

## Download/Install IDENTD

IDENTD is the small software program that must be installed on each user's computer if multiple filters are to be used in ComSifter. The program may be installed and executed locally on each client computer or may be installed on a Domain Controller and pushed to client computers on user login. If a Domain Controller is available this is considered a best practice as the program is installed once and is installed from a secure source.

As part of configuring ComSifter usernames must be entered in the User List and a filter level associated with the username. During normal operation when a user computer requests a web site the ComSifter will query the IP of the requesting computer and ask for its IDENTD. The IDENTD program will respond with the username of the user currently logged into the computer.

ComSifter then matches the username with the filter associated in the User List and applies the filter settings appropriate for that filter. By using IDENTD, multiple users may log into and out of a computer during the day and they will be filtered based on their username, not the computer.

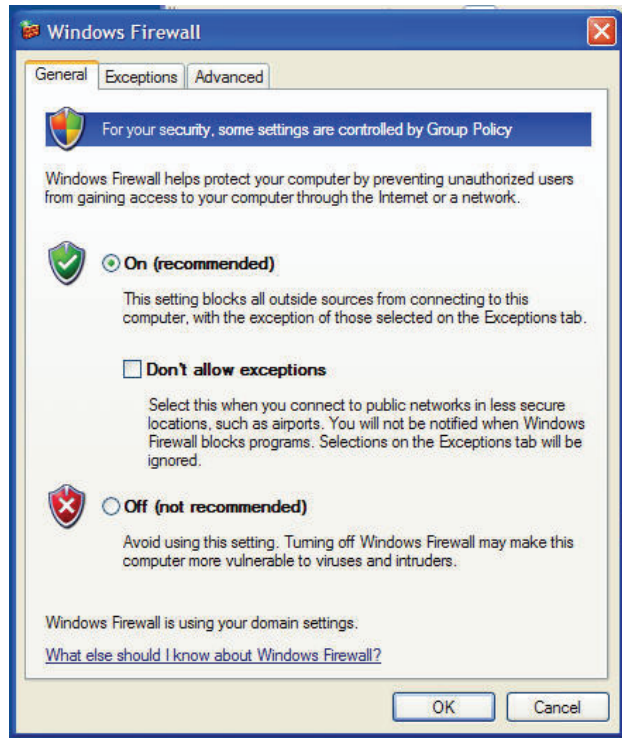
If a user computer that does not have IDENTD installed is queried, and thus does not respond, ComSifter will automatically assign that computer user the username "nousername". By default, "nousername" is automatically routed to the non-IDENTD filter. This default behavior may be changed by adding "nousername" to the ComSifter "user list" and assigning an appropriate filter.

### Port 113 Exception

For the Identd protocol to operate properly Port 113 TCP must be open in both directions on client computers. This may be accomplished by making a port exception in the client firewall. If the client computers are under the control of a Windows 2003 or greater Domain Controller then this may be easily pushed out with a Group Policy rule.

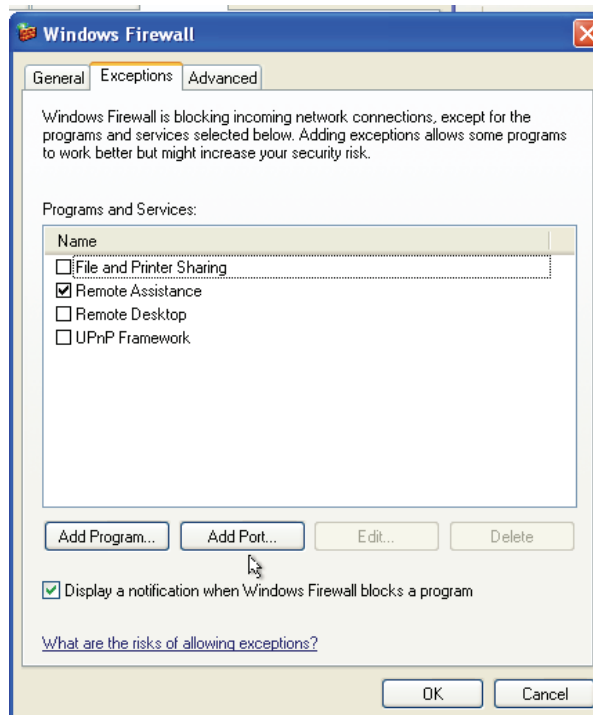
<p><b>Warning:</b> Identd listens on Port 113 of the client computer. If client computers have personal firewalls Port 113 must be opened. If Port 113 is not opened Internet access will fail.</p>
---

