

---

Technical documentation:

# **SPECOPS SELF SERVICE PORTAL 2.2 INSTALLATION AND CONFIGURATION GUIDE**



By Markus Lassfolk, Product Specialist,

---

SPECOPS SELF SERVICE PORTAL 2.2 INSTALLATION AND CONFIGURATION GUIDE .....	1
1 Introduction.....	4
2 Specops Self Service Portal and Active Directory.....	5
3 SSP Prerequisite Components .....	5
3.1 Windows Server Operating System.....	5
3.2 Microsoft .Net Framework 3.5 SP1 .....	5
3.3 Microsoft Management Console 3.0 .....	5
3.4 Microsoft Group policy Management Console.....	5
3.5 Microsoft SQL Server .....	5
3.6 Mail Server .....	6
3.7 Microsoft PowerShell 2.0 .....	6
3.8 Microsoft Silverlight.....	6
4 How to Setup Specops Self Service Portal .....	7
4.1 Self Service Portal Server Installation.....	8
4.2 Admin Tools Installation.....	12
5 Specops Self Service Portal – Configuration .....	14
5.1 Delegate Control for SSP Service Account .....	14
5.2 Remote GpUpdate.....	17
5.2.1 Adding SSP Service Account to all client’s Local Administrators Group.....	18
5.2.2 Configuring Windows Firewall to allow remote management for Windows 7.....	19
5.2.3 Configuring Windows Firewall to allow remote management for Windows XP. ....	20
5.3 Controlling ownership of clients. ....	21
5.3.1 Configuring automatic client ownership .....	21
5.3.2 Delegating permission to client’s to update ManagedBy attribute. ....	24
5.4 Allowing users to trigger a reinstall from SSP .....	26

# SPECOPS : TECHNICAL DOCUMENTATION

6	Specops Self Service Portal – Administration Guide .....	27
6.1.1	Creating units .....	28
6.1.2	Creating Services or applications .....	29
6.2	Administrative Rights .....	30
6.3	Deployments .....	30
7	Verification .....	31
7.1.1	Approval and Revocation .....	31
7.1.2	Single Sign On.....	32
8	Customizations .....	33
8.1.1	Branding .....	33
8.1.2	Reducing wait time for Specops Deploy .....	33
9	Support and Troubleshooting.....	34
9.1	Event Log.....	34
9.2	Debug Logging .....	34
9.3	Online Resources.....	34

## 1 Introduction

The Specops Self Service Portal (SSP) allows a user to request applications automatically without contacting the helpdesk. SSP portal is a stand-alone product that can be used in combination with Specops Deploy or with another deployment solution that can utilize security groups for control.

There is built-in support for a request and approval workflow with deployments per user and per computer with control of which computer(s) a user can request software to.

The main focus of SSP is to manage application and OS Deployments, but it can also be used to manage other scenarios like Access to Shares, Mail Distribution Lists or other security group features.

Some customers may allow users to request access to services (controlled by for example Group Policies security filtering) through SSP in addition to applications.

- Microsoft Direct Access
- Microsoft BitLocker
- Folder Redirection
- Offline Files
- Access to Network Shares
- Access to Printers
- Distribution lists

## 2 Specops Self Service Portal and Active Directory

- *NOTE: Although Specops Self Service Portal integrates into Active Directory, it does not edit or extend the Active Directory Schema.*
- An Active Directory Service Account is required to run the Specops Self Service Windows Service. This account should be setup and configured in advance. The account should only be part of the “Domain Users” security group. This account should have a very strong password.
- Active Directory administrative rights are required to configure the product and modify and apply group policies during setup.

## 3 SSP Prerequisite Components

### 3.1 Windows Server Operating System

The SSP Server requires Windows Server 2003 or higher installed to host the SSP components. This can be an existing server or a dedicated server.

### 3.2 Microsoft .Net Framework 3.5 SP1

The SSP Setup Assistant requires that Microsoft .Net Framework 3.5 SP1 is installed on the server where the Setup Assistant is started. If it is not installed it can be downloaded from Microsoft for free.

### 3.3 Microsoft Management Console 3.0

SSP requires the Microsoft Management Console version 3.0 installed on the computers where group policies for SSP will be managed.

### 3.4 Microsoft Group policy Management Console

The SSP Admin Tools requires that Microsoft Group Policy Management console be installed on the computer where the admin tools need to be used.

### 3.5 Microsoft SQL Server

An instance of Microsoft SQL Server is required to host the SSP Database. This is used to store the configuration and approval information. The SQL Server does not have to be running on the same computer as the SSP Server and any SQL server (including SQL Server Express) instance can be used.

SSP uses a database called *SpecopsSelfServicePortal*. The SSP Setup Assistant will create the database if no database with that name exists. The database will use default values for location on disk and other settings and the initial size will be 50 MB with a transaction log of 20 MB. If special requirements exist for location, size etc. for the database files then the database can be created manually before the SSP Setup Assistant is started. All versions of SQL above Microsoft SQL 2005 SP3 are supported with SSP

## **3.6 Mail Server**

SSP requires a mail server with SMTP support to send e-mail notifications for request and approval workflows. The server has to support anonymous SMTP relay from the SSP Server.

## **3.7 Microsoft PowerShell 2.0**

SSP requires PowerShell 2.0 on the server where it's installed. It can be downloaded for free from Microsoft if not installed.

## **3.8 Microsoft Silverlight**

Silverlight has to be installed on any client computer using the SSP for administration or application requests. Microsoft Silverlight is a free extension to the Web Browser.

## 4 How to Setup Specops Self Service Portal

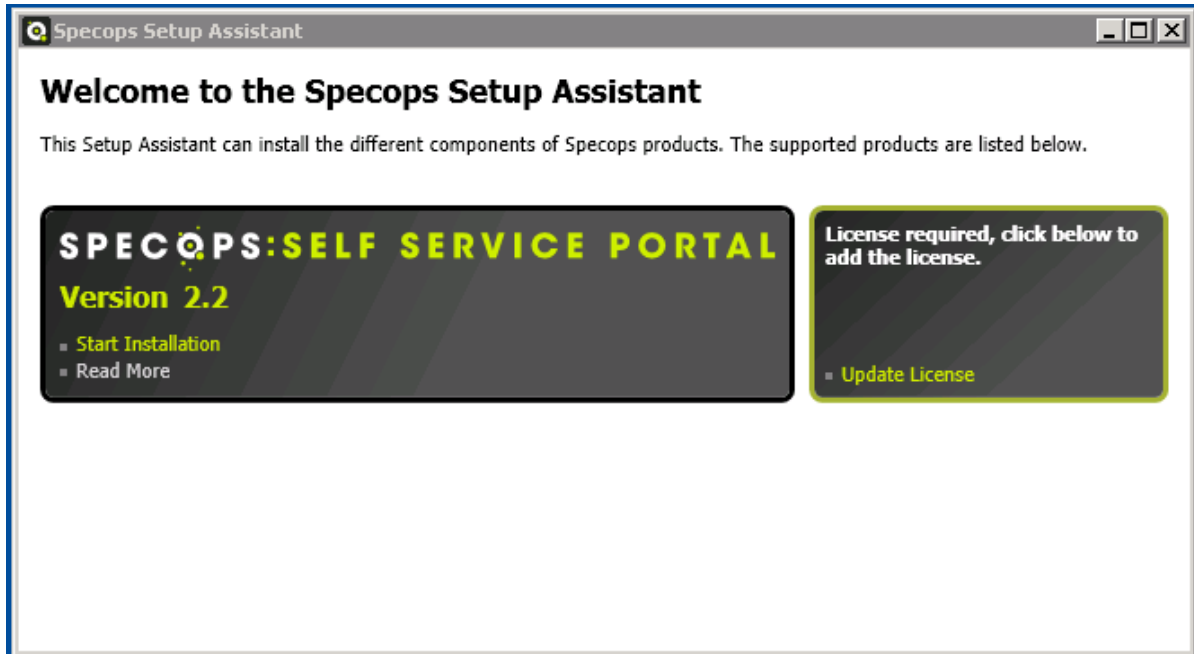
The Specops Self Service Portal (SSP) ships as one binary file. When extracted it launches a program called Specops Self Service Portal Setup Assistant. This Setup Assistant will help an administrator install SSP in an Active Directory environment.

The Setup Assistant should be run for the first time on the computer intended to be used for the SSP server. The Setup Assistant guides the administrator through two different steps that should be performed in the following order to get started as fast as possible:

- **Server installation** – This will install the SSP Database and Server Service software on the local computer.
- **Admin tools installation** (on a single computer) – Installs the Specops Self Service Administrative Tools on the local computer. Admin Tools can be installed on multiple computers in the environment.

## 4.1 Self Service Portal Server Installation

1. Start the Self Service Portal Setup Assistant
2. If .NET Framework 3.51 is not installed, a dialog box will inform the end user that it's required to install before the Setup Assistant can be launched.



