



Adroit Secure Mobile Gateway

Quick Start Guide

COPYRIGHT

Copyright © 2020 Advanced Worx 112 (Pty) Ltd. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Advanced Worx 112 (Pty) Ltd.

Advanced Worx 112 (Pty) Ltd
20 Waterford Office Park
189 Witkoppen Road (c/o Waterford Drive)
Fourways
South Africa

www.adroittech.co.za

Version	Date	Author	Comment	Approval
1.0	21.11.2019	Unknown	Original	D. Wibberley
2.0	22.05.2020	J. Duncan	Update Cover and formatting	F. Kok
3.0	10.07.2020	J. Duncan	Updated and new sections added	F. Kok
4.0	28.08.2020	J. Duncan	Finalise	
5.0	13.11.2020	J. Duncan	Mods to Troubleshooting and Firewall Rules	

Contents

1.	Requirements:	3
2.	Installation	3
2.1.	Step 1: Download the Launcher	3
2.2.	Step 2: Run the Launcher	3
2.3.	Step 3: Register and Connect	3
2.4.	Step 4: Retrieve the Connection Information / Launch a Browser	4
2.5.	Step 5: Run the Secure Gateway Operator	4
2.6.	Usage within the Browser:	5
3.	Frequently Asked Questions:	5
4.	Troubleshooting	8
5.	Addendum – Multiple Sessions	9
6.	Addendum – Security	10
6.1.	SSH 2.0	10
6.2.	HTTPS	10
6.3.	Cloud based process	10
6.4.	Firewall Rules	10
6.5.	To secure a project even further:	10

1. Requirements:

Internet Connection

PC with SmartUI installed <- This could simply be an Operator PC which is configured to connect to another Server within the network OR the actual SmartUI Server PC.



NO open firewall ports, external -> internal internet access, IIS installation or other software is required

2. Installation

2.1. Step 1: Download the Launcher

Download the **Launcher** application here:

https://adroittechnologiesautomation.com/securedownload/smg_launch.exe

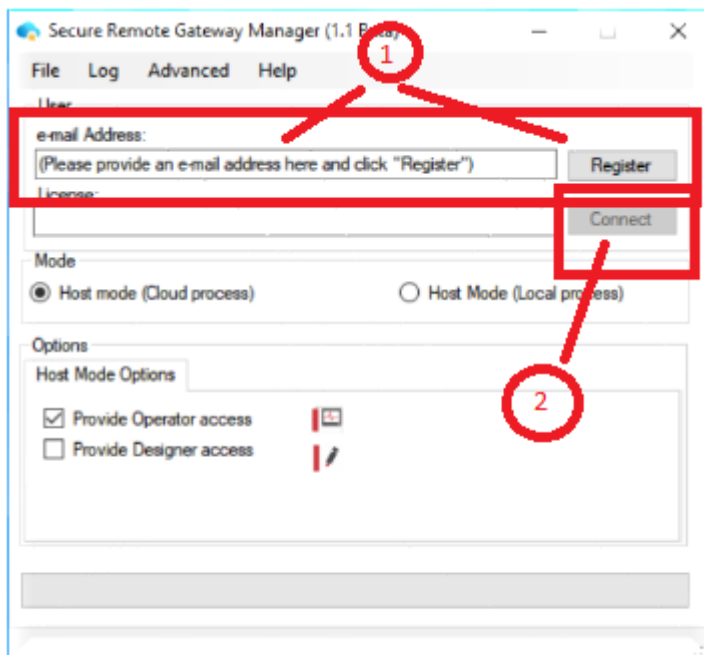
2.2. Step 2: Run the Launcher

Run SMG_LAUNCH.EXE

This will connect to the distribution service and always ensure that the latest version of the Secure Gateway Manager is installed.