## Windows Firewall (local rule for XP)



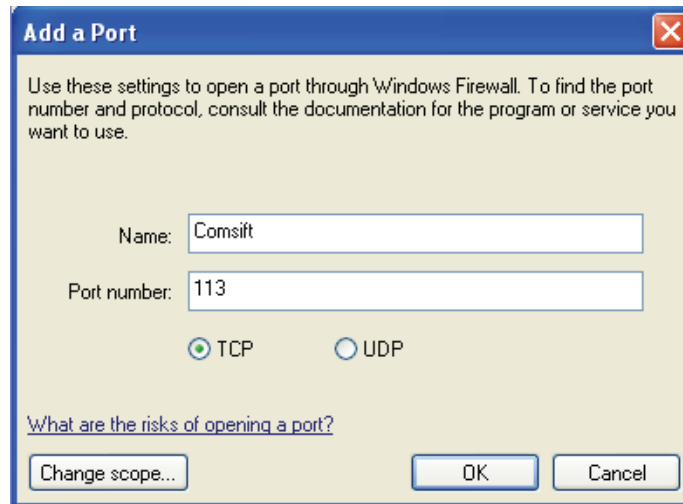
Windows Firewall

1. Open the Windows Firewall.
2. Click on **Exceptions**.



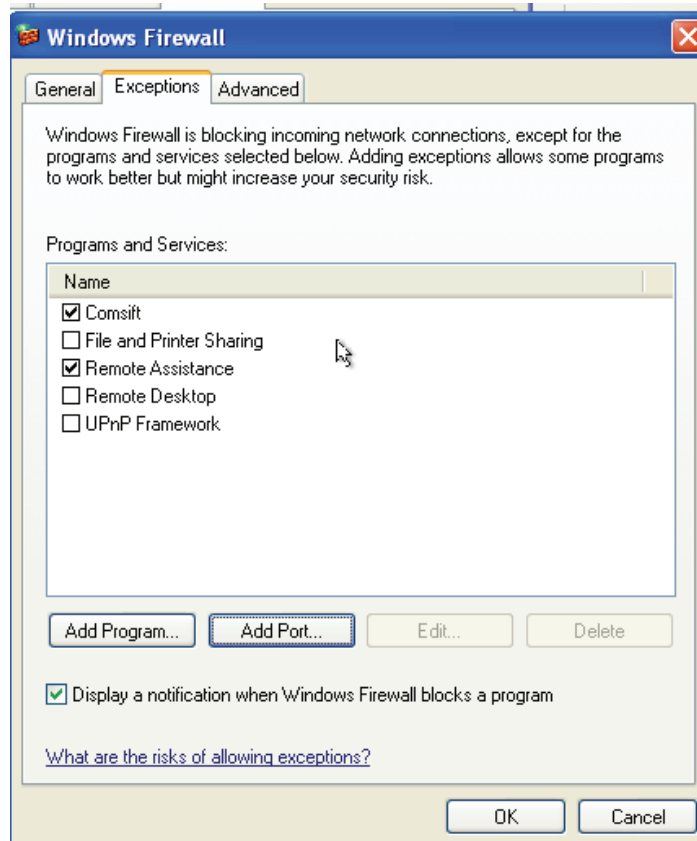
Click Exceptions

3. Click on **Add a Port**.



**Add Port 113 TCP**

4. Enter Comsift as the Name.
5. Enter the port as 113.
6. Ensure that TCP is selected.
7. Click **OK**.

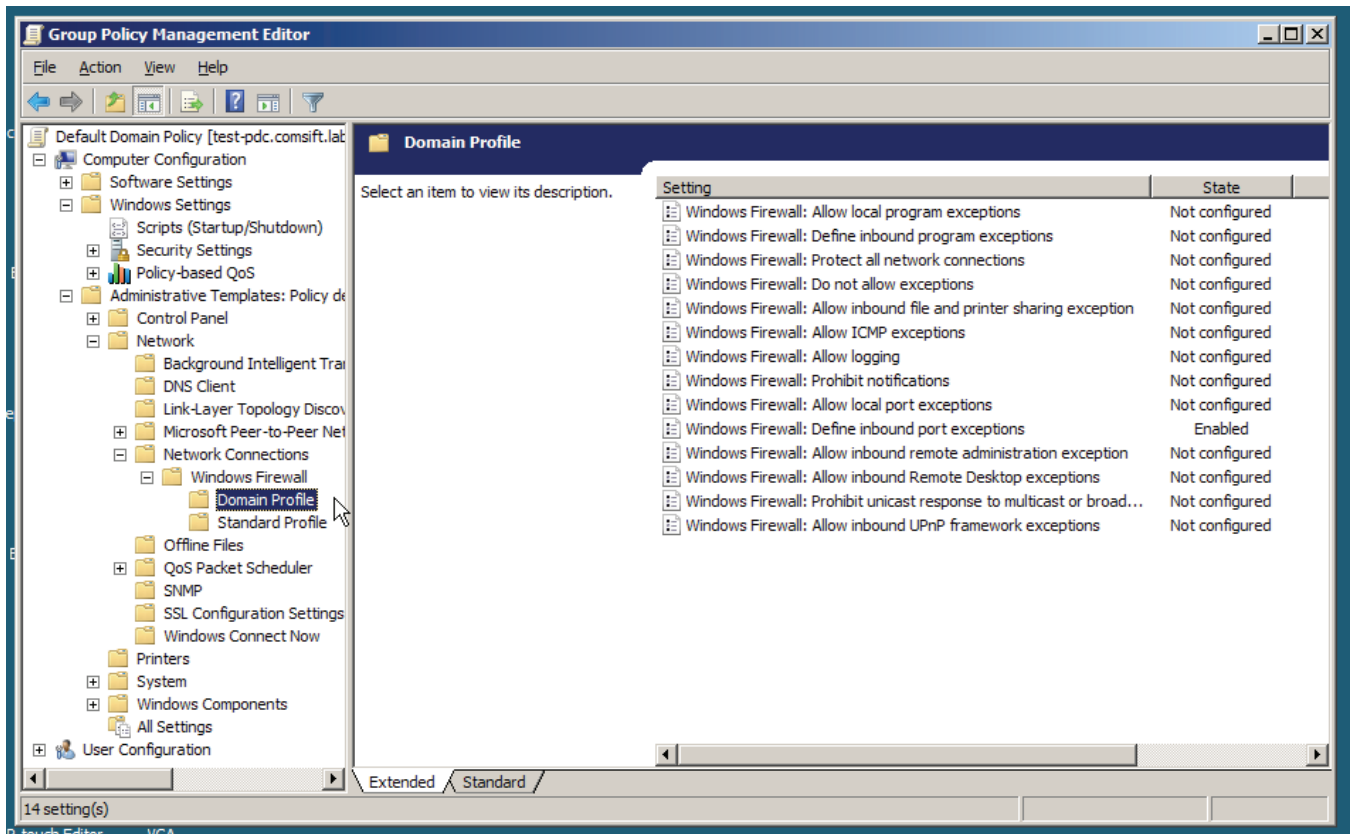


**Finished Rule**

8. You should now see the rule added to your exception list.

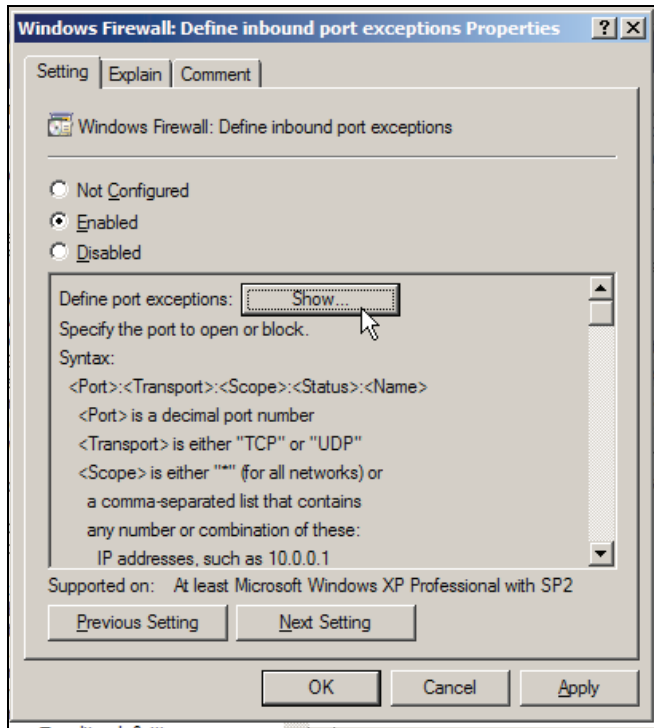
### Windows Firewall (Group Policy rule)

The following rule is applied by way of a Group Policy on Windows 2003 and Windows 2008 servers. This rule will open port 113 inbound on any computer connected to the Domain. As this rule is under Computer Configuration a one time restart of all Domain Computers will be required to activate the rule.