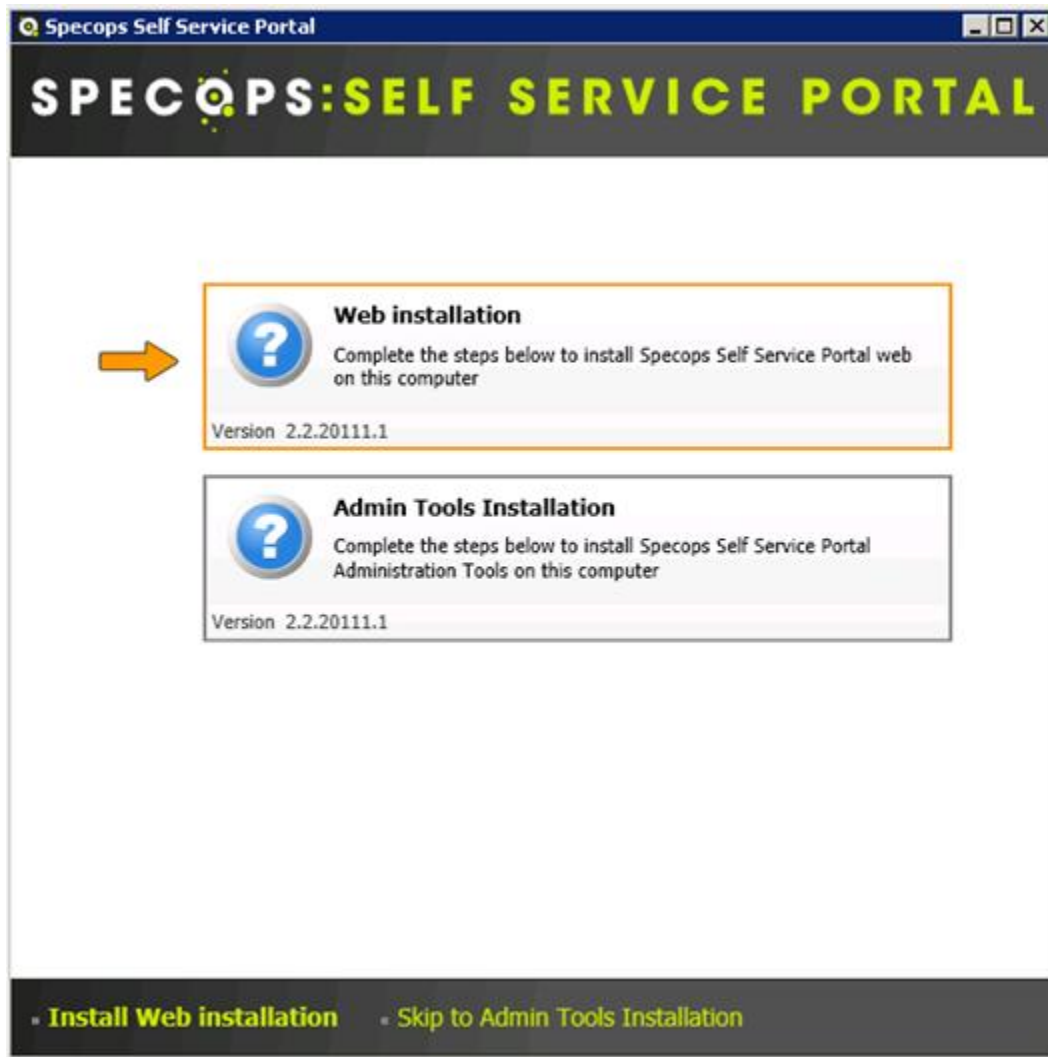
3. Import the SSP 2.2 License File by clicking “Update License” and browse to the License file.
4. When the license is imported, click Start Installation.
5. Read and Accept the License Agreement.



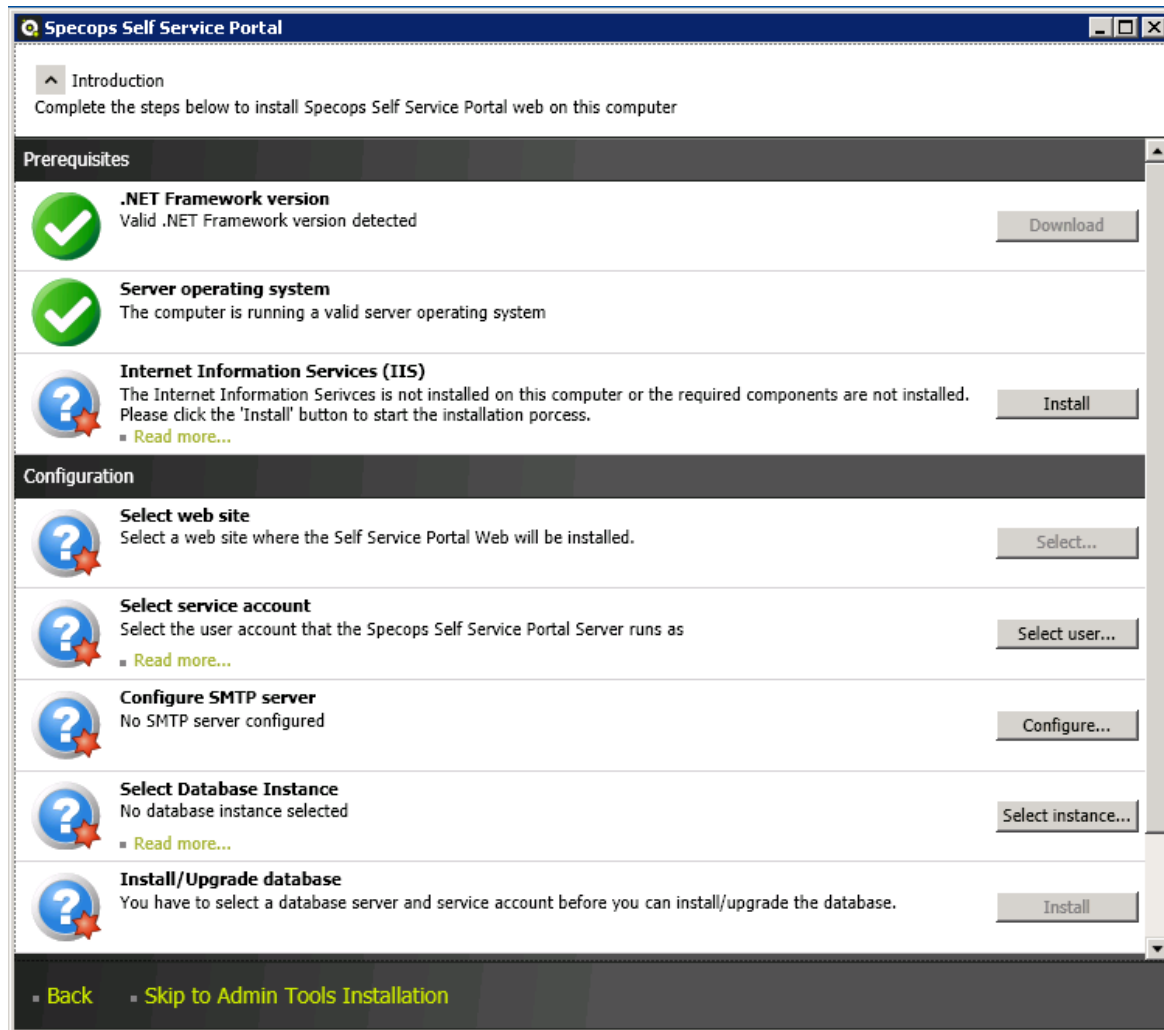
# SPECOPS : TECHNICAL DOCUMENTATION

6. A window will now present two options, to install the Web Component and Administrative Tools.

Click on “Web installation” to initiate the web installation.



7. SSP Server setup is initiated and a window similar to this should be presented;



8. .NET Framework 3.51 is a Prerequisite to launch the Setup Assistant so that check should pass.
9. SSP is required to run on a Windows Server OS.
10. If needed, click Install to install IIS automatically with all required components.
11. Next, select WEB Site to use.  
No passwords or sensitive information is sent to/from SSP. A secure connection (HTTPS) is optional.
12. Enter an existing service account. A normal Domain User account with no extra permissions is recommended.  
If there is no process in place to renew passwords on service accounts, use "password never

expire” on the SSP service account.

More details below on how to grant the required permissions for each function and feature.

13. Configure SMTP Settings.

SSP will use an anonymous connection to the SMTP server.

Enter the e-mail address used by SSP to communicate with users and admins.

