E-SSOM

CONFIGURATION GUIDE

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Contents

1. Introduction **1**

2. Admin Console Overview **2**

3. Application Definitions **3**

3.1. Overview 3
3.2. Configuring 5

4. Application Version Types **6**

4.1. Win32 / x64 7
4.1.1. Win32 Window Layout Event 8
4.2. HTML - Internet Explorer / FireFox 10
4.2.1. Web Page Event 11
4.2.2. Web Layout Event 13
4.3. CLI / Telnet 16
4.3.1. CLI Event 17
4.4. HLLAPI Telnet 18
4.4.1. HLLAPI Event 19
4.5. Java 20
4.5.1. Java Event 21
4.5.2. Java Monitor Installation 23

5. Scripts 25

5.1. Overview 25
5.2. Configuring 26

6. Application Policies 27

6.1. Overview 27
6.2. Configuring 27

7. User Policies 30

7.1. Overview 30
7.2. Configuring 30
7.3. Citrix 33

8. Password Policies 34

8.1. Overview 34
8.2. Configuring 34

9. Client Service Settings 36

10. Fast User Switching 36

10.1. Requirements 37
10.2. Configuration 37
10.3. Follow Me 38

11. Authentication Management 38

11.1. Requirements 38
11.2. Smartcard Policies 39
11.3. Managing Smartcard Assignments 40

12. Reporting 40

12.1. Introduction 40
12.2. Process Monitoring 40

13. E-SSOM AppInit Client 41

14. E-SSOM Anywhere 42

14.1. Requirements 42
14.2. IIS 6 Configuration 42
14.3. IIS 7 Configuration 46

15. High availability / Fail Over 47

15.1. User Client Offline Mode 47
15.2. Multiple Central Services 48
15.3. MSSQL Replication Configuration 49
15.3.1. Publication 49
15.3.2. Subscription 55

16. Examples **62**

16.1. Importing and assigning an application to a user 62
16.2. Creating a win32 application definition using the default scripts 63

17. E-SSOM Error Codes **67**

18. Index **69**

1. Introduction

This document describes how to configure E-SSOM so that a user can automatically log on to one or more applications. This document does not describe how to install the product. A step by step guide discussing how to install the product can be found in the 'E-SSOM Installation Guide'.

For a step by step guide discussing how to assign a pre-configured application to a group of users, please refer to the 'Importing and Assigning an Application to a User' chapter.