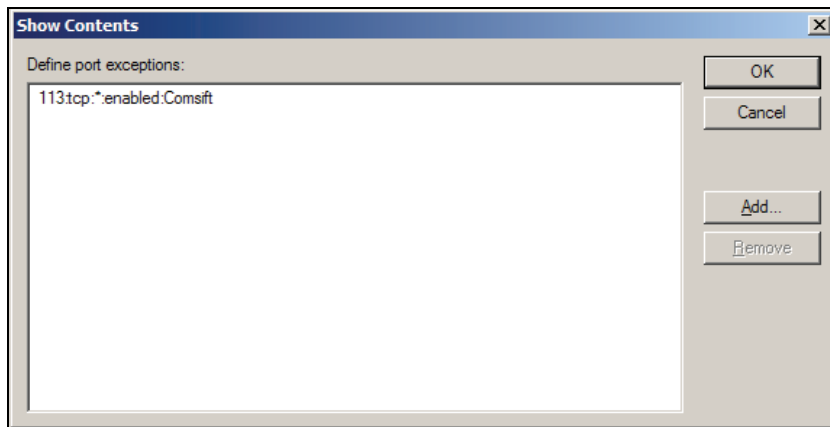
### Port 113 Exception

1. Edit your Group Policy
2. Under Computer Configuration click **Administrative Templates > Network > Network Connections > Firewall > Domain Profiles > Define Inbound Port Exceptions.**



**Define Properties**

3. Click on **Enabled**.
4. Click on **Show**.



**Show Contents**

5. Enter the following string into the text field. 113:tcp:\*:enabled:Comsift
6. Click **add**.

## Install Identd

Identd must be executed on the local client computers. The best method of deploying Identd is dependent on the types of operating systems used in your network and if your network is part of a domain. The following matrix described the best method for each type of installation.