2.3. Step 3: Register and Connect

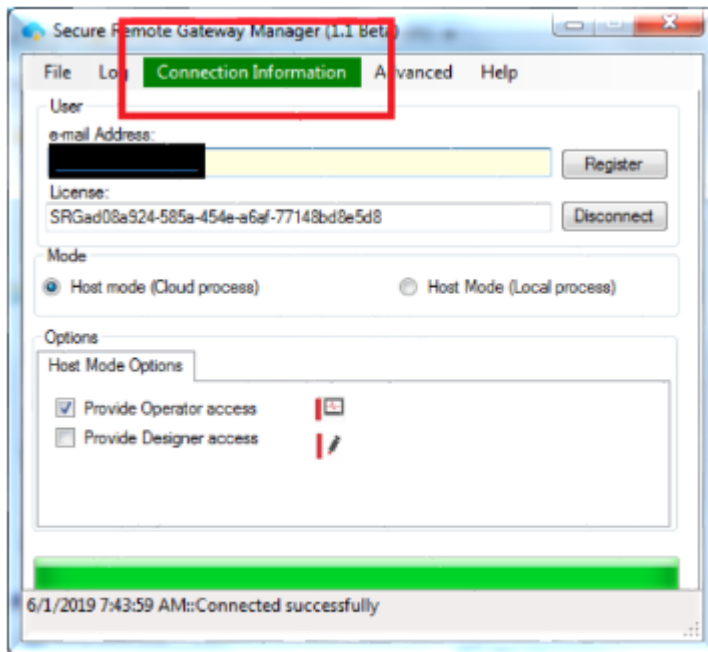
Provide an e-mail address and click **Register**.



Once registration is complete, a license code will be displayed in the "License" box. If this is successful, click **Connect**.

2.4. Step 4: Retrieve the Connection Information / Launch a Browser

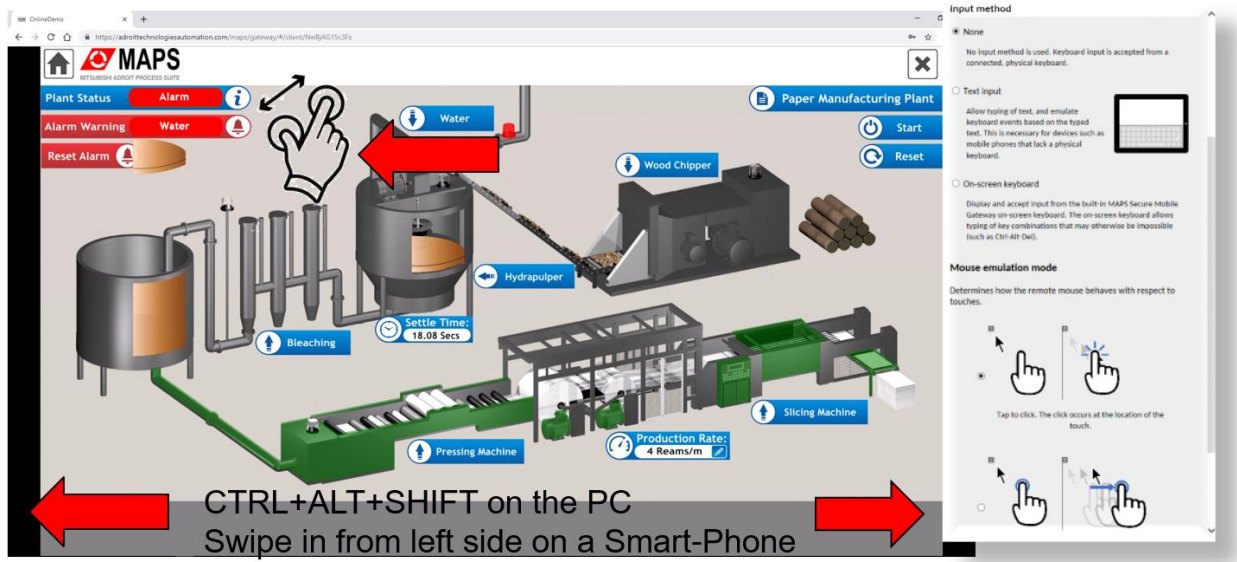
If the connection is successful, the "Connection Information" will appear green. Click on the "Connection Information" for the Connection URL.



By clicking on the URL, the default browser will open and automatically launch the Operator connection from within the Browser. Right-click on the URL to Copy the connection information to the Clipboard (This URL can be pasted in a browser directly).