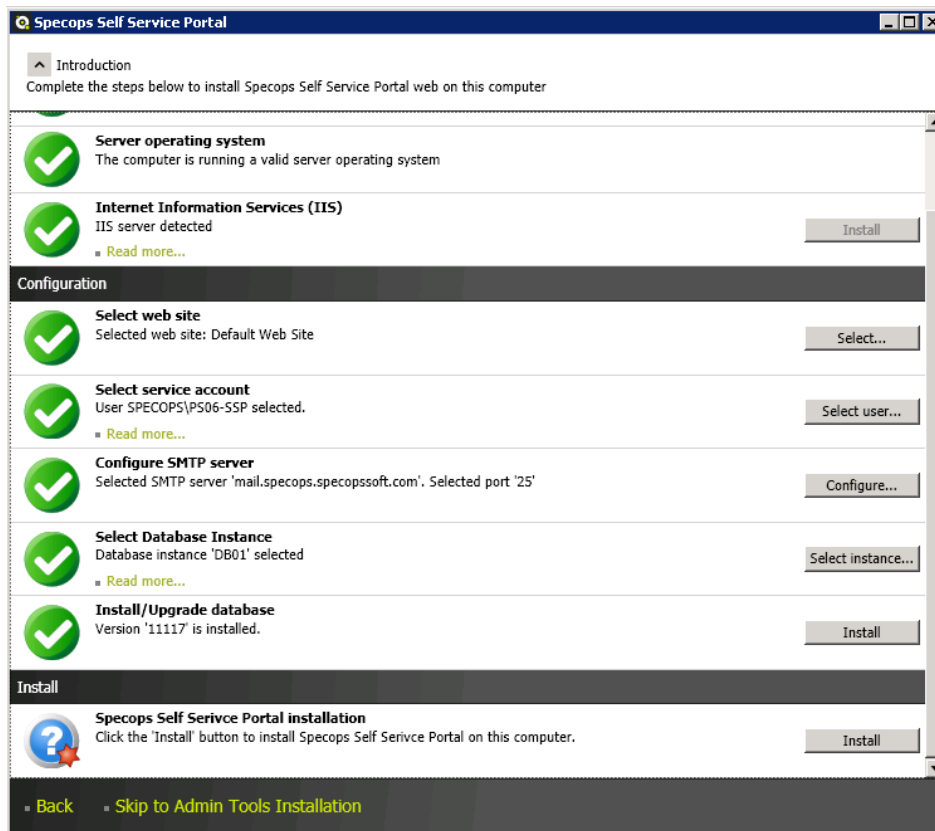
This should preferably be a monitored e-mail address in case a user replies to the e-mail.

14. Select the SQL Server to install the database on. If there is no SQL Server in the domain it’s possible to download a free version of SQL Express from Microsoft and install locally before proceeding.

A database called “SpecopsSelfServicePortal” will automatically be created and used.

15. Click Install to install the Database on the SQL Server.

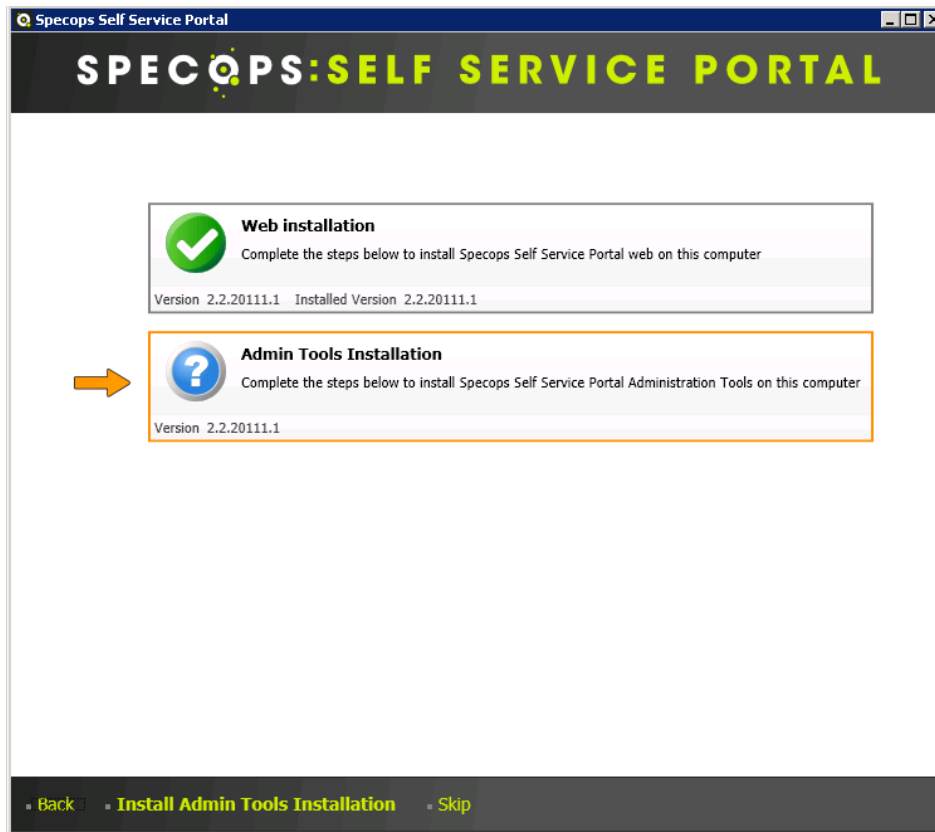
16. When all prerequisites are met, click Install to initiate Specops Self Service Portal installation.



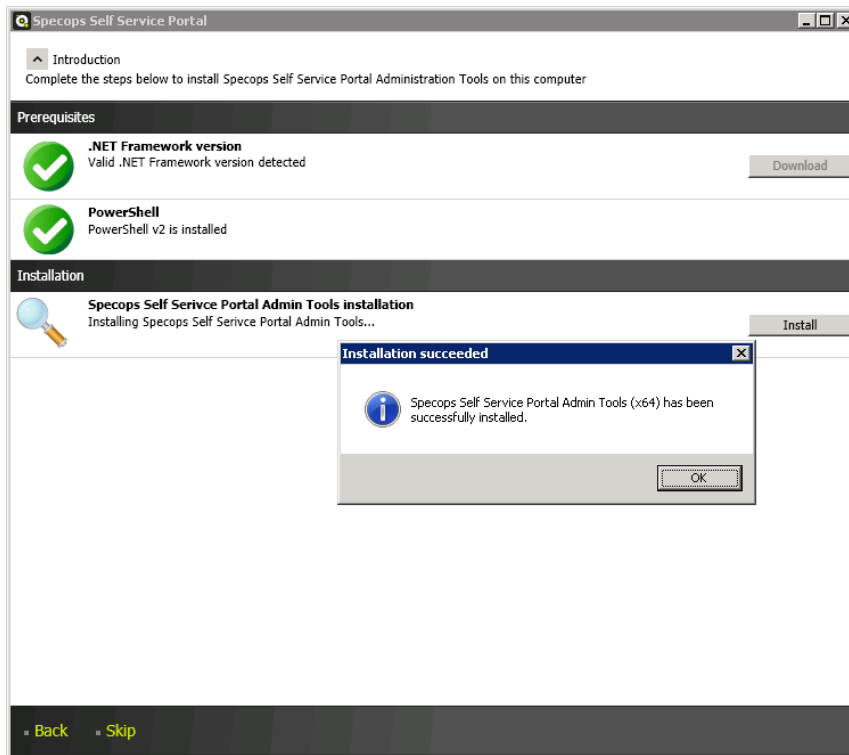
## 4.2 Admin Tools Installation

The Specops Self Service Portal Admin tools can be installed on any computer being used to administer the Specops Self Service Portal.

- Next, install Admin Tools



- Installation of Specops Self Service Portal is done.



There are some additional configurations needed depending on which features in SSP that will be used.

## 5 Specops Self Service Portal – Configuration

To allow the SSP to manage group membership, delegate control to the service.

