

## ContentWatch Auto Deployment Tool

ContentWatch™ gives administrators the ability to easily distribute ContentProtect™ (or say our products) over any network. With our Unattended Installer you can install ContentProtect™ automatically via any auto-deployment utility including: autoexec.bat, network startup scripts, or any kind of scripting/deployment tool. You can also place ContentProtect's executable file and the unattend.txt files on shared network drive and have users install from there.

The install requirements are:

1. The unattend.txt and the installation exe both be in the same directory. (If a script copies the files to the hard drive before executing them, both the unattend.txt and install.exe need to be in the same directory)
2. The process executing the script will need to have read and execute permission to the directory it where the files are housed.
3. The process or person installing on the computer will need to had local administrative rights to the computer.

### **Setup**

Unzip the downloaded files in an easily accessible folder

Edit "unattend.txt" (see UnattendReadme.doc for help)

Make these files accessible to all computer or users accounts you wish to install to. (These two files MUST exist together in the same folder)

Deploy ContentProtect install executable as desired (i.e. Active Directory)

Create Additional Users via ContentProtect LDAP Import Tool (see [Ldap Import Tool.doc](#))

### **Making the file accessible to users or computers**

After you have completed [editing the unattend.txt](#) file you will need to put both the executable and the unattend.txt file in a directory that is Network Accessible.

Example: On the server create a folder called CWNetInstall, copy both the executable file and the unattend.txt file to this directory.

Right click on the folder and select properties, then select the Sharing tab. Under the Sharing tab select "share this folder" then select the permissions button. Make sure that the users or computers that you will deploy the software to have at least read and change permission to the directory. Then click ok.

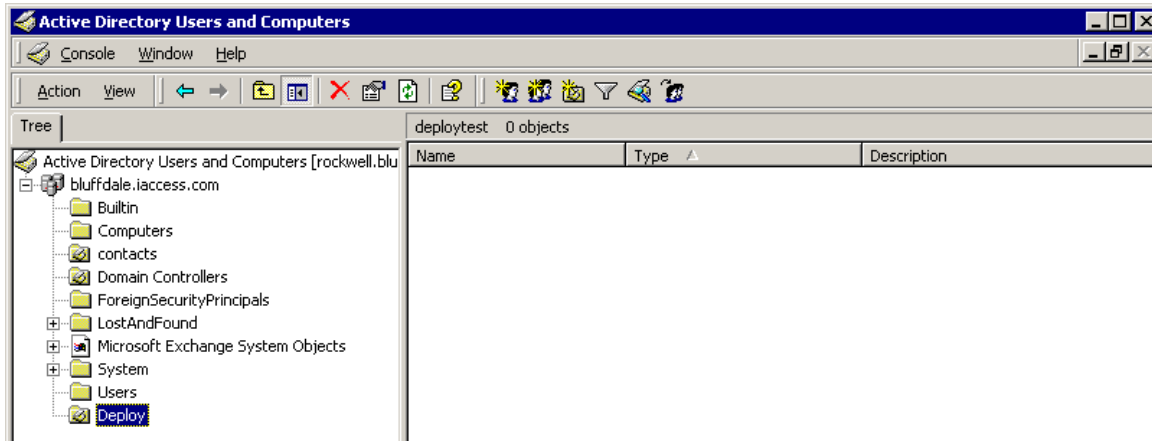
### **Deploying the software to computers via active directory**

To add a the installation script to a new or existing Group Policy Object (GPO), open the Active Directory Users and Computers console (Microsoft Management Console, MMC), Right-click the organizational unit O.U. in which you want to create a new policy or access an existing policy.

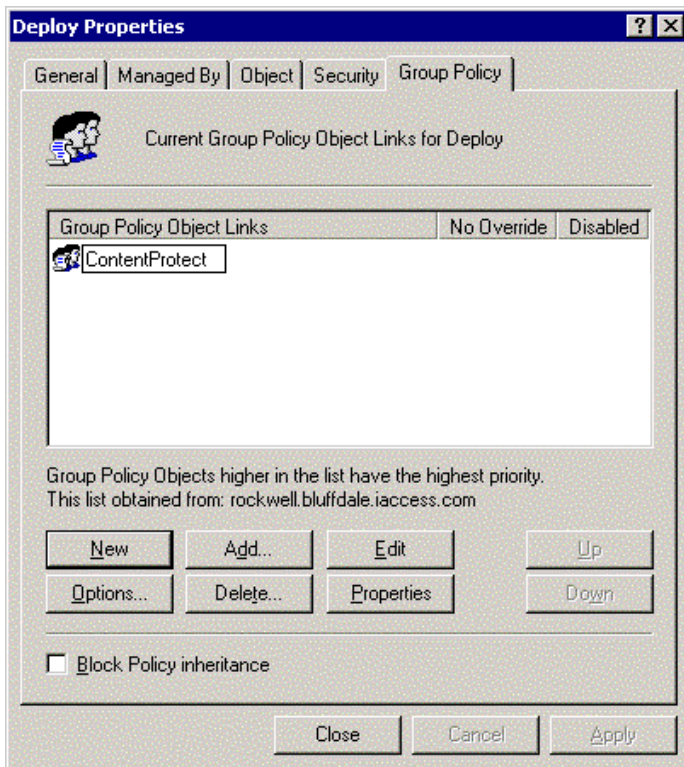
The preferred method for deployment is to an Organizational Group (OG) that contains computer accounts (Not User Accounts). This method will on Organizational Units (O.U.) that contain users accounts also, but the users must have previously have been granted administrative rights to their personal computer for this to work correctly.