2.5. Step 5: Run the Secure Gateway Operator

The Operator should launch within the browser and automatically be configured to connect to the Server. If a username and password is required, provide the necessary credentials and Login to the Operator window within the Browser. These are the same credentials as if connecting with the local Operator. If the Operator has been configured to automatically login, the Operator within the browser will also be configured to automatically login.



2.6. Usage within the Browser:

On a PC, pressing CTRL+SHIFT+ALT will bring up the connection menu.

On a Touch Device / Mobile, Swipe in from the left side to bring up the connection menu.

3. Frequently Asked Questions:

Q: Which versions of Adroit are supported on the Secure Gateway?

A: 8.4.2.x LTS, 10.0.4.x and 10.0.5.x

Q: How many simultaneous Cloud connections are supported?

A: By default 2 simultaneous connections are supported for each registration. If more connections are required, please contact your Sales representative.

NOTE: A maximum of 10 simultaneous connections are supported.

Q: Which Browsers are supported?

A: Internet Explorer, Edge, Firefox, Chrome, Safari, Opera

Q: What licensing is required?

A: The Cloud Hosted version requires Performance Anywhere licenses at the Server and a monthly hosting fee. The first 14 days is provided as a free trial.

Q: What happens when I click on "Connect" in the Secure Gateway Manager?

A:

- The Secure Gateway Client Manager determines whether a local Adroit Operator is installed.
- If found, it contacts the Secure Cloud Delegation Server and configures an Adroit Cloud Operator with the same encrypted credentials and connection information as the local Adroit Operator.

Q: How does the Operator Scaling work in the Web Browser?

A: By default, the Operator scaling is configured for 1920x1080 (Full HD). The Cloud Operator will always be scaled in order to maintain these dimensions without scroll bars. *Scaling can be enabled/disabled in the Advanced Menu -> Options -> Enable web client scaling.* If scaling is turned off, scroll bars may appear at the side of the browser depending on the client resolution. For example: If a web browser is

open in full screen mode on a display that is configured for 1920x1080 resolution, no scrollbars should be visible.

Q: Should I redesign my project for mobile devices?

A: No, this is not required. However, this can sometimes be preferred if the current level of detail on the graphic forms are too much for smaller form factor devices. Also if the navigation is difficult to use on touch based devices. In these cases, it can be useful to design a set of graphic forms with large navigation options (such as large buttons) and a limited amount of detail in order to translate into a better usability experience for users on smaller form factor and touch based devices. The selection between the two types of projects can be configured by specifying a landing page where the user can choose between either of the two types of projects.

Q: What are the network requirements for the Secure Gateway?

A: An Internet Connection of at least 2Mbps is recommended.

Q: Will the Secure Gateway connection resume if the PC is restarted?

A: Yes. The "Secure Gateway" Windows Service is automatically started when the PC reboots. A Secure Gateway session can also be started / stopped via the Windows Service manager.

Q: Will the Secure Gateway connection re-connect in the event of a network failure?

A: Yes, the Secure Gateway connection will attempt to reconnect after a successful network connection has been established again.

Q: Can I use the same e-mail address for multiple connections?

A: No, this is not currently supported.

Q: What if I want to use the same e-mail address for another connection?

A: First de-register the current connection through the *Advanced -> Registration* menu. Thereafter the e-mail address can be used for another connection.

Q: What if my project requires additional DLLs and third party controls?

A: In this case the Secure Gateway Manager can be configured for **Own Process** mode. In this mode the Operator runs in a virtual session **on the actual host that initiated the Secure Gateway Client Manager and not on a Cloud Host**. This mode requires Windows 2008, 2012 or 2016 Server editions. To configure **Own Process** mode, please refer to the **Secure Gateway Enterprise Mode** documentation.

Q: Which secure technologies are implemented?