Other E-SSOM Guides

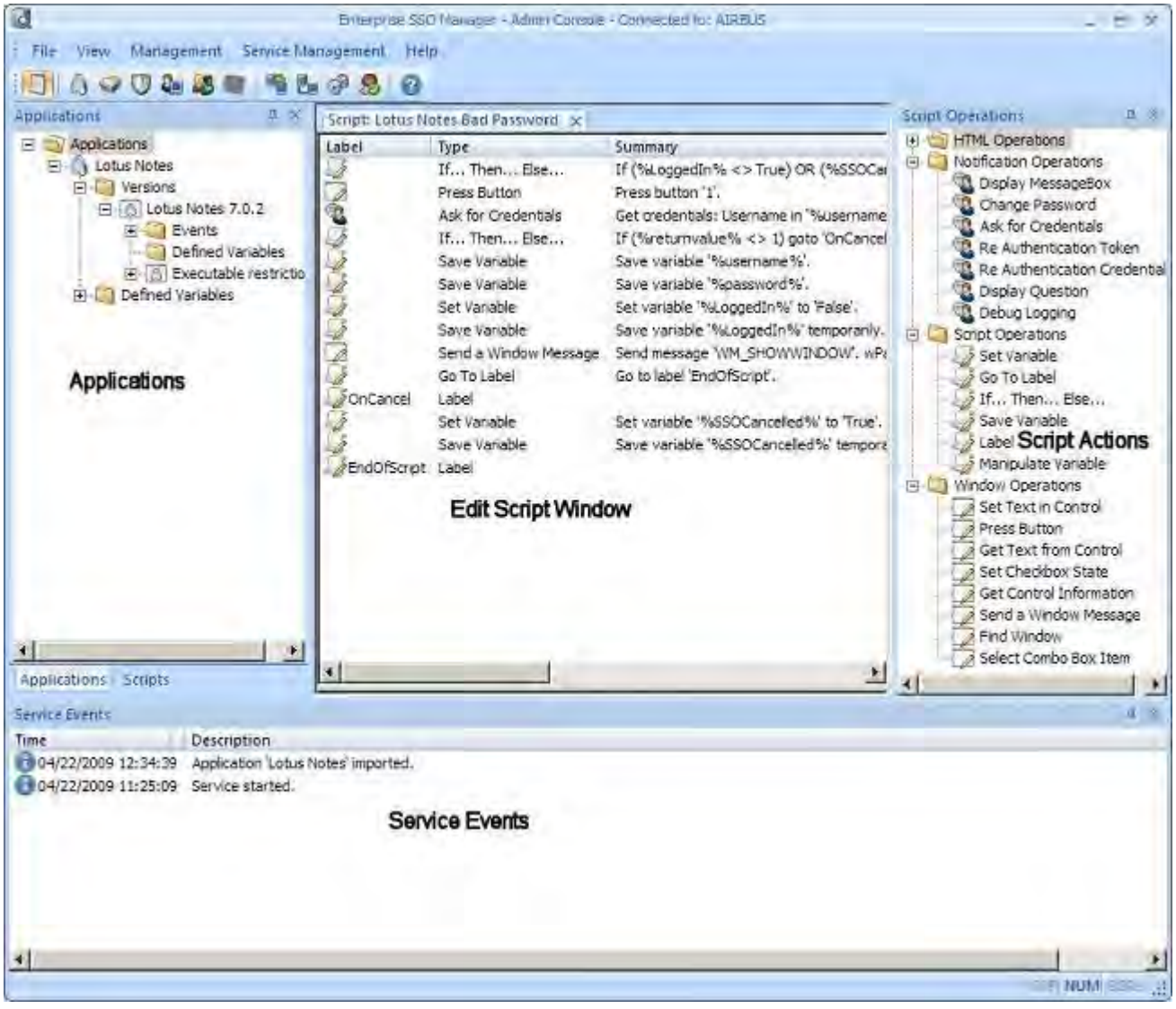
- Installation Guide
- Scripting Guide
- Deployment Guide

2. Admin Console Overview

The E-SSOM Admin Console is used to manage the E-SSOM Central Service.

The Admin Console can among other things be used to:

- Create new applications and scripts to perform automatic logon.
- Assign applications to users and/or groups
- Restrict what users can do with the E-SSOM Client Software
- Install/Update and delete E-SSOM Central Services.



3. Application Definitions

3.1. Overview

Application Definitions in E-SSOM are used to instruct the E-SSOM Client Software how to log on to a specific application.

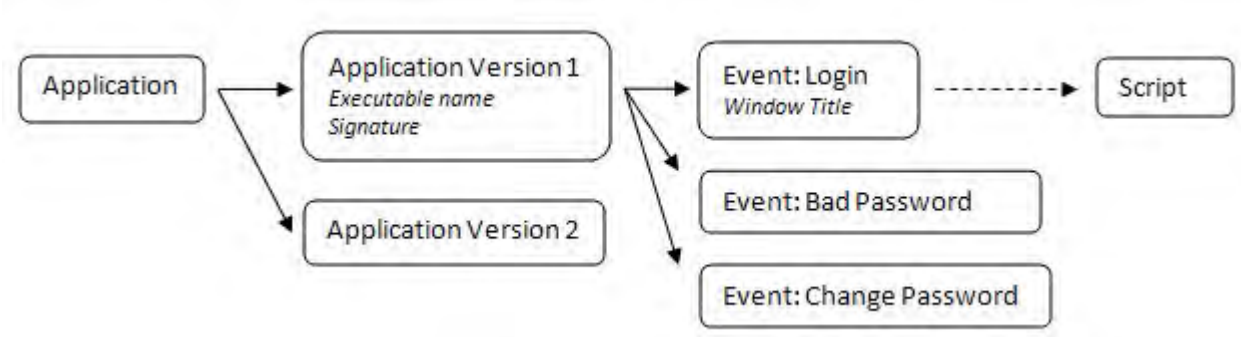
Detection

When a window is displayed in an application, the E-SSOM Hook checks if it can find an application definition that matches the running application. If the hook finds a match, it continues to check if the displayed window matches a window described in the definition's configured events. If the hook finds a match, the user data is loaded and a script is executed. A script can be used to perform various actions such as: logging on, changing a password or handling bad passwords.