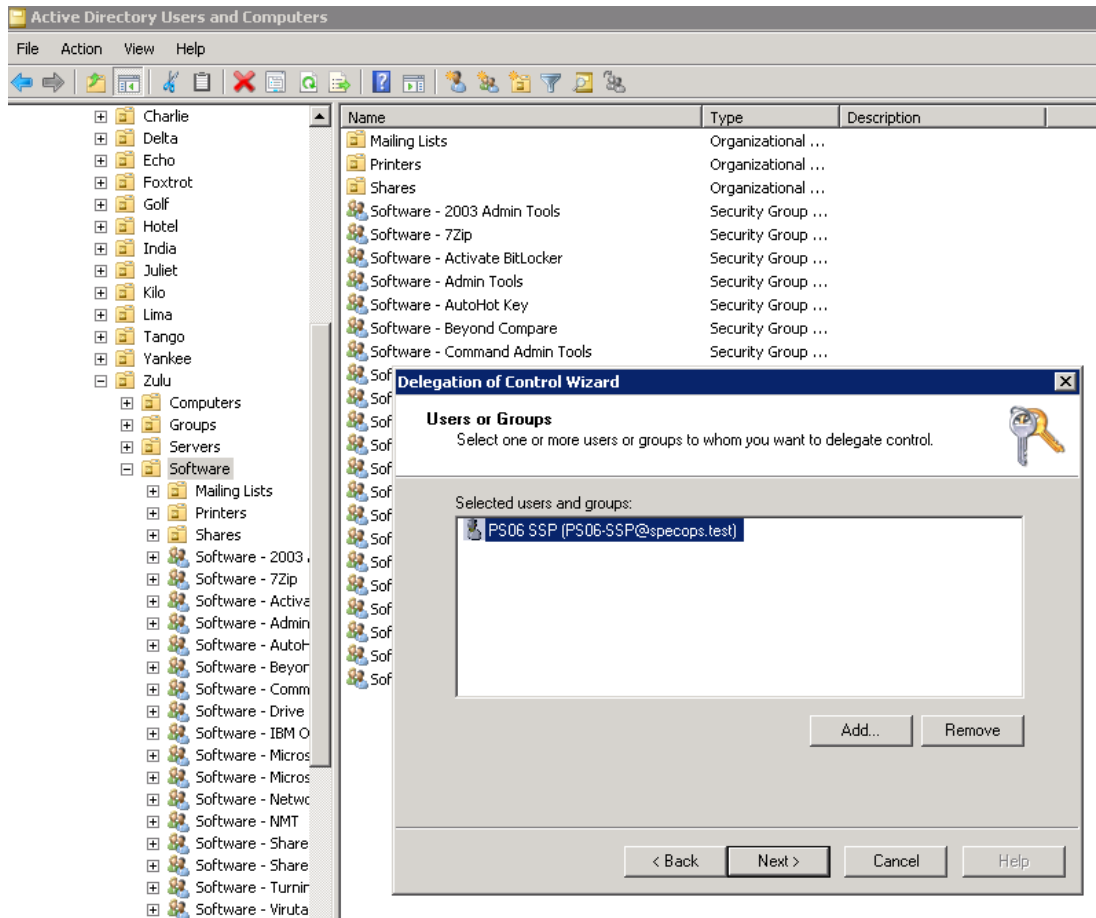
*Note: A best practice is to create a separate root OU with SubOU's for various services that can be managed through SSP.*

*Note: Do not delegate control from the Domain Root, this could give the SSP Service Account far more access than intended and make it possible for a rogue admin to get access to additional resources.*

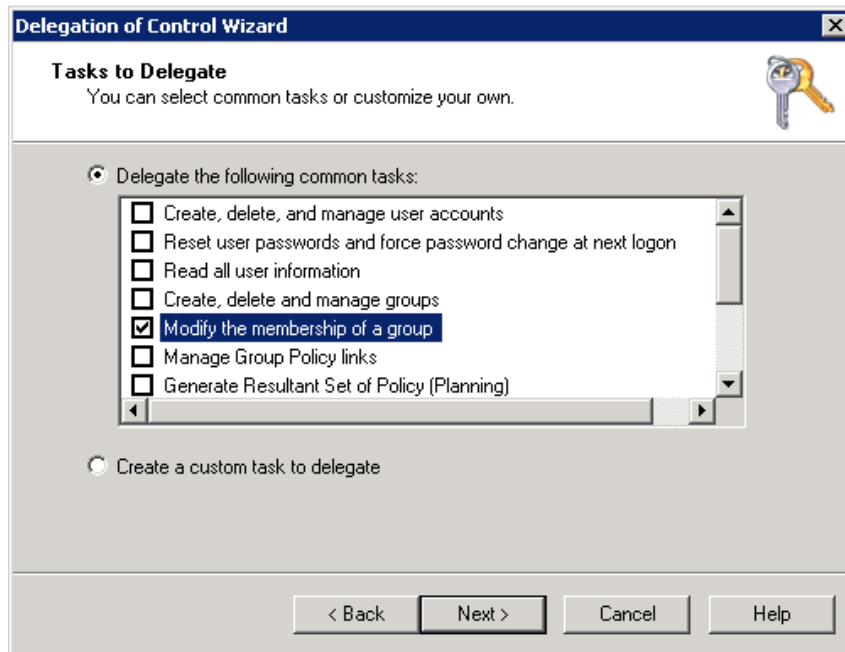
### 5.1 Delegate Control for SSP Service Account

1. Open Active Directory Users and Computers
2. Navigate to the root OU of where the Security Groups are, or do this multiple times when groups are stored in multiple different OU's.
3. Right Click on the OU and choose “Delegate Control...”
4. Click Next

5. Choose the Specops Self Service Portal Service Account to grant it permission.



6. Grant Permission to “Modify the membership of a group”.



7. Click Next.
8. Click Finish.

The SSP Service Account now has permission to modify membership of the security groups.



## 5.2 Remote GpUpdate

It's possible to allow the Specops Self Service Portal to perform a remote gpupdate on a client and thus initiate a software installation at once. For this functionality, the SSP Service Account requires permissions on the client, and the Firewall must not be blocking traffic.

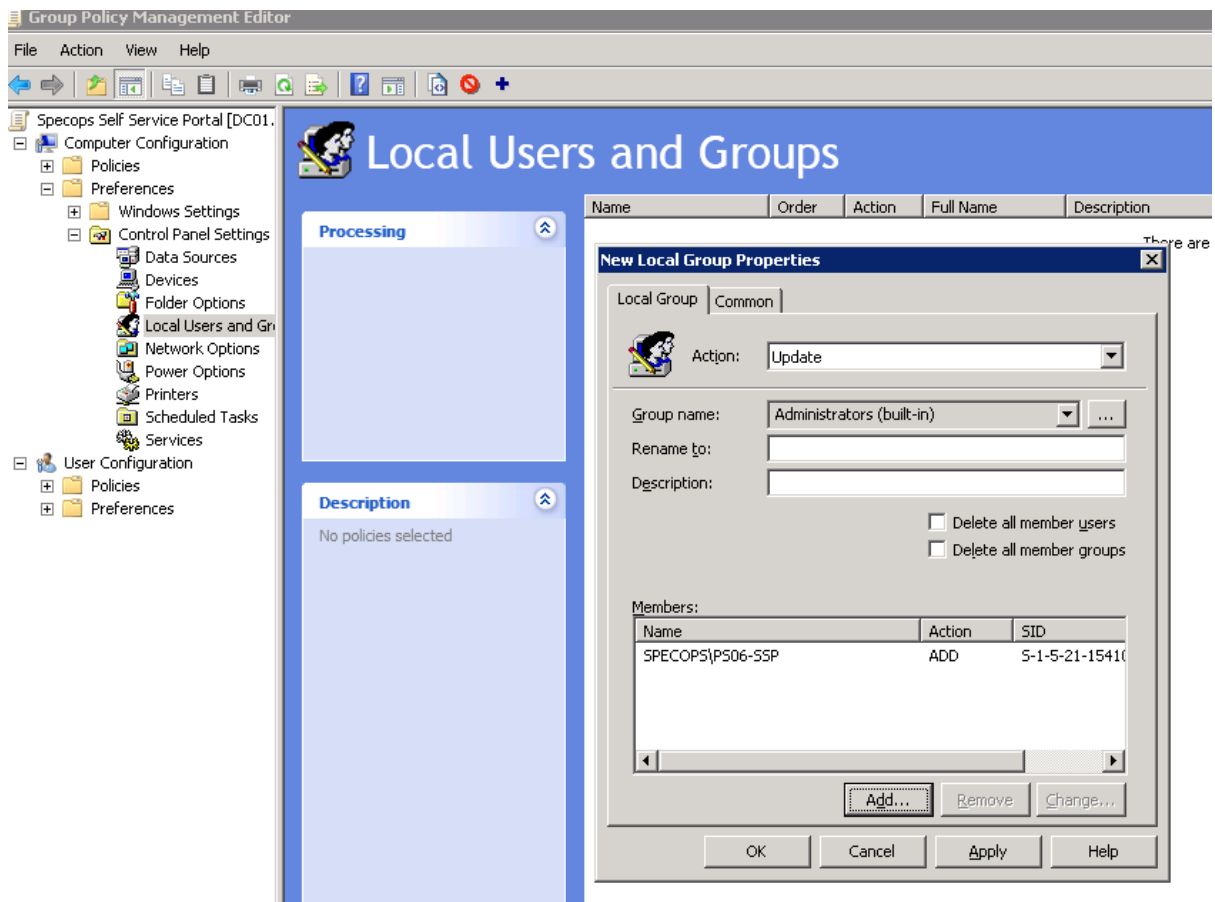
If this feature is not used, a computer will install the software at the next group policy update which is either executed manually by a user or normally executed every 90-120 minutes.

It's possible to use Group Policies to automatically configure this on all clients in the environment.

1. Open Group Policy Management Console (GPMC).
2. Create a New GPO or use an existing GPO that is applied to all clients that will use SSP.

