

****

SapphireIMS Windows Agent Installation Scripts

**Copyright**

Copyright © 2018 [Tecknodreams Software Consulting Pvt. Ltd.](http://www.tecknodreams.com) All Rights Reserved.

**Restricted Rights Legend**

This documentation is subject to and made available only pursuant to the terms of the Tecknodreams License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the documentation except as specifically allowed in the agreement. This document may not, in whole or in part, be copied photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from Tecknodreams.

Information in this document is subject to change without notice and does not represent a commitment on the part of Tecknodreams.

# Introduction

SapphireIMS supports windows agent deployment from SapphireIMS server when there is a direct connectivity available between end user machine and server, along with certain service pre-requisites. But the typical scenario is, end user machines will be outside the network and will not have the direct connectivity from server where SapphireIMS is hosted. In this case, customer will have two options to deploy agents in end user machine.

1. Active Directory script push for machines which are managed by AD.
2. Installation package which will be run by end user manually to install agent.

This document explains various scenarios where AD startup script to be used for agent installation and enabling end user to install agent without knowing the admin credentials and bypassing UAC prompt if it is enabled.

# Active Directory Push

Large scale deployment of SapphireIMS agent can be done with the help of Active Directory. For this to work, end user machines should be under a domain in Active Directory.

## Why to use start-up script? Why not logon script?

SapphireIMS agent installation needs privilege to interact with registry, OS drive and windows services. Typical end user will not have access to these areas. Hence, we require scripts to be pushed via AD start-up script.

## Install/Upgrade Scenario

Scripts are available in two folders for install or upgrade scenario. Scripts in one can be used when the shared folder is accessible without any credential (***active-directory-scripts*/*sapphireimsagent-install-upgrade-reinstall-open-share***). Scripts in another folder can be used when the shared folder requires credential for access (***active-directory-scripts/sapphireimsagent-install-upgrade-reinstall-share-credential***).

|  |  |  |  |
| --- | --- | --- | --- |
| If agent is not available | If old version agent is available | If latest/baseline agent is available | Script to be used |
| Install | Upgrade | Abort (No action) | sapphireimsagent-install-upgrade.bat |
| Abort (No action) | Upgrade | Abort (No action) | sapphireimsagent-only-upgrade-old-agent.bat |
| Install | Abort (No action) | Abort (No action) | sapphireimsagent-only-install-if-not-available.bat |
| Install | uninstall, reinstall | Abort (No action) | sapphireimsagent-uninstall-reinstall-old.bat |
| Abort (No action) | compare SapphireIMS server configuration in end user machine, if not matching uninstall and install | compare SapphireIMS server configuration in end user machine, if not matching uninstall and install | sapphireimsagent-uninstall-reinstall-wrong-serverconf1.bat |
| Install | Compare SapphireIMS server configuration in end user machine, if not matching uninstall and install | compare SapphireIMS server configuration in end user machine, if not matching uninstall and install | sapphireimsagent-uninstall-reinstall-wrong-serverconf2.bat |

## Uninstall Scenario

Scripts available inside ***active-directory-scripts\sapphireimsagent-uninstall*** can be used for performing agent uninstallation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| If agent is not available | If old version agent is available | If latest/baseline agent is available | Script to be used | Comments |
| Abort (No action) | Uninstall | Uninstall | sapphireimsagent-uninstall-all.bat |  |
| Abort (No action) | Uninstall | Abort (No action) | sapphireimsagent-uninstall-old.bat |  |
| Abort (No action) | Uninstall | Uninstall | sapphireimsagent-uninstall-wrong-serverconf-open-share.bat | This operation requires additional executable to be available in open shared folder |
| Abort (No action) | Uninstall | Uninstall | sapphireimsagent-uninstall-wrong-serverconf-remote-share-credential.bat | This operation requires additional executable to be available in shared folder which can be accessed with specific credential |
| Abort (No action) | Abort (No action) | Uninstall (Specified Version) | sapphireimsagent-uninstall-specific-version.bat |  |

## Active Directory Start-up Script Creation Steps

Before proceeding with AD start-up scripts steps, make sure to create agent installer package with *Force Agent Installation (Upgrade)* and *Silent Installation* options enabled in SapphireIMS web portal. This package along with additional executable (in specific scenario) needs to be placed in a common folder (open folder/share with credential) to perform installation via AD start-up.