1. An application is started.
2. The hook loads the application definitions that match. (Several criteria can be defined including the name of the executable and a signature.)
3. If the hook does not find a fitting definition, it will stop looking for events until the next time the application is started.
4. A window is displayed.
5. The hook checks all application definitions to see if a configured event matches the displayed window. (Several criteria can be defined including window title, class, text and controls)
6. The user data is loaded from the database. (Only the user data for the logged on user and the application containing the event are loaded.)
7. The script is executed.
8. If necessary, variables are written to the database.
9. The event is logged to the database.

Application Definition

The entire E-SSOM configuration for an application is stored in an application definition. This definition contains all of the information necessary to log on automatically to an application. The definition describes all the events that must be handled. (ie: 'login', 'bad password' and 'change password', etc.). It tells the E-SSOM Hook which script should be executed when a window is displayed.



Application Version

Since different versions of the same application can use different logon procedures and windows, E-SSOM has been designed so that i can support different configuration settings for each version. On the other hand, logon credentials could be unchanged for different versions of the same application.

New versions of applications can have changes to the user interface or even a completely new interface. If a new version of such an application is installed, it is possible that the configured application definition will no longer function with the new version. If a new application definition is created for this new version, users will have to re-enter their credentials. This is because the stored credentials are linked to the original application definition. It is possible to create a new 'application version' in the application definition containing its own criteria and events. This way the users can easily migrate to the new version without having to reenter their credentials.

Events

Events describe when a script must be executed. They also describe how the event is detected. Scripts can be executed when the following events occur in an application:

- When a window is displayed in a win32/x64 application
- When a specific web page is loaded
- When specific text is displayed in CLI/HLLAPI/Telnet applications
- When a specific window in a java application is displayed

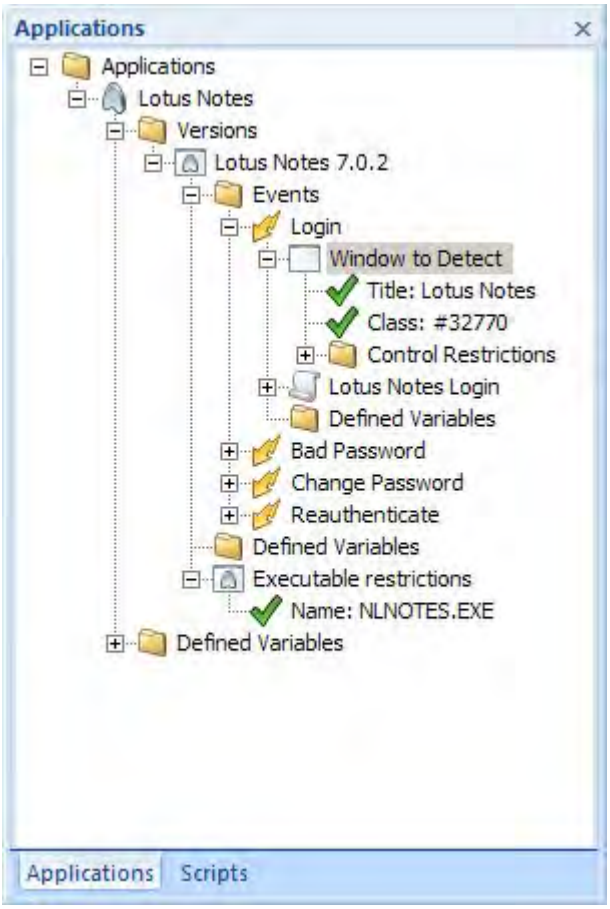
Events may be configured so that they are triggered when the user logs of during fast user switching. The scripts that are ran during log off can be used to log off the application, close the application or perform other cleanup actions.