In a default Active Directory setup all client computer accounts are stored in the Computers O.U. We suggest you use this method for production roll out but first create a testing O.U. for initial testing.

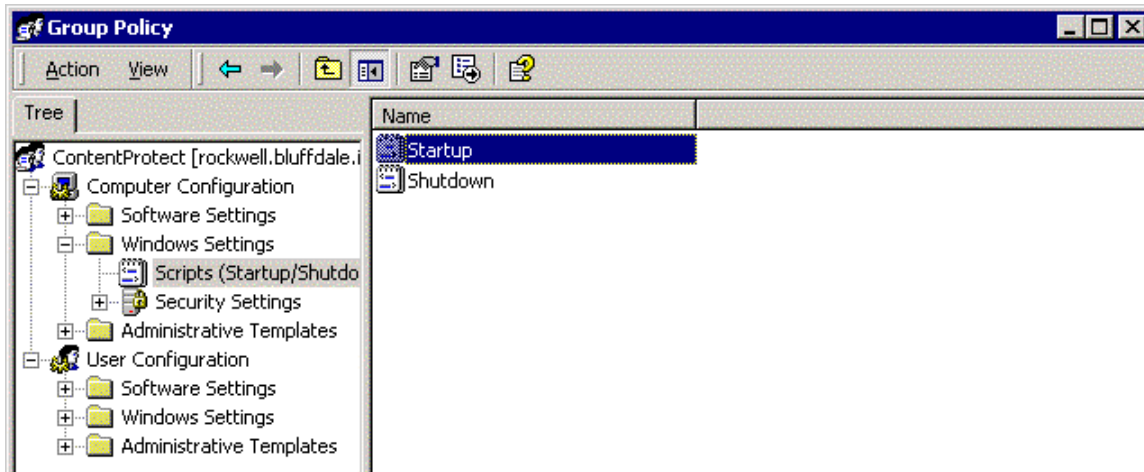
Right click on the domain name at the top of the Active Directory tree and say new, then choose Organizational Unit, and choose a name for the new O.U. For testing purposes you may wish to call this "Deploy".



After creating the new Organizational Unit or selecting an existing one, right click on the O.U. and select properties from the context menu, then select the Group Policy tab. Click New to add a new policy. Name the new policy (an example name could be ContentProtect install), then click Edit.

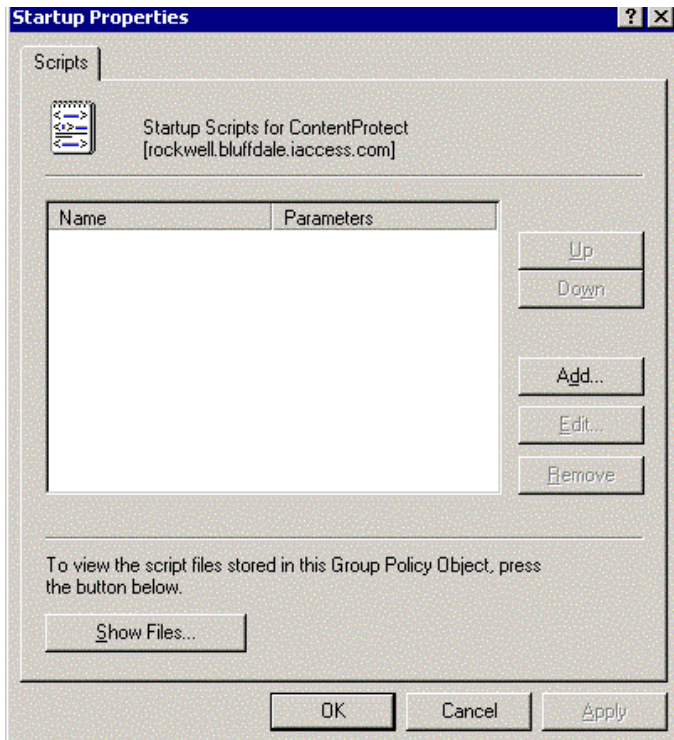


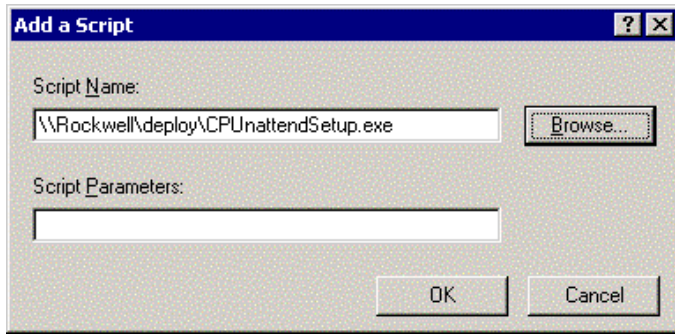
Under the new policy, drill down to Computer Configuration > Windows Settings > Scripts (Startup/Shutdown). Double-click Startup in the right panel to open the Startup Properties page.