## 5.2.1 Adding SSP Service Account to all client's Local Administrators Group.

1. In GPMC Navigate to: Computer Configuration -> Preferences -> Control Panel Settings -> Local users and Groups
2. Right click, choose "New -> Local Group"
3. Use these settings:  
Action : Update  
Group Name : Administrators (built-in) - (Pick from the list)  
Rename to : <empty>  
Description : <empty>  
Members : add the SSP service account



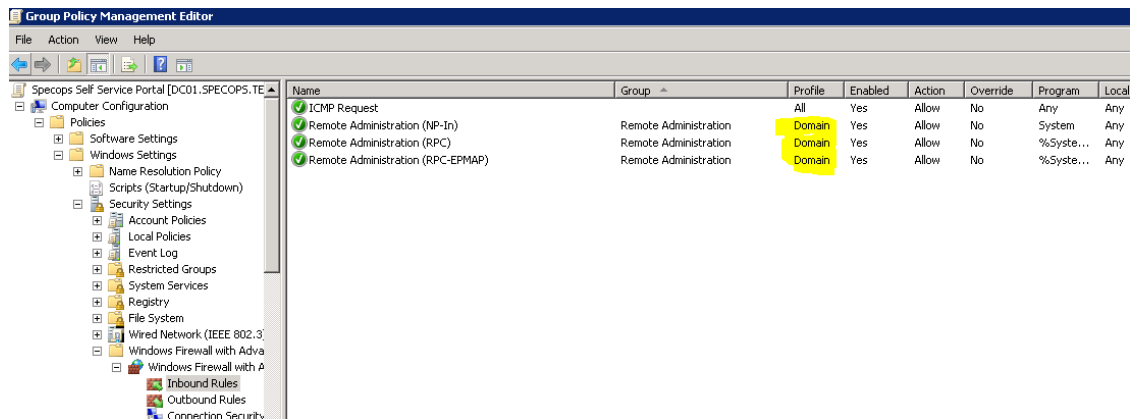
4. Then click OK

## 5.2.2 Configuring Windows Firewall to allow remote management for Windows 7.

To allow the SSP Service Account to initiate a remote gpupdate, Windows Firewall (or any third-party firewall) needs to allow that traffic from the SSP Server to the client.

To configure Windows Firewall on all Windows 7 clients to allow remote management follow these steps.

1. Navigate to Computer Configuration -> Policies -> Security Settings -> Windows Firewall with Advanced Security -> Inbound Rules
2. Right click, New Rule ...
3. Choose Predefined : Remote Administration
4. Click Next
5. Click Next
6. Click Allow the connection
7. Click Finished
8. Do the same for ICMP (Echo) to make the client answer to Ping requests.
9. An administrator may want to increase security by modifying the rules to only open the ports when the computer is connected to the corporate (domain) network.

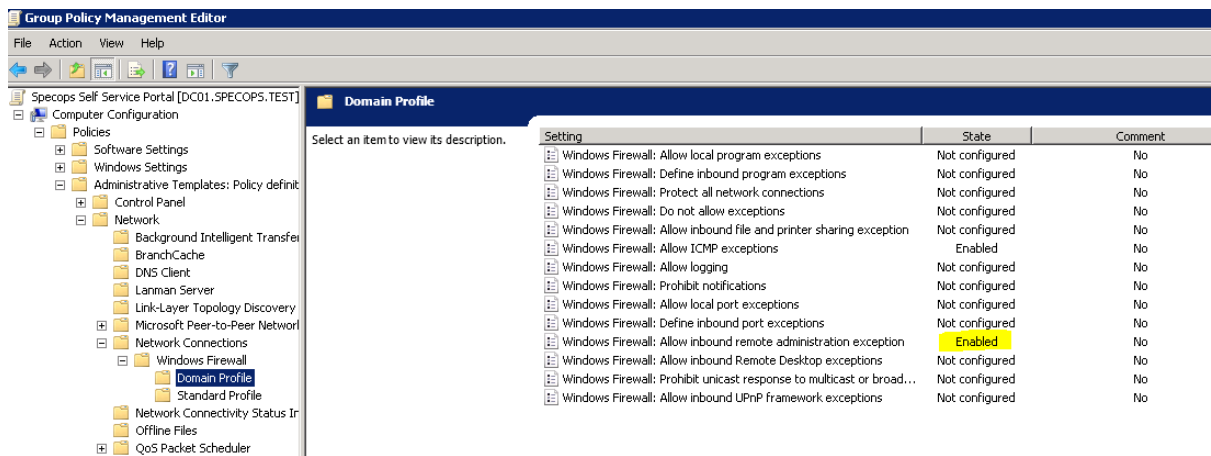


## 5.2.3 Configuring Windows Firewall to allow remote management for Windows XP.

To allow the SSP Service Account to initiate a remote gpupdate, Windows Firewall (or any third-party firewall) needs to allow that traffic from the SSP Server to the client.

To configure Windows Firewall on all Windows XP clients to allow remote management follow these steps.

1. Navigate to Computer Configuration -> Administrative Templates -> Network -> Network Connections -> Windows Firewall -> Domain Profile
2. Enable “Allow inbound remote administration exception”.



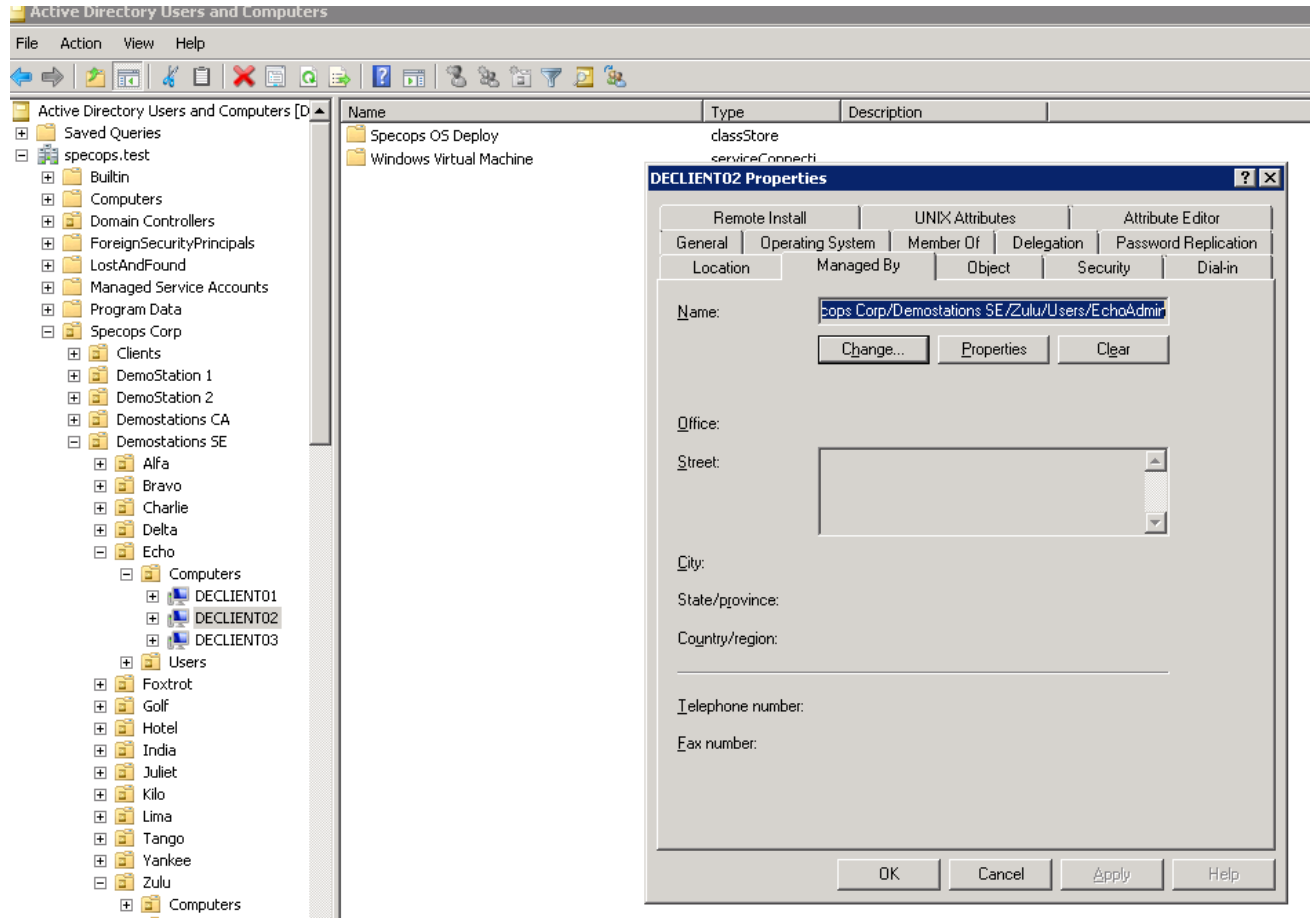
ICMP is automatically allowed when the Remote Admin exception rule is enabled, but it's also manually added it in the picture above.

Close GPMC and force a gpupdate on a client to verify that the SSP Service account is added to Local Administrators and the firewall has an exception for Remote Administration.

## 5.3 Controlling ownership of clients.

For a user to be able to request and deploy software to a computer, that user has to be designated manager of that client. This is to prevent users from ordering software to other clients.

The Specops Self Service Portal reads the ManagedBy Attribute on a computer to decide who the owner is. One client can only have one owner. Groups are not supported.