When a new application definition is created in E-SSOM, three events are created by default:

- *Login:* A login window or page is displayed in the application. When this event occurs, the E-SSOM Client must enter the stored credentials in the specific window or ask the user to enter those credentials.
- *Bad Password:* A bad password wndow or page is displayed in an application. When this event occurs, the E-SSOM Client must tell the user that their stored credentials are incorrect and then ask the user to re-enter their credentials.
- *Change Password:* The application requests that the user changes his or her password. When this event occurs, the E-SSOM Client must display the 'Change Password' dialog which allows the user to change his or her password. It is also possible to automate this procedure by generating a random password.

3.2. Configuring

Application definitions can be created and edited using the Admin Console. The easiest way to manage application definitions is by using the applications tree:



Creating a new application definition
Right click in the applications tree and select 'Add Application...' from the menu.

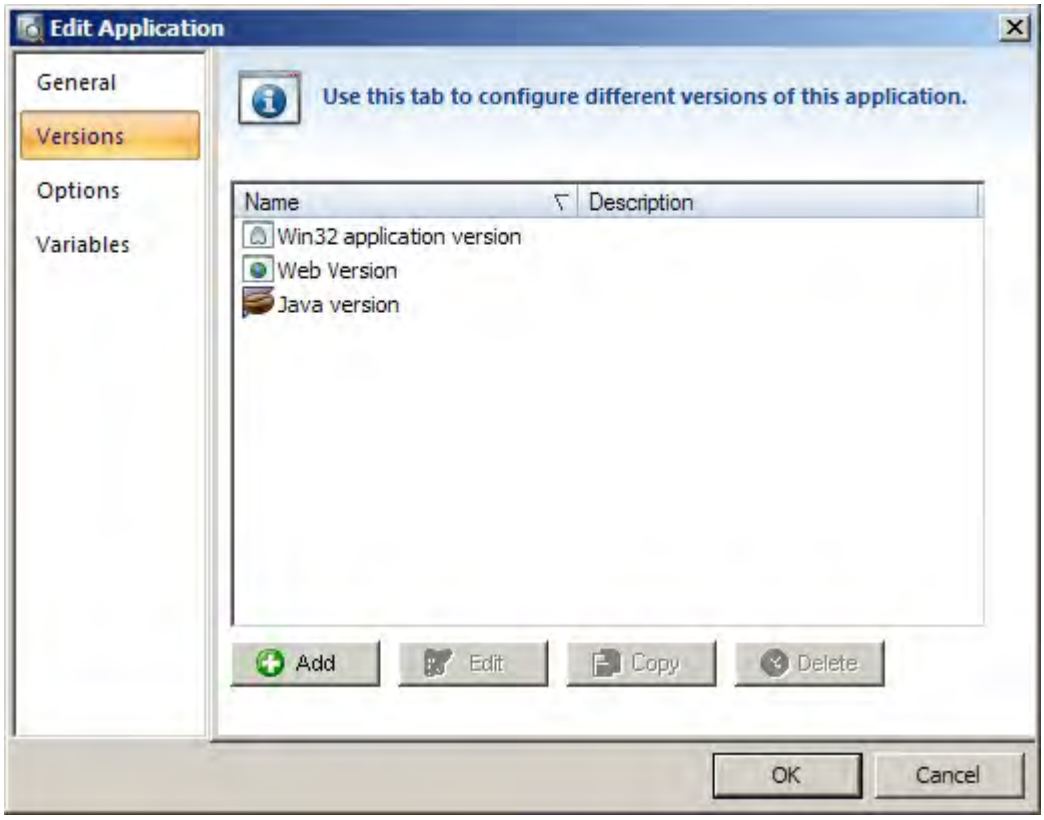
Editing an existing application definition
Double click on the item in the tree that you want to edit.

