Active Directory - Group Policy Setup

UserAgentx86.msi

UserAgentx64.msi

UserAgentIDServer32.mst

UserAgentIDServer64.mst

Active Directory

Ensure you've followed the PC User Agent Install article before proceeding.

You can use Group Policy Objects (**GPOs**) to assign and install software to computers in a domain, and it can be useful to to deploy this software based on group membership or OU's. This section describes how to have your User Agent software deployed across multiple OU's.

(For more information on the basics of assigning software to specific groups by using a GPO, refer to Microsoft Knowledge Base article**302430**)

Instructions:

1. Create a network share folder to hold the deployment MSI and MST files. Set the security on this folder to allow AD users and computers ("Everyone" group) to have ***'read and execute'*** privileges. Build, copy or move the required MSI and MST files into this location.
2. Log onto your network's Active Directory server as a domain administrator, and then launch the **Active Directory Users and Computers** snap-in.

	Though you can apply group policies to an entire domains and multiple OU's, it is highly recommended, that when planning the installation of the User Agent software that you apply the group policy to ONLY the lowest common workstation OU, not at a Domain level.

3. From the Active Directory **'Users and Computers'** snap-in, locate the OU that you want to have the GPO linked to. Right-click that OU, click **Properties**, and then click on the **Group Policy** tab.
4. Click the **<New>** button to create a new GPO for installing the User Agent MSI package. Enter a descriptive name for this new Group Policy, such as ***"Deployment of User Agent"*** and click **<Enter>.**
5. Select the new GPO name that you just created and click **<Edit>.** This starts the Group Policy Editor.
6. Expand the **Software** node of the **Computer Configuration** set, then right-click **'Software Installation'**. Select the ***'New -> Package'*** option to open the browse dialog for selecting the User Agent MSI.
7. Navigate to the network location that contains the User Agent installer files. Click on the ***'UserAgent(x86 or x64).msi'*** file, and then click **<Open>.**

	If the installer files reside on a local hard drive, do not use a local path provided by the browser - instead, use a UNC path (such as \\servername\sharename\path\filename.msi) for the local PC to universally indicate the location of the installation files. If you allow the Group Policy to be created with the file location specified as 'local', client computers that attempt to install the package will look in their LOCAL hard drive folders, and will not find the installation files and the installation will fail.

8. The **Deploy Software** options dialog is displayed. Click and select the ***Advanced*** option, which will allow you to specify modifications (MST files) for the software installation then click **<Enter>** to move to the installation properties dialog.
9. Click on the **Deployment** tab and make sure that the ***'Uninstall this application when it falls out of the scope of management'*** option is NOT ENABLED.
10. Click on the **Modifications** tab, then click the **<Add>** button to browse for the associated MST file. This file should have been labeled ***"UserAgent ServerID.mst"*** and should be in the common file share where the ***"UserAgent(x86 or x64).msi"***file is located. Select this file and click the **<Open>** button to add it to the modifications list.
11. Click the **<OK>** button when all properties are complete. This will save and assign the GPO to the selected OU. Click on the**Software Installation** node to refresh and display the completed/assigned policy.

	Changes to a GPO are not immediately imposed upon the target computers, but are applied in accordance with the currently valid group-policy refresh interval. You can use the Secedit.exe command-line tool to impose GPO settings upon a target workstation immediately. For information on using the Secedit.exe program refer to Microsoft KB article**227032**.

You should verify your TTC Security Server settings for name resolution services. Refer to KB article **Required Settings for Full Name Resolution - Q11089** for details on the necessary server settings, registry settings and services credentials.