The ManagedBy attribute can be automatically updated by using Specops Deploy CSE granting the computer account permissions to update the attribute.

### 5.3.1 Configuring automatic client ownership

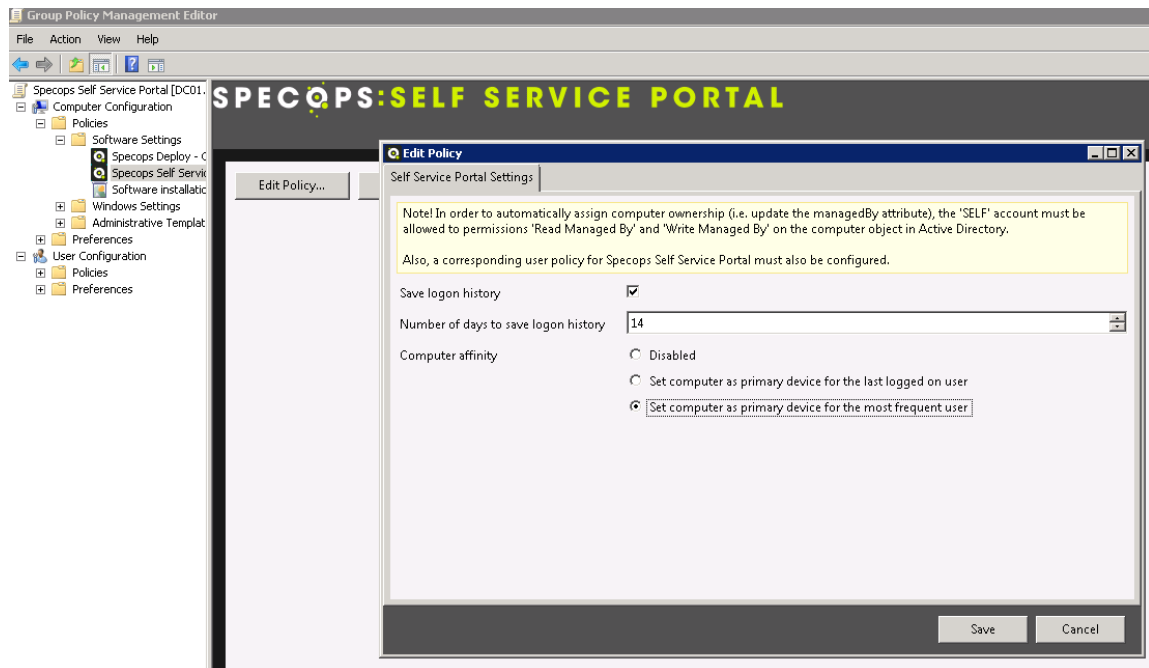
There are two new group policies that control how the owner is decided, and who can be owner of a computer.

## 5.3.1.1 Configuring how the owner is decided.

1. Open Group Policy Management Console on a computer with Specops Self Service Portal Admin Tools installed, and edit a policy that is being applied to client computers (security filtering is supported).
2. Navigate to : Computer Configuration -> Software Settings -> Specops Self Service Portal
3. Click Edit Policy...
4. Check “Enable logon history”
5. Configure the number of days to record logon history.

If there is no current owner, a new owner will be added at first occasion.

If there is a current owner, that owner will not be replaced until the configured settings are met.



6. Click Save

## 5.3.1.2 Configuring which users are allowed to be owner of computers.

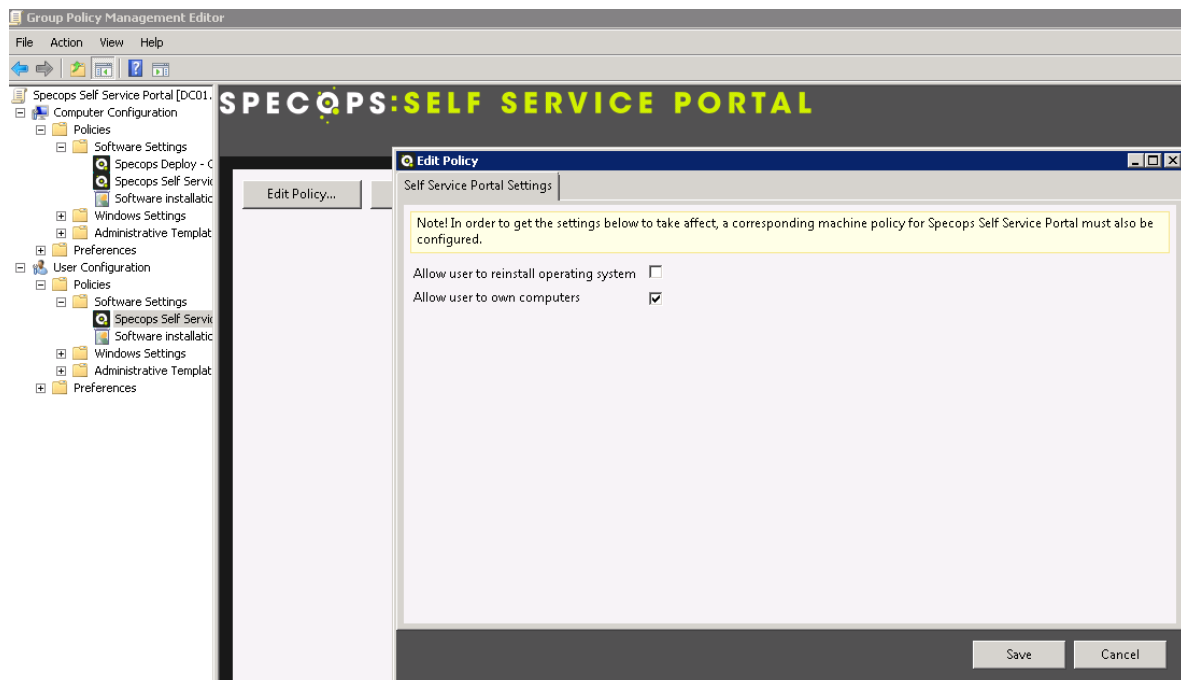
It's possible to control which users in the environment that can be assigned ownership of a computer. In most environments all users will be allowed to be owner, but there are some exceptions.

User Accounts who are regularly logging on to new clients could be added to an exception list. For example, an IT Staff member installing a new PC and logs on to that PC a few times performing configuration changes. That user will now be owner of that PC.

The end user is then not able to request additional applications from SSP until that user is the most frequent user of the PC and is granted ownership.

To configure if a user is allowed to be owner follow these steps.

1. Open Group Policy Management Console on a computer where Specops Self Service Portal Admin Tools are installed.
2. Open a Group Policy that is being applied to the users.
3. Navigate to : User Configuration -> Software Settings -> Specops Self Service Portal
4. Click Edit Policy...
5. Check : Allow user to own computers



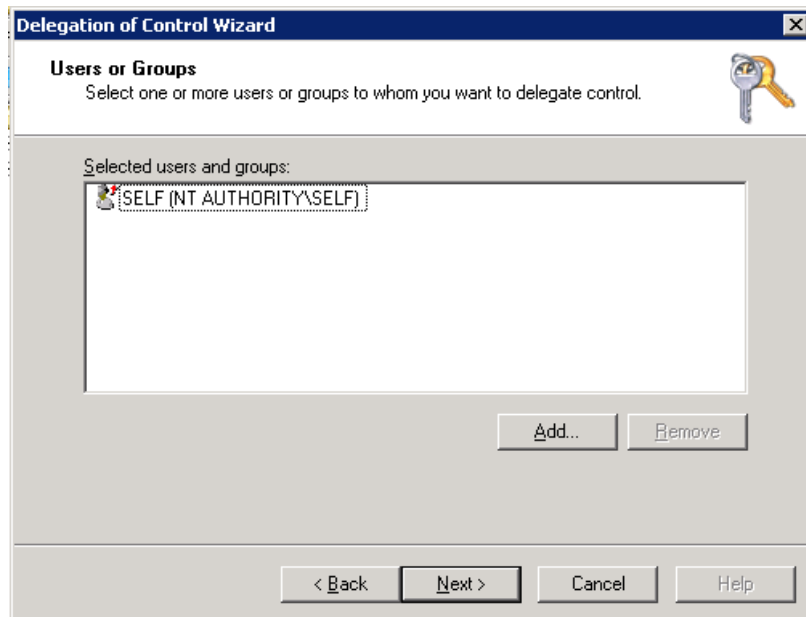
6. Click Save

## 5.3.2 Delegating permission to client's to update ManagedBy attribute.

The client PC is running a Client Side Extension (Specops Deploy CSE) to update the ManagedBy attribute in Active Directory. This process is executed by group policies in the system context and will use the computer account in Active Directory to update the attribute.

For the computer to be allowed to update the attribute delegated permission is required for the computer account (self). Follow these steps to delegate permissions.