Importing and Exporting
Application definitions can be imported and exported. E-SSOM is shipped with several pre-configured application definitions that can be imported. These application definitions can be found by default at: 'C:\Program Files\Tools4ever\SSO\Admin Console\Applications'.

4. Application Version Types

E-SSOM support several different application version types. This chapter describes the different application types and how they can be configured.

When an application definition is created, one or more application versions can be added in the 'versions' tab:

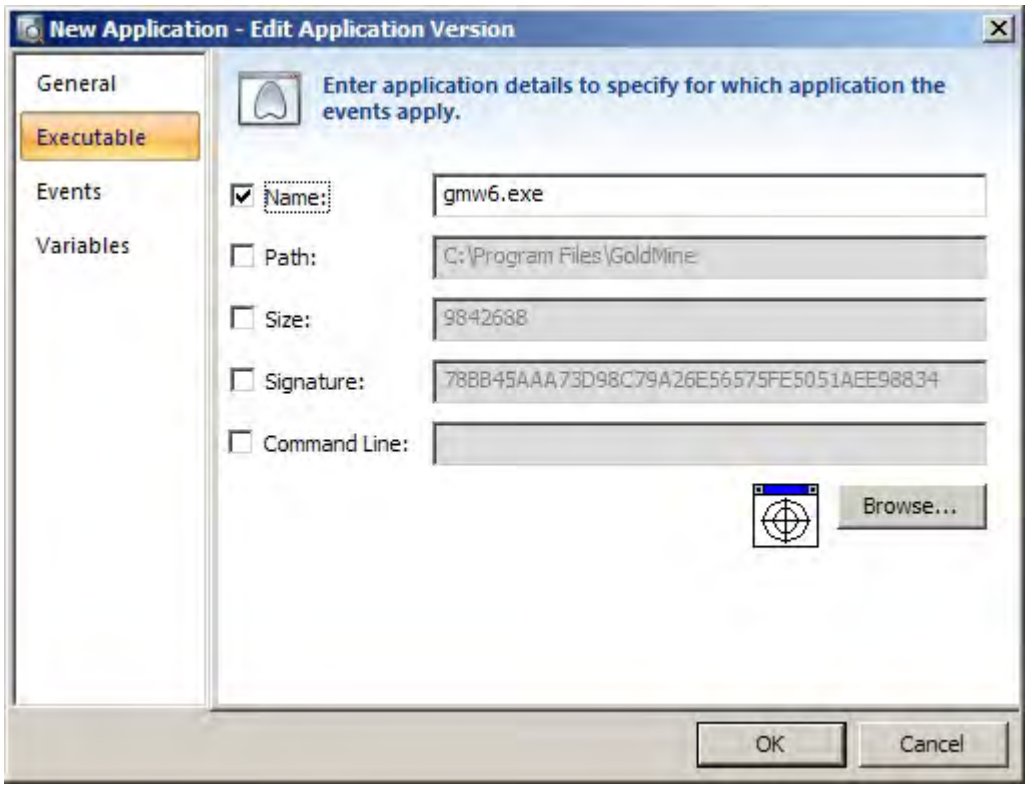


Currently there are five different application version types that are described in this chapter. These types include 'normal' applications, web applications, CLI/Telnet and Java Applications. Click on 'Add' to add a new application version.

Please note: An application definition can contain multiple different application types. This makes it possible to create an application definition for an application that consists of for instance an win32 application and a web interface to which users log in using the same credentials.

4.1. Win32 / x64

A Win32 / x64 application version type is a 'normal' Windows application.