1. Create a network share (e.g. \\MyServer\ShareName).
2. Place the appropriate **agent package**, **batch file,** optionally **read-server-conf-value.exe (needed in specific scenario)** and copy in the network share Created in step 1
3. Edit the batch file and fill the required information such as share folder, baseline version, share credential.
4. In AD machine, Start -> Run -> gpmc.msc
5. Right-click the domain and select "Create and Link a GPO here"
6. Specify a name for the GPO
7. Select the GPO from the tree.
8. Select the Scope tab.
9. Click the Add button in the Security Filtering to specify the computers
10. Click the Object Types button in the "Select User, Computer, or Group" dialog and select Computers object type and click OK.
11. Specify the computer names and click Check Names to add the required computers.
12. Click OK to close the "Select User, Computer, or Group dialog"
13. Right-click the GPO and select Edit. It will open a new group policy window.
14. Expand Computer Configuration > Policies > Windows Settings > Scripts
15. Right-click Startup and select properties.
16. Click Show Files and drag and drop the **agent installation batch file** to this location and close.
17. In the Startup Properties dialog, click Add.
18. Specify the script name as mentioned below: **\\MyServer\ShareName\SapphireIMS-agent installation bat** file script. This refers to the shared location where you have stored the SapphireIMS agent Installer.
19. Click OK to close the Add a Script dialog.
20. Click OK to close the Startup Properties dialog.
21. Close the Group Policy Object Editor
22. Close the Group Policy Management dialog.

When the end user machine is rebooted for the next time, start-up script will be triggered.

# Note on AD Push

Before rolling out script in all systems, try it in a test machine and verify whether script works as expected. Then roll out in other systems. If agent is available in end user machine, then upgrade/reinstall/uninstall script will be triggered in the machine after 15 minutes of sleep. This is to make sure that all services are started, and system is usable.

# Manual Installation Package

This option can be used when end users are not managed by active directory (work group machines).

## Scenario 1 – All end users having admin privilege

In this scenario, just create agent installer package from SapphireIMS web portal and give it to end users and request them to install.

## Scenario 2 – End users not having admin privilege

In this scenario the user who launches the agent package will not have privilege to registry, service control and OS drive. In this case, the package should be triggered in another user account which has Admin privilege. Customer environment will have one/more common user account in all systems which will have admin credential. Also, the installer should proceed bypassing UAC prompts. In this case, use below given steps.

## Steps to Create Multi-Credential Agent Package

1. Placegiven **multi-credential-agent-package** folderin SapphireIMS installed machine (Application Server)**.**
2. Fill agent communication information in **ServerConf.ini** file using below given steps:
	1. Provide the SapphireIMS Server's IP/Hostname/FQDN and Port under [AGENTCONF] section.
	2. If agent is going to communicate via proxy, then provide proxy information under [AGENTPROXY] section.
	3. Provide the base64 encrypted OU Path in the logicalgroup of [AGENTPPOLICY] section
	4. If SSL(HTTPS) is enabled, then provide 1 in the SSL of [AGENTPPOLICY] section.
3. Fill admin credential information in **ExtendedServerConf.ini** file using below given steps:
	1. Specify number of credentials under [GENERAL\_INFO] section.
	2. Provide the AgentInstallationCondition in the [GENERAL\_INFO] section as per the following value.

 1 – Force Agent Upgrade

 2 - Uninstall and Install

 3 - Already Installed, exit the installation

* 1. For each credential create a [LOGONPOLICY] section ([LOGONPOLICY-1], [LOGONPOLICY-2], …., [LOGONPOLICY-10], if number of credential profile is 10.)
	2. Under each LOGONPOLICY section, specify the encrypted username and password. Encryption can be done using Aracrypt.exe by following [Steps for Encrypting Credential](#_Steps_for_Encrypting) available in next section of this document.
	3. In case machine is in domain, please enter the domain name under [LOGONPOLICY-N] section as a plain text.
1. Download **PsExec.exe** from Microsoft web site and place it in *multi-credential-agent-package* folder. This tool will be used to bypass the UAC prompt in end user machine. (<https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>)
2. Open command prompt in **Run as Administrator** option and change directory to *multi-credential-agent-package* folder and launch **multi-credential-agent-package.bat** file.
3. One new folder named **Output** will be generated and package will be created inside that folder. In case of any failure, package will not be created.
4. If customer needs multiple package, then rename/take backup of created package and repeat given steps with necessary change.

## Steps for Encrypting Credential

1. Open command prompt in Run as Administrator option and change directory to multi-credential-agent-package folder.
2. In above opened command prompt, execute 'ARACrypt.exe' by using username and password as command line separately to encrypt username and password.

ARACrypt.exe Username

ARACrypt.exe Password

1. Encrypted password will be appearing in the command prompt. Copy it and use it in step number 3.d of [Steps to Create Multi-Credential Agent Package](#_Steps_to_Create).
2. No need to encrypt domain name (if available).