Network	Comsift Service Local Install	Comsift Service Automated Install (preferred)	Comsift Connection Local Install	Windows Server, Comsift Connection pushed out at login
Peer to peer Vista/XP	Install Comsift Service on each workstation			
Domain Vista/XP		Use Group Policy Software install to install Comsift Service on each workstation		
Peer to peer Vista/XP/2000/98			Install Comsift Connection on each workstation	
Domain Vista/XP/2000/98				Use Group Policy login Script to push out at each login

**Warning:** ComSifter CS-8 Pro NS relies on secure authentication from the client workstation. Windows NT/2000/XP, Apple Mac and Linux are able to provide this secure authentication. Windows 95/98/ME is unable to provide secure authentication. As a result Comsift is unable to officially support Windows 95/98/ME. If you have a mixed environment that includes these unsupported Operating Systems, Comsift suggests the following best practices.

Option 1: The identification program Comsift uses, IDENTD, should be executed from a file server or domain controller, which requires proper

authentication. Do not load the IDENTD program from a local hard drive.

Option 2: Do not use the IDENTD program on Windows 95/98/ME workstations. Without IDENTD, client workstations will be routed automatically to the non-IDENTD filter. Configure this filter for your Windows 95/98/ME clients.

**Note:** Administrator privileges are required for all operating systems to properly install Identd.

## Identd location

The Identd Utilities are located on the Documentation and Utilities CD that came with your ComSifter and also located in the Comsifter under Maintenance > Download/Install Identd. To download the utilities from the ComSifter follow these steps:



### Download/Install IDENTD from ComSifter

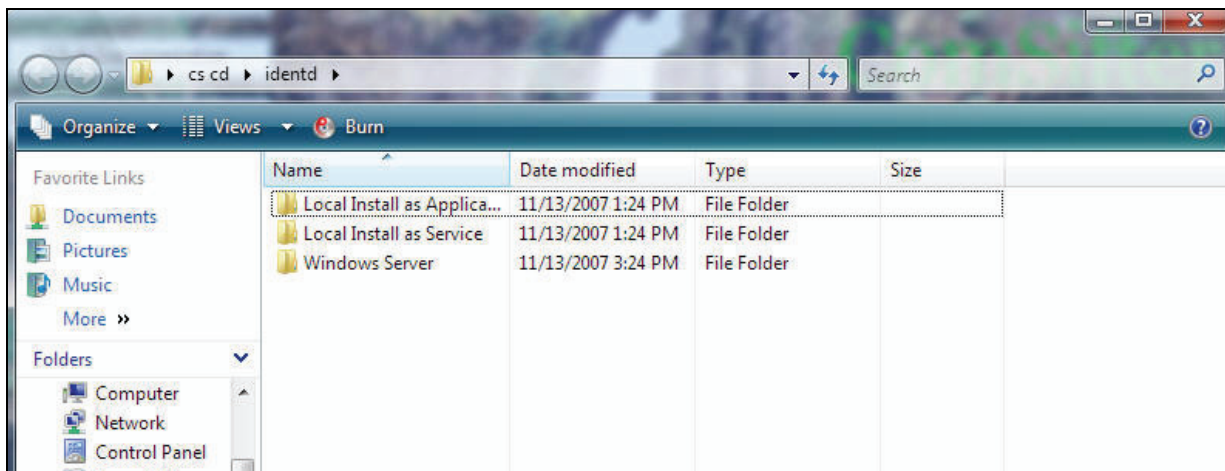
1. Select **Identd.zip** from within the directory for the type of installation being performed and click on the **Save** icon.
2. A standard save dialog box for your operating system will open allowing you to save the file to the location of your choice.
3. Unzip the program using any standard zip/unzip program to a location of your choice.

To use the utilities available on the CD follow these steps:



**ComSifter CD**

1. Insert the CD.
2. Autorun will run and you should see the ComSifter splash page.
3. Click on **Identd Utilities** to open the following page.
4. Determine which Identd to install.