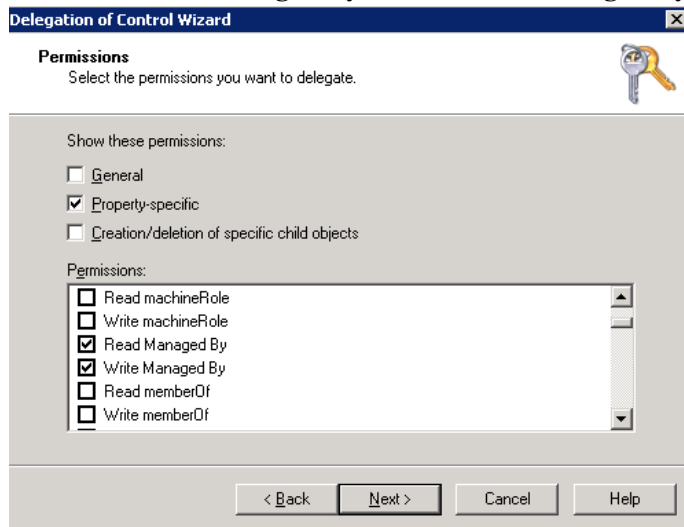
1. Open Active Directory Users and Computers
2. Navigate to the root OU of the domain clients.
3. Right click on the OU and choose “Delegate control...”
4. Click Next
5. Click Add and type “self”, then click “Check Name”



6. Click Next
7. Choose: Create a Custom task to delegate
8. Click Next
9. Choose: Only the following objects in the folder:
10. Enable Computer Object
11. Click Next
12. Choose : Property-Specific



## 13. Enable: “Read Managed By” and “Write Managed By”



## 14. Click Next

## 15. Click Finished

If Specops Deploy 4.6 is in use and the Specops Deploy 4.6 CSE is installed on the clients computers no further action is needed.

## 5.4 Allowing users to trigger a reinstall from SSP

To allow users to reinstall their PC from SSP, Specops Deploy / OS has to be installed in the environment. This function is not supported with any other deployment solutions.

To allow users to initiate a reinstall from Specops Self Service Portal,

1. Open Group Policy Management Console (GPMC) from a computer with Specops Self Service Admin Tools installed.
2. Navigate to User Configuration -> Software Settings -> Specops Self Service Portal
3. Click Enable
4. Click “Allow user to reinstall operating system”
5. Click Save

The Specops Self Service Portal Service Account requires permission to initiate a Specops Deploy OS reinstallation.

1. Add the SSP Service Account to domain security group “Domain Specops Deployment Servers” if it’s not part of the group already.

## 6 Specops Self Service Portal – Administration Guide

SSP is using three user roles and web pages.

Administrator: <http://server.name.com/SpecopsSelfServicePortal/Admin/>

Owner: <http://server.name.com/SpecopsSelfServicePortal/Owner/>

User: <http://server.name.com/SpecopsSelfServicePortal/User/>

Admin is where administrators define who and what services the users should be able to request.

Owner is where a request can be approved or denied.

User is where users will request services.

Users are grouped into Units. A unit can be a department, a country, a group of users, a project or any other grouping of users. A unit can contain multiple Users and/or Groups. A unit always has at least one person or group of users who can approve requests for that unit.

A user can be part of one or multiple units, giving the user permission to request applications and services. Administrators can configure the services to require approval or to be installed without approval for various units.

## 6.1.1 Creating units

1. Open the administration URL in a Web Browser :  
<http://server.name.com/SpecopsSelfServicePortal/Admin/>
2. Click Units
3. Click New to create a New Unit
4. Enter a name: for example “Everyone” or “All Users”
5. Enter a description
6. Add an Owner

An owner is one or multiple persons who will be notified if a user of that unit is requesting something that needs approval.

For a unit defining a Project or Department, it's usually the Project Leader or Manager who will be owner.

While for the “All Users” unit, it might be Helpdesk.

7. Add members to the Unit.

A member is a person who can request applications for that unit. It can be one or multiple users or groups.

The screenshot shows a web-based configuration window titled "Unit". At the top, there is a "Name" text box containing "Everyone" and a "Description" text box containing "All Domain Users". Below these are two columns: "Owners" and "Members". The "Owners" column contains a list box with "Helpdesk" and buttons for "Add" and "Delete". The "Members" column contains a list box with "Domain Users" and buttons for "Add" and "Delete". At the bottom right of the window are "OK" and "Cancel" buttons.

8. Click OK.
9. Repeat and add more units if needed.

## 6.1.2 Creating Services or applications

The main purpose of Specops Self Service Portal is to handle applications, but it's also supported and possible to add other services.

A service is something that is controlled by membership in a security group and that a user can request through the Self Service Portal.

To create a new application and connect it to a unit.

1. In "Applications" click New
2. Enter a name of the service, for example "Microsoft Office 2007"
3. Enter a description.
4. Choose a Security Group that's controlling this service.
5. Choose installation Type to a computer account or user account.  
If computer is selected, only users with ownership of one or more computers will be able to request the service. The computer account the user choose will be added to the security group.  
If user is selected, that user account will be added to the security group.
6. Click New to add the number of available licenses.
7. Enter details (Name and Licenses are required).
8. Click Ok
9. Click New to add license distribution and control who can request the service.
10. Choose the License.
11. Choose which unit this applies to.
12. Enter how many of the total number of licenses that unit is allowed to use.
13. Define if this unit requires approval to use the service.

Name	Version	License Key	Cost per License	Purchase Date	Expiration Date	Number of Licenses	Distributed	In Use	Remaining
Office 2007						5	5	0	0

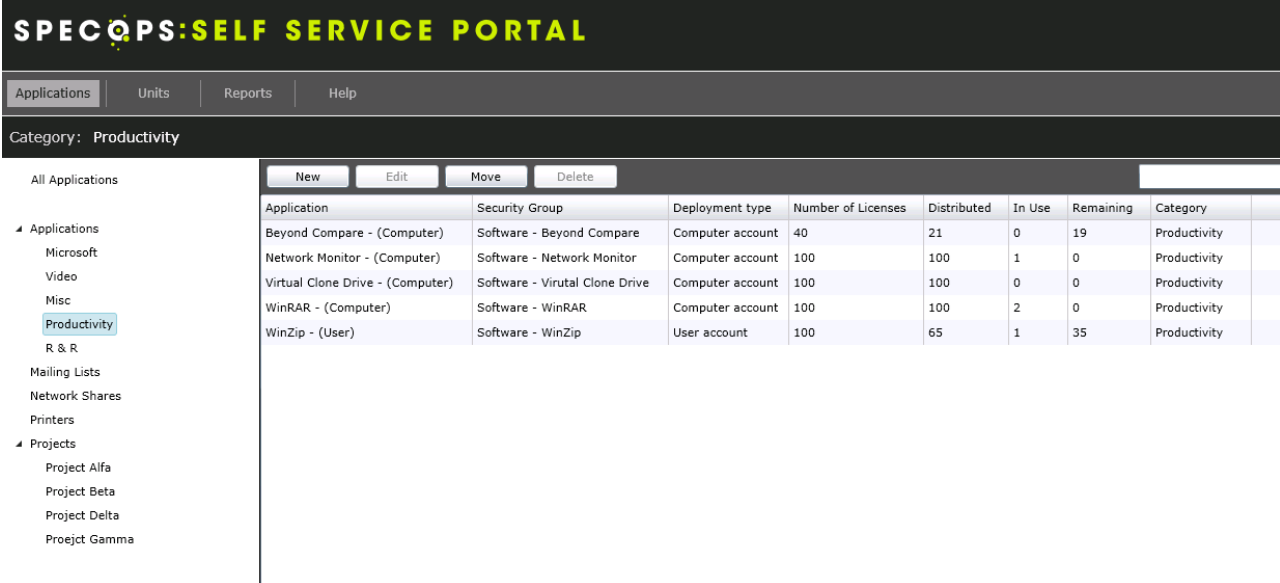
  

License	Unit	Requires Approval	Number of Licenses	In Use
Office 2007	Everyone		5	0

14. Click Ok

Using categories makes navigation easier for the users.

An example of how it could look like;



The screenshot displays the SPECOPS SELF SERVICE PORTAL interface. At the top, there is a navigation menu with 'Applications', 'Units', 'Reports', and 'Help'. Below this, the current category is set to 'Productivity'. A sidebar on the left lists various application categories, with 'Productivity' selected. The main area features a table with columns for Application, Security Group, Deployment type, Number of Licenses, Distributed, In Use, Remaining, and Category. The table lists five applications: Beyond Compare, Network Monitor, Virtual Clone Drive, WinRAR, and WinZip.

Application	Security Group	Deployment type	Number of Licenses	Distributed	In Use	Remaining	Category
Beyond Compare - (Computer)	Software - Beyond Compare	Computer account	40	21	0	19	Productivity
Network Monitor - (Computer)	Software - Network Monitor	Computer account	100	100	1	0	Productivity
Virtual Clone Drive - (Computer)	Software - Virtual Clone Drive	Computer account	100	100	0	0	Productivity
WinRAR - (Computer)	Software - WinRAR	Computer account	100	100	2	0	Productivity
WinZip - (User)	Software - WinZip	User account	100	65	1	35	Productivity

## 6.2 Administrative Rights

To receive administrative rights to the Specops Self Service Portal, add the user to Local Administrators group on the server or add the user to the local group “Specops Self Service License Administrators”.