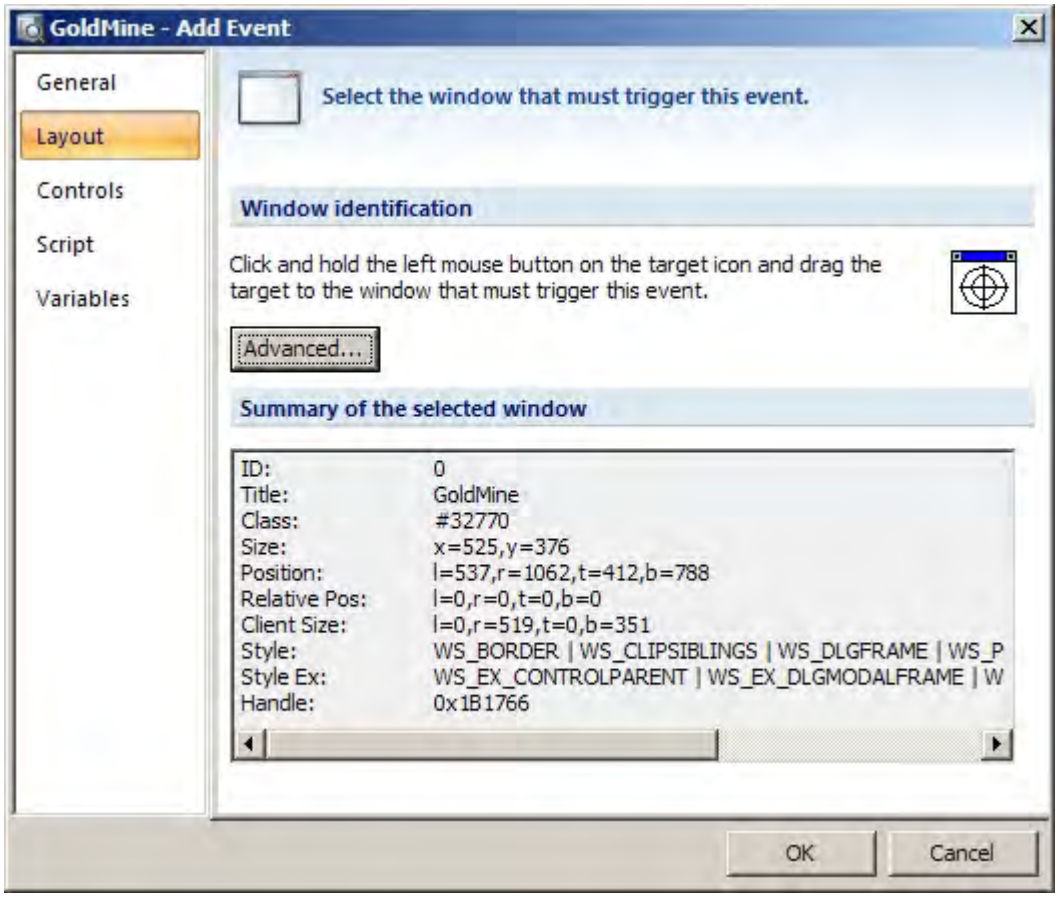


The application can be detected using several restrictions. By default only the name of the executable is used to identify an application.