**Open Identd Utilities**

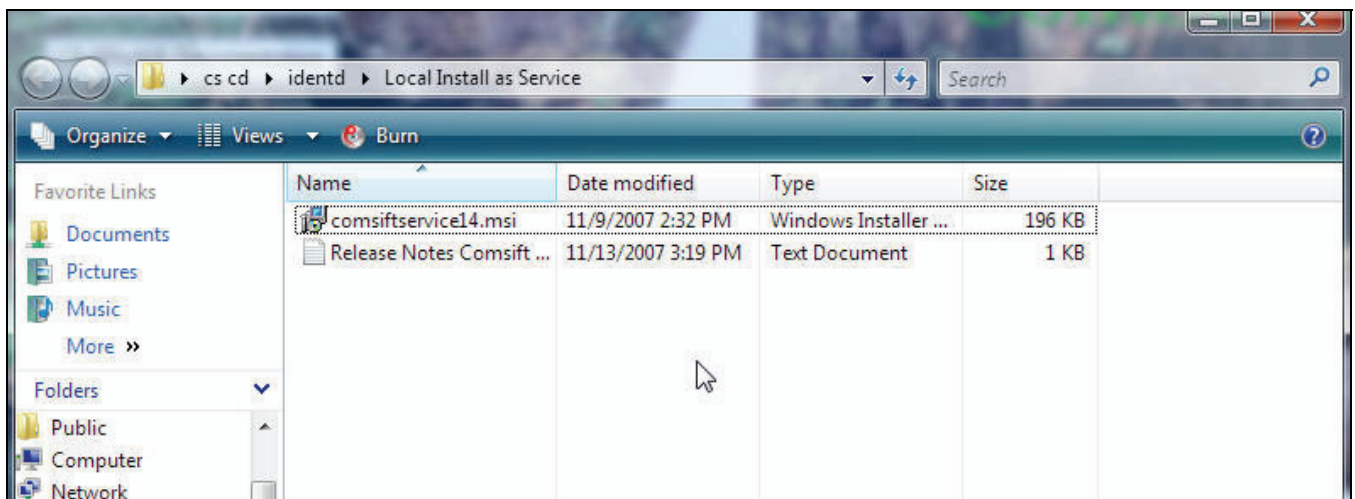
## Comsift Service Local Install

Comsift Connection runs as a Service and is compatible with the following Windows OS's.

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

To install Comsift Service on a local computer double click **comsiftservice14.msi**. After installation completes Comsift Service will be listed in the computer's Services.

**Note:** Comsift Service will not appear in Add/Remove Programs. It must be installed by an administrator. The installer is designed for silent installation. Once started it will complete unless there is an error. This design allows the .msi file to be used in a Group Policy for automated software installation as defined in the user guide.