## 6.3 Deployments

The Specops Self Service Portal is not performing any deployments by itself. All deployments are handled by the software deployment solution in place. SSP is only handling group membership, all other criteria have to be controlled and verified in some other way.

SSP does support initiating a group policy refresh on a remote computer when it has been approved for a service which in turn will initiate a Specops Deploy software installation if Specops Deploy is being used in the environment.

## 7 Verification

### 7.1.1 Approval and Revocation

Navigate to the three different web pages and add services, then request and approve them.

Verify that the user can choose the right computer(s) to request services too, and choose to reinstall the operating system if that feature is enabled and the user has access.

Verify that the user or computer is added to or removed from the correct security groups depending if it's an approval or revocation.

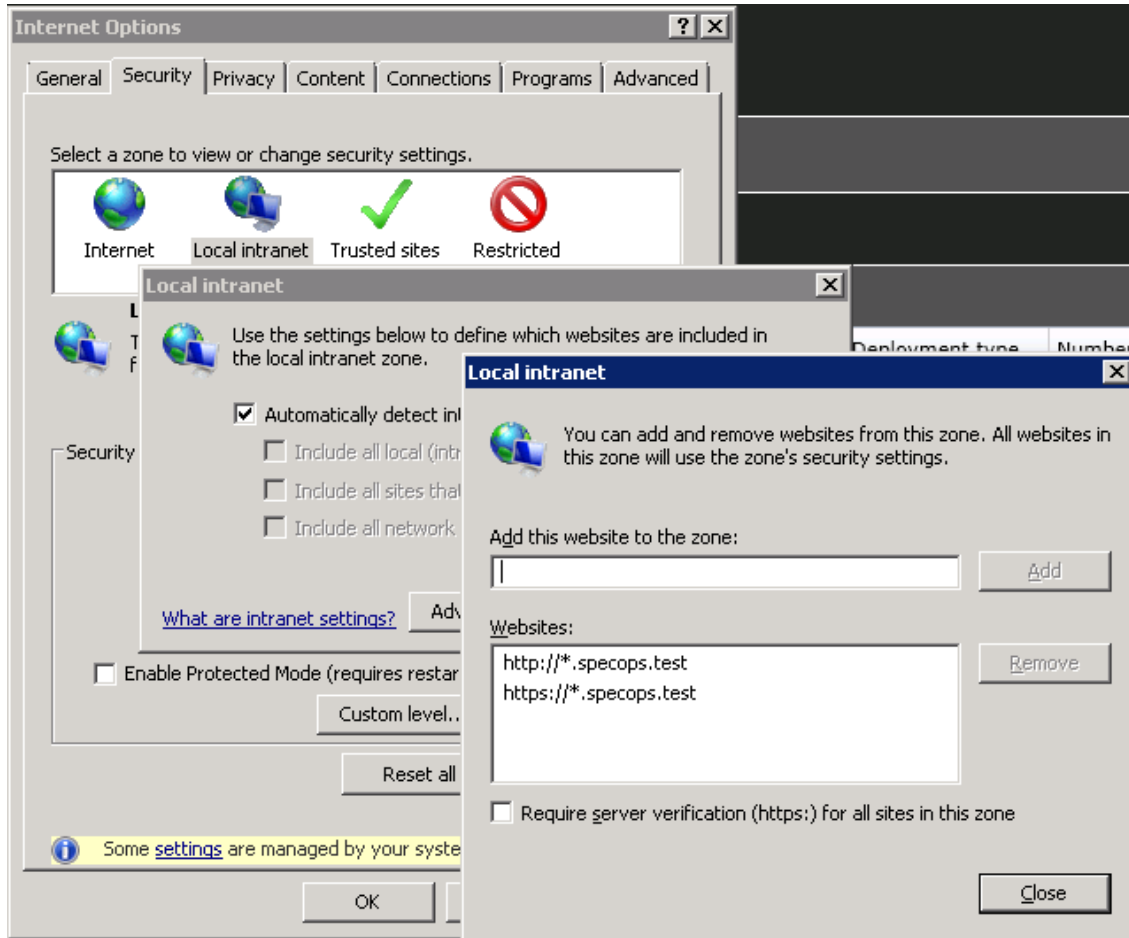
Administrator: <http://server.name.com/SpecopsSelfServicePortal/Admin/>

Owner: <http://server.name.com/SpecopsSelfServicePortal/Owner/>

User: <http://server.name.com/SpecopsSelfServicePortal/User/>

## 7.1.2 Single Sign On

Authentication to the portal is done with windows integrated authentication. It's required that the server is identified as an intranet server for this to work. Or the user will be prompted for username and password.



This can be configured through Microsoft Group Policies.

*Note: If Single Sign On is not used, the user will be prompted for username and password which will use "Basic Authentication" and send the user information over HTTP (clear text).*



## 8 Customizations

### 8.1.1 Branding

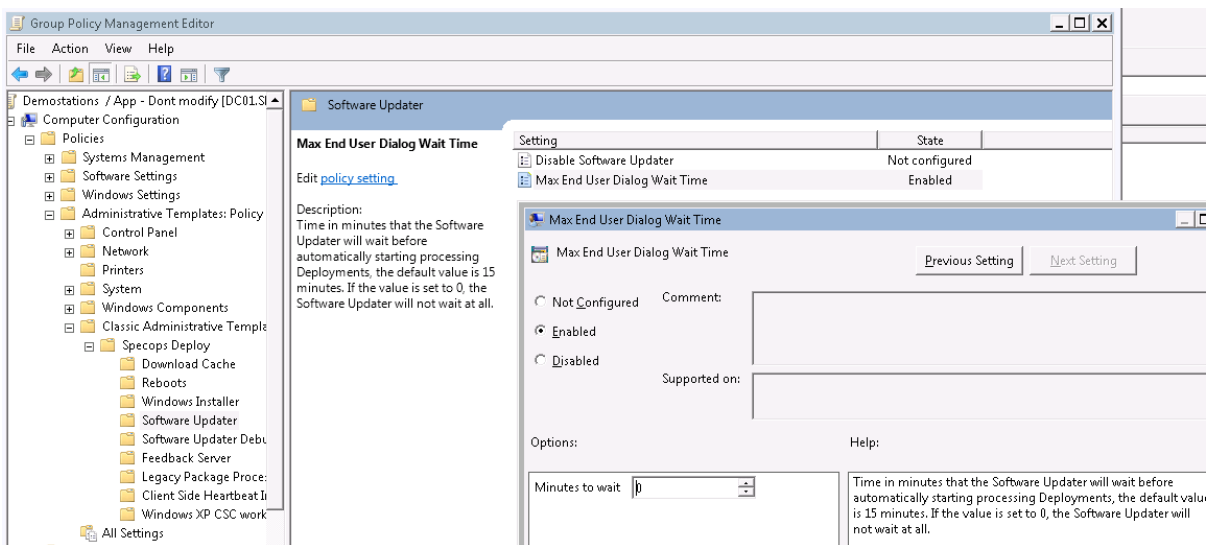
To change the color schema and logo of the Self Service Portal, navigate to `C:\Program Files\Specopssoft\Specops Self Service Portal\Web\App_Themes\Default` and modify the style sheet and replace the logo image with a corporate specific logo.

### 8.1.2 Reducing wait time for Specops Deploy

By default, Specops Deploy will wait 15 minutes before starting an application installation if a user is logged on and if it's not forced by a user.

To give a better user experience, it's recommended to change this setting to 0 minutes.

Open the Group Policy Management Editor and change the “Max End User Dialog Wait Time” to 0. This may require importing the `SpecopsDeploy.adm` file first.



## 9 Support and Troubleshooting

### 9.1 Event Log

The Windows Event Log contains all Specops Self Service Portal related information.

### 9.2 Debug Logging

For enabling Debug Logging set Debug = 1 in these regkeys

HKEY\_LOCAL\_MACHINE\SOFTWARE\Specopssoft\Specops Self Service Portal\Web

HKEY\_LOCAL\_MACHINE\SOFTWARE\Specopssoft\Specops Self Service Portal\Administration

### 9.3 Online Resources

Please visit the Specops Forum for support and help with troubleshooting at:

<http://forum.specopssoft.com>

For Tips and Tricks in Relation to Specops Products visit the blog at

<http://blogs.specopssoft.com>

For support and help with troubleshooting go to:

<http://www.specopssoft.com/about-specops/contact>

Urgent requests for support may be submitted to:

[http://www.specopssoft.com/resources/support\\_1](http://www.specopssoft.com/resources/support_1)

Feedback on documentation can be sent to:

[Specops-documentation@specopssoft.com](mailto:Specops-documentation@specopssoft.com)