A:

- The Secure Gateway Client Manager requires no open firewall ports, a secure channel is initiated from client side – This prevents any direct exposure to sniffing, DDOS attacks and hack attempts.
- SSH 2.0 implemented (RFC 4419/4432/6594 compliant) –Used by millions of organisations worldwide to provide secure communication
- HTTPS and TLS to ensure secure web connectivity (TLS 1.2, AES128 with SHA256)
- Provides optional 2FA – Two-Factor-Authentication can be used to provide additional security.
- Application specific – Access is only provided to the Operator and not to any underlying Operating System functions.

- If the Operator is compromised or exits, the end-result is a virtual session hosted on a Cloud Server and not on the actual host (Applies only to **Cloud Process** hosting)

Q: Where is the Secure Gateway Manager application installed?

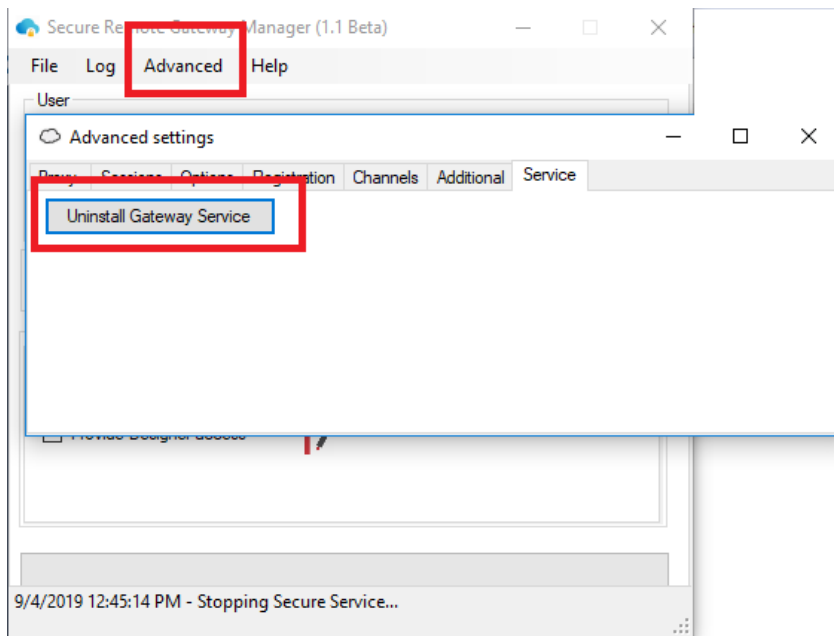
A: It is installed in the C:\SECUREGATEWAY folder. If required, a shortcut can be created to the VIP LAUNCHER.EXE <- This is the executable that is responsible for ensuring that all files are up to date and will then continue to launch the Secure Gateway Manager.

Q: How do I remove the Secure Gateway Manager?

A:

Step 1

Uninstall the Secure Gateway Service:

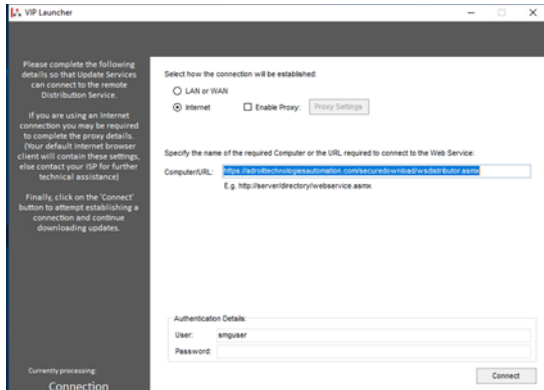


Step 2:

Delete the C:\SECUREGATEWAY folder. This removes the application completely.

4. Troubleshooting

Q: When I run the launcher, nothing happens, or it freezes at some point during or after the files have been downloaded.

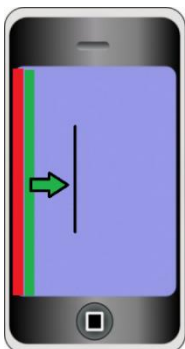


A: Certain Anti-Virus products as well as certain Windows Updates may cause this behaviour. Normally this behaviour occurs after the necessary files have already been downloaded. Then the launcher can be closed, and the *SMG_MANAGER.EXE* application can be run from within the C:\SECUREGATEWAY folder to configure the Secure Gateway connection.