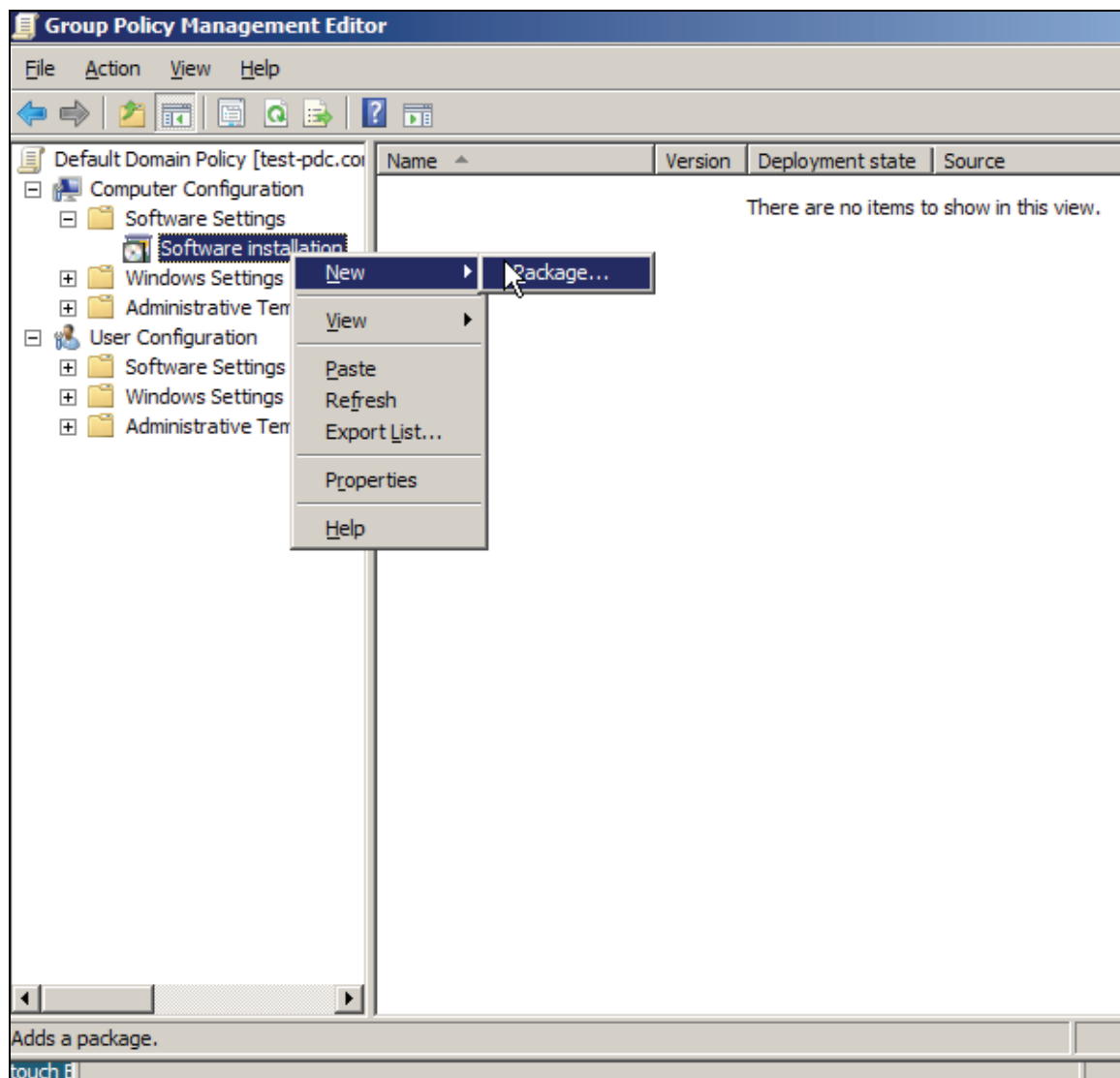


**Comsift Service Local Install**

### Comsift Service Domain Automated Install (preferred)

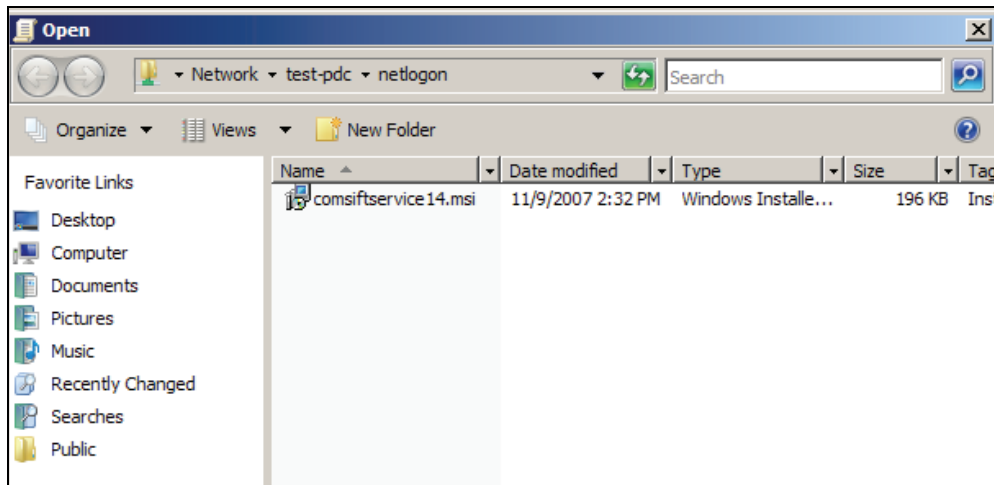
Comsift Service is designed to be easily used in a Group Policy and automatically installed to all Vista/XP computers that are part of a Domain.

1. Copy comsiftservice14.msi to a Domain User accessible directory located on your domain controller.
2. Open the Group Policy editor to the Group Policy of your choice.
3. Open Computer Configuration > Software Installation > New > Package.



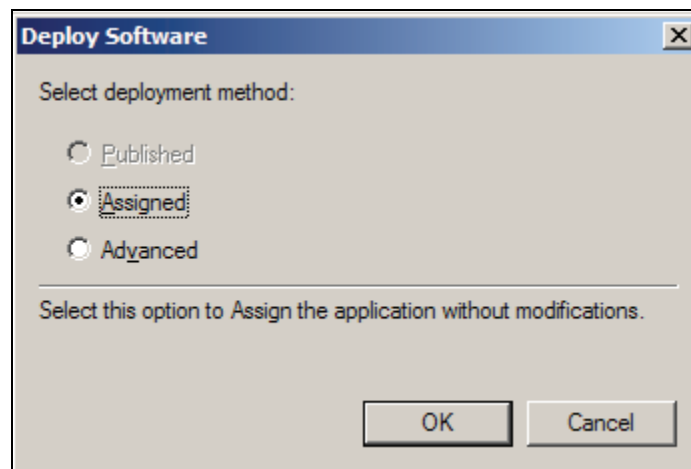
**Add New Package to Software Installation**