Click the add button on the right hand side, and dialog box will appear. Click the browse button and browse through the network to the share previously created, and select the executable file in that directory, click OK.

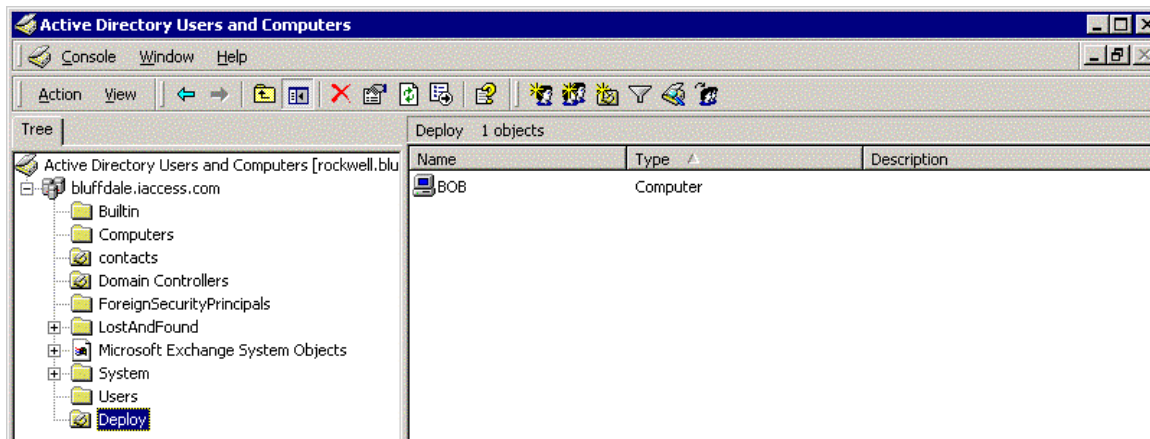
(NOTE) DO NOT Browse the to file locally, you must have a full network path to the executable. The path should look something like \\yourservername\CWNetInstall\CWNetSetup.exe (notice the server name and full UNC path.)





Click ok to close the Startup Properties box and close the Group Policy window and exit all cascaded windows. If you have chosen to make a test O.U. for deployment, you will need to move the Computer Account from the existing Computers O.U. into the new "Deploy" OU. You can move a single Computer Account by right clicking the computer account in the Active Directory admin screen (MMC) and say move, then choose to move it to the "Deploy" O.U.

After verifying the deployment works correctly for your needs, we suggest you then move the computer account back to the default Computers O.U. and deploy the group policy to the original OU.



After verifying that the Computer Account is in the correct OU the next time the computer reboots the software will be installed automatically without any user interaction.

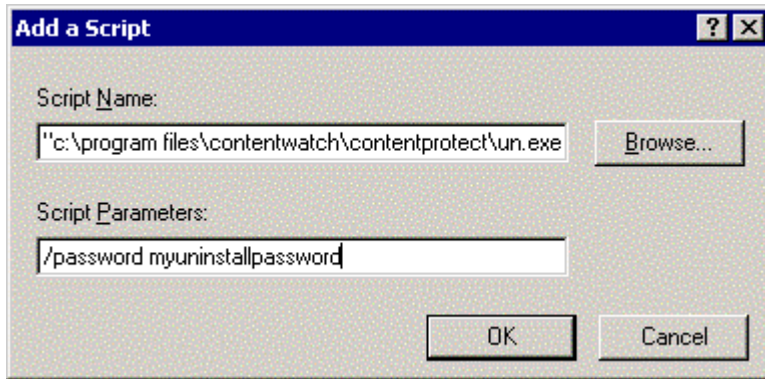
Be sure to thoroughly test the installation script in a test environment before implementing them in your production environment.

### Other Methods

There are several other methods of deployment for the ContentProtect software, the basic requirements are that the installation executable be ran on the computer and that the unattend.txt file exists in the same directory as the installation executable. This could be accomplished with batch files, startup scripts or software deployment tools.

### Uninstall

Repeat the exact same thing except for pointing to the install file, change the script to point to the machines uninstall file.



Script Name: "c:\program files\contentwatch\contentprotect\uninstall.exe"

Script Parameters: /password myuninstallpassword

where "myuninstallpassword" contains the uninstall password created during setup.

To edit/confirm your uninstall password visit <http://ce.contentwatch.com> under the "Organization" menu