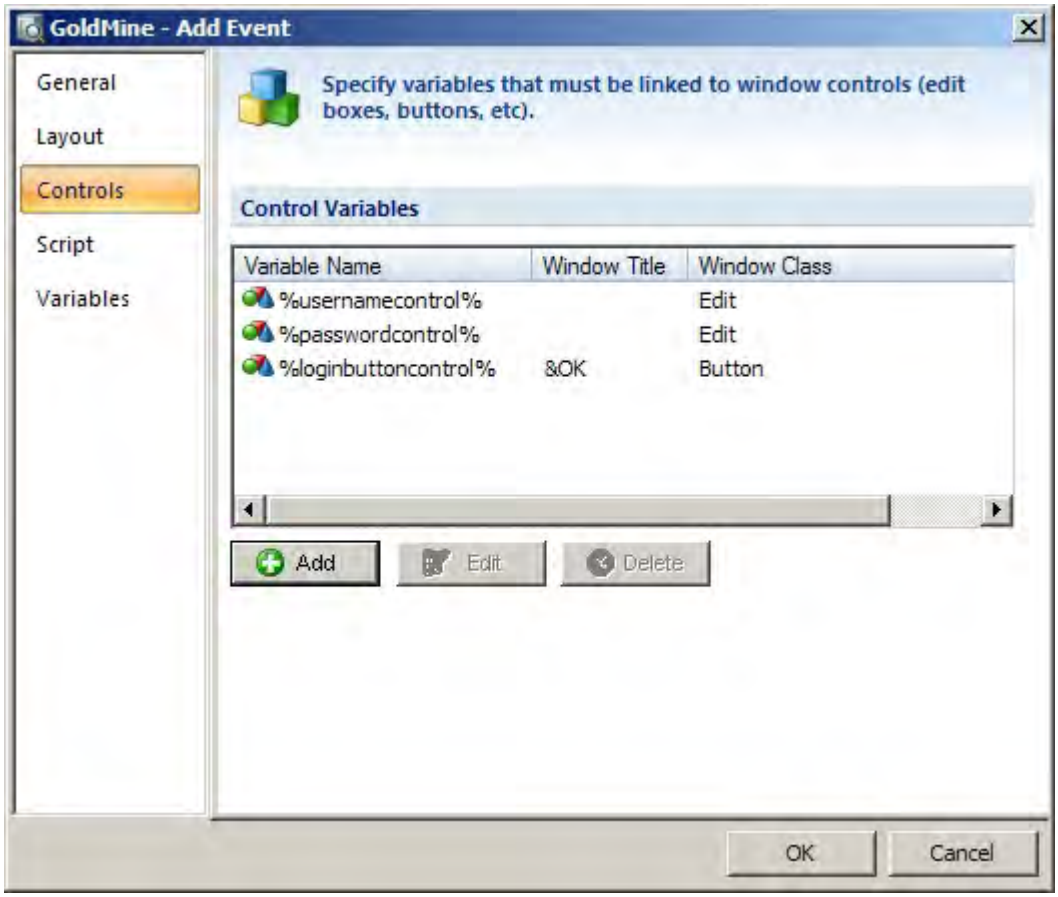
Please note: A detailed step by step guide on how to configure a Win32 application can be found in the examples chapter of this document. The chapter is called 'Creating a win32 application definition using the default scripts'.

4.1.1. Win32 Window Layout Event

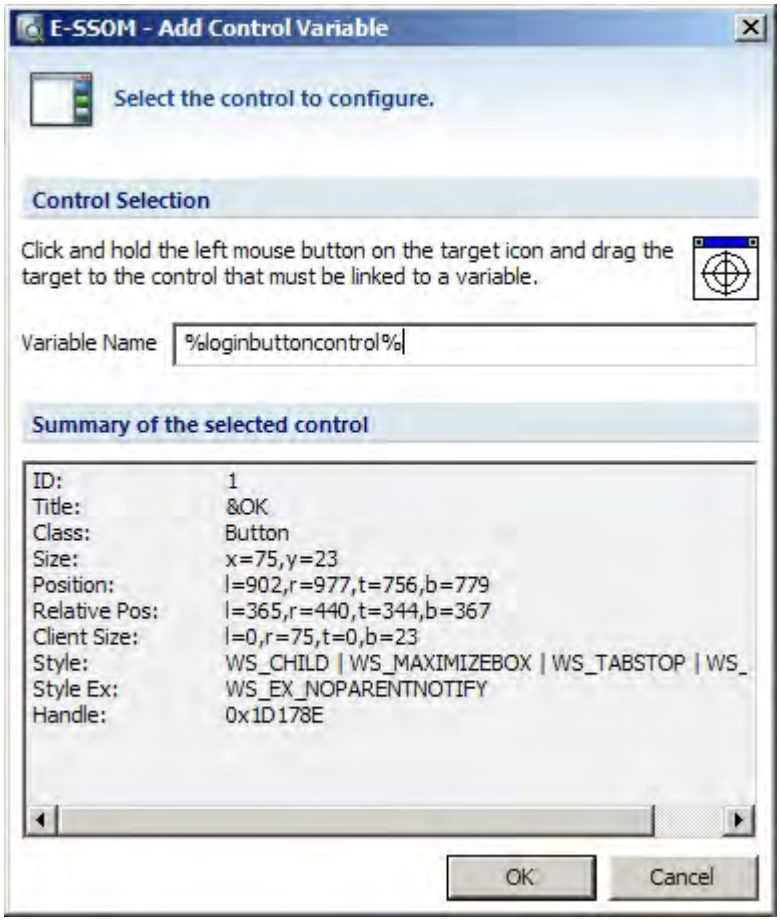
An event in a Win32 application is triggered when a specific window is displayed. To configure an event, click and hold the target icon in the 'Layout' tab of the 'Edit Event' dialog and drag it to the window of the application that must trigger this event.