4. Browse to the location that you copied `comsiftservice14.msi` to and double click **comsiftservice.msi**.



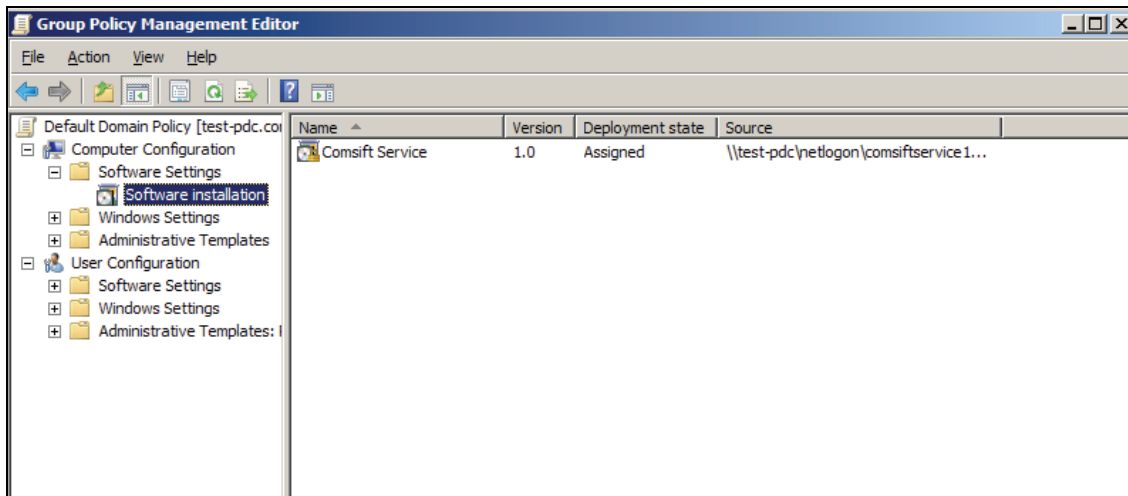
**Select comsiftservice.msi**

5. You will be prompted to select a deployment method. Select **assigned** unless your requirements differ.



**Select Deployment Method**

6. After a few seconds Comsift Service will appear as shown in the following figure.



**Finished Rule**

### Comsift Connection Local Install

Comsift Connection has been deprecated and replaced by Comsift Service. Comsift Connection should only be used for Windows 2000 or earlier OS'S.

Comsift Connection runs as an application and is compatible with the following Windows OS's.

- Windows 98
- Windows ME
- Windows 2000
- Windows Server 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

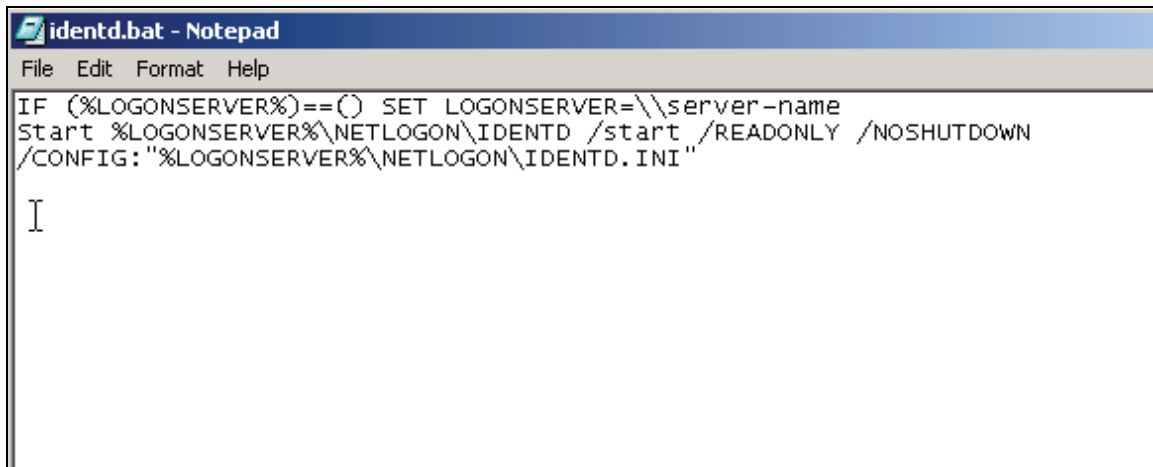
**Note:** Comsift Connection will not appear in Add/Remove Programs. It must be installed by an administrator. The installer is designed for silent installation. Once started it will complete unless there is an error. This design allows the .msi file to be used in a Group Policy for automated software installation as defined in the user guide.

1. Double click the local Installation as Application folder.
2. Double click the **comsiftconnection.msi** file
3. When prompted restart the computer.

The IDENTD program will now start every time the computer is started.