OR:

1. A full version of the Secure Gateway Manager can also be downloaded here:
https://adroittechnologiesautomation.com/securedownload/SecureGateway_latest.zip
2. All the files inside this archive **must be placed in the C:\SECUREGATEWAY** folder.
3. The *SMG_MANAGER.EXE* application can be run from within this folder to configure the Secure Gateway connection.

Q: I am having trouble invoking the menu on a touch device



A: On certain touch devices (such as iPhones) as well as certain browsers (such as Safari), the swipe action from left to right from the edge of the device triggers a "back" action instead of invoking the menu.

On these devices, to invoke the menu, take care not to swipe to close to the edge of the device. In the picture below, be careful to swipe from left to right in the green area to the centre of the screen, and not the red area.

To remove the menu swipe from the right to the left again.

There is an on-screen keyboard which can be enabled for touch devices with and without built-in keyboards on the menu. You can also make use of the built-in touch keyboard available on many Operator dialogs:



5. Addendum – Multiple Sessions

Normally a web browser (Firefox, Chrome, IE etc.) will store the Secure Gateway session information as a session cookie for ALL OPEN TABS. In other words, opening a new tab in order to open another Secure Gateway session will not work. The browser will simply navigate to the existing session.

In order to create multiple independent sessions:

- In **Internet Explorer**:
 - Click File->New Session in order to create separate independent Secure Gateway sessions
- In **Firefox**
 - Install the "Multi Account Containers" extension
- In **Chrome**
 - Install the "SessionBox" extension

6. Addendum – Security

The Secure Gateway makes use of several mechanisms to ensure confidentiality and integrity:

6.1. SSH 2.0

- Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.
- This protocol is used widely by commercial and governmental organisations to establish a cryptographic network channel and ensure the confidentiality of the underlying communication.
- This protocol implements the RFC 4250 through 4345 Internet standards.
- The encryption protocol is used to establish an encrypted channel between the Secure Mobile Gateway Client Manager and a Cloud Delegation Server.
- The protocol implementation that forms part of the Secure Mobile Gateway will only connect to a trusted set of Cloud Delegation Servers as identified by their public/private key pairs.

6.2. HTTPS

- Web based access is provided via *HTTPS only* and *all traffic* is encrypted between the Browser and the Cloud Delegation Server.

6.3. Cloud based process

- If the “Cloud process” host mode is used, the actual Operator process does not run on the Host infrastructure, but rather in a protected sandbox environment on one of the trusted Cloud Delegation Servers.

6.4. Firewall Rules

- If required, specific firewall rules can be configured. All the rules require an OUTBOUND direction only, NO INBOUND rules are required.
 - i. RULE 1; Outbound; ALLOW HTTP/HTTPS **secure.pharaday.org (port 80 & 443)**
 - ii. RULE 2; Outbound; ALLOW HTTP/HTTPS **41.185.80.219 (port 80 & 443)**
 - iii. RULE 3; Outbound; ALLOW HTTP/HTTPS **41.185.80.222 (port 80 & 443)**
 - iv. RULE 4; Outbound; ALLOW HTTP/HTTPS/TCP **adroittechnologiesautomation.com (port 80 & 443)**
 - v. RULE 5; Outbound; ALLOW HTTP/HTTPS/TCP **mapscloudsolutions.com (port 80 & 443)**

6.5. To secure a project even further:

- *Provide two-factor authentication* - If an automatic login is performed through the Secure Mobile Gateway, ensure that the default credentials in the Operator is of a *low level user (i.e. no write access)*.
- Any elevated task (for example, changing a setpoint), would require an additional login process from within the Operator:
 - a. The Secure Mobile Gateway Client Manager retrieves the user details from the current active configuration.
 - b. In order to change the credentials that the Client Manager uses, simply run the Operator, change the credentials, and select “automatically login with these settings next time”.
 - c. The next time the Secure Mobile Gateway Client Manager connects, it will use the newly configured Operator credentials.

- d. Provide an optional *login* graphic form within the project, if a user could login and establish a higher level of access for a specific task OR ensure that Data Element security is enabled for configured write access.