from the TACACS+ server. (Valid range is between 2000 and 15000 inclusive with 5000 as the default.)
9. Click **OK** to return to the **iPass Configuration** dialog box.
10. Optionally, to add your TACACS+ server as an accounting server, under **Accounting Servers**, click **Add**. In the **Accounting Servers** dialog box, enter all the information you entered for the TACACS+ Authentication Server. Click **OK**.
11. On the **iPass Configuration** dialog box, select **Restart RoamServers on Update**. Then click **Update**. The RoamServer will restart and the changes will take effect. (If this box is not checked, you must manually restart the RoamServer before any changes will take effect.)

Appendix

iPass Transaction Server Communication

In order for your primary and secondary RoamServers to communicate with our transaction servers, you will need to open your firewall for TCP communications on port 577. Please refer to http://help.ipass.com/doku.php?id=required_configurations_for_open_mobile_access for a list of Transaction Center IP addresses and further details.

> *iPass recommends using the **Simple Option** (described in the link above) to configure your firewalls, in order to reduce future changes to your firewall configurations.*