## Windows Server Automated Push

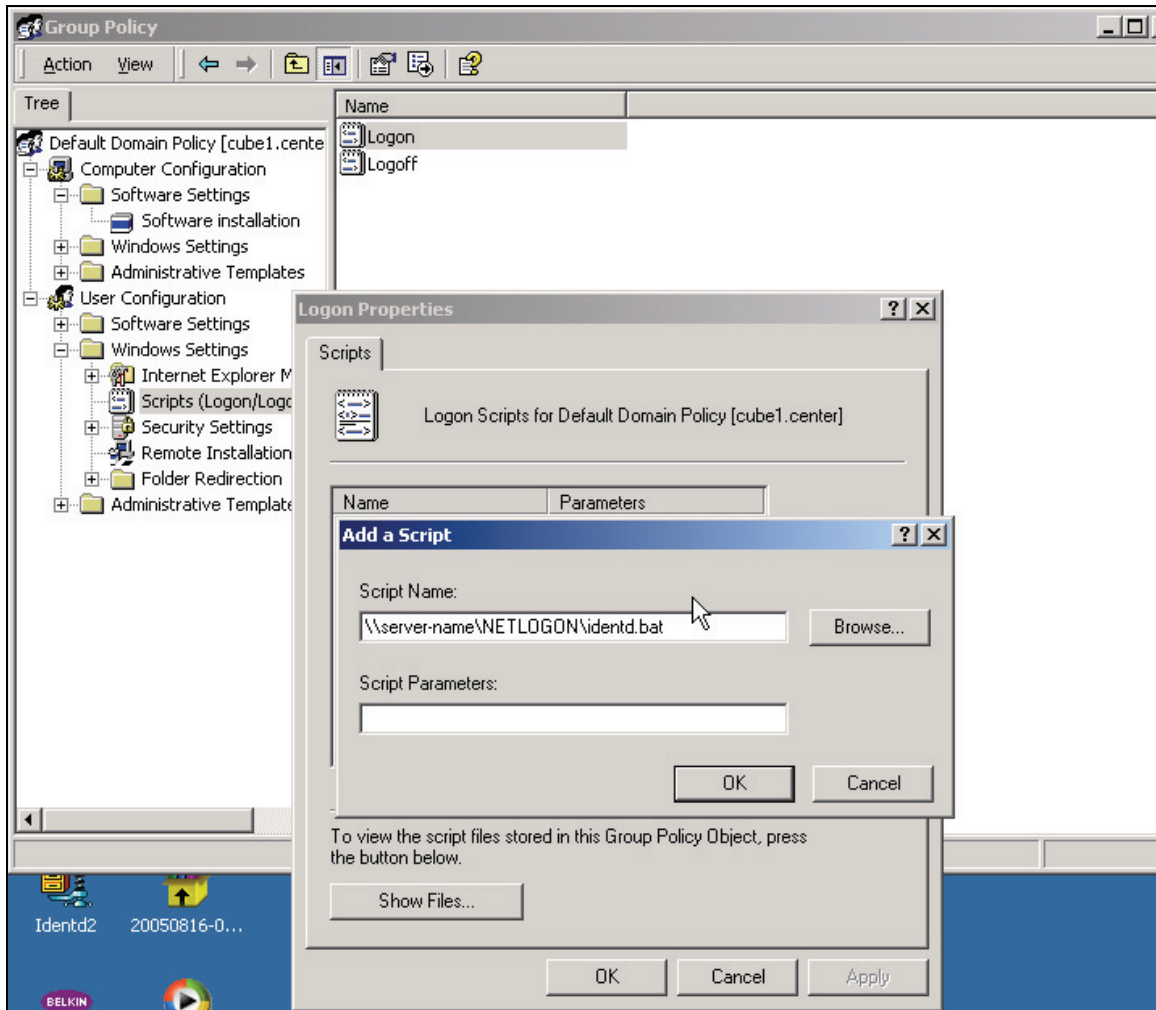
1. Unzip the files that are in identd.zip. This file is found on the Documentation and Utilities CD or in the ComSifter under Maintenance > Download/Install Identd > Windows.
2. Extract the files into your domain controller NETLOGON directory which by default is in c:\winnt\sysvol\sysvol\yourdomainname\scripts
3. Edit the first line of identd.bat file by changing server-name to the computer name of your server (not your domain name).



```
identd.bat - Notepad
File Edit Format Help
IF (%LOGONSERVER%)==( ) SET LOGONSERVER=\\server-name
Start %LOGONSERVER%\NETLOGON\IDENTD /start /READONLY /NOSHUTDOWN
/CONFIG: "%LOGONSERVER%\NETLOGON\IDENTD.INI"
I
```

### Identd Server Batch File

7. In Control Panel open Administrative Tools > Active Directory Users and Computers.
8. Right click your domain name and click properties.
9. Click the tab that says **Group Policies**
10. Open Default Group Policy
11. Open User Configuration -> Windows Settings -> Scripts(logon/logoff) -> Logon -> Add



### Server Logon Script

12. In the Script Name field enter the UNC path to your server (\\your servername\NETLOGON\identd.bat) (netlogon is case sensitive)
13. There are no Script Parameters

The IDENTD program will now be installed and started every time a Domain User logs into a Domain Computer.