The 'Controls' tab can be used to select controls so that they can be used in the script that is executed when this event is triggered.



Click on 'Add' to add a control to the list.



Click and hold the target icon and drag it to the control that must be configured and enter the name of the variable. This variable can be used to identify the control in the script that is executed by this event.

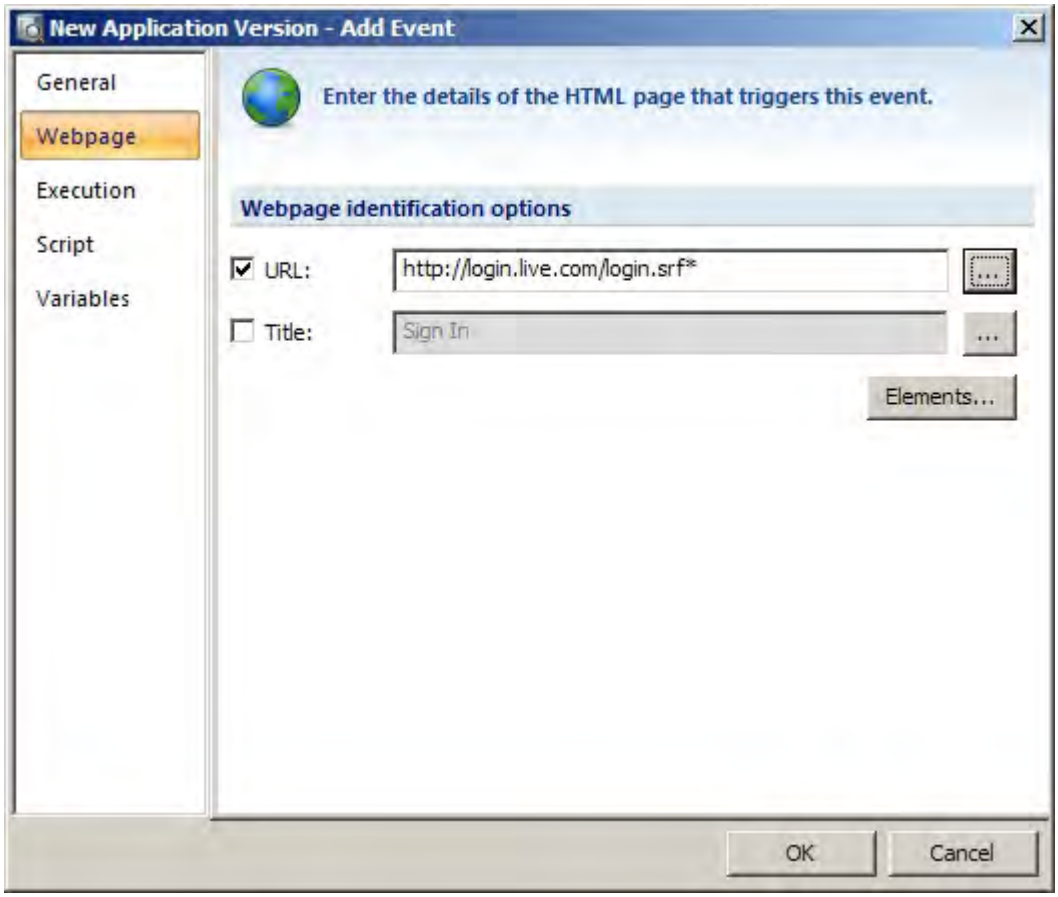
Please note that the control must be inside the window that is configured in the 'Layout' tab.

4.2. HTML - Internet Explorer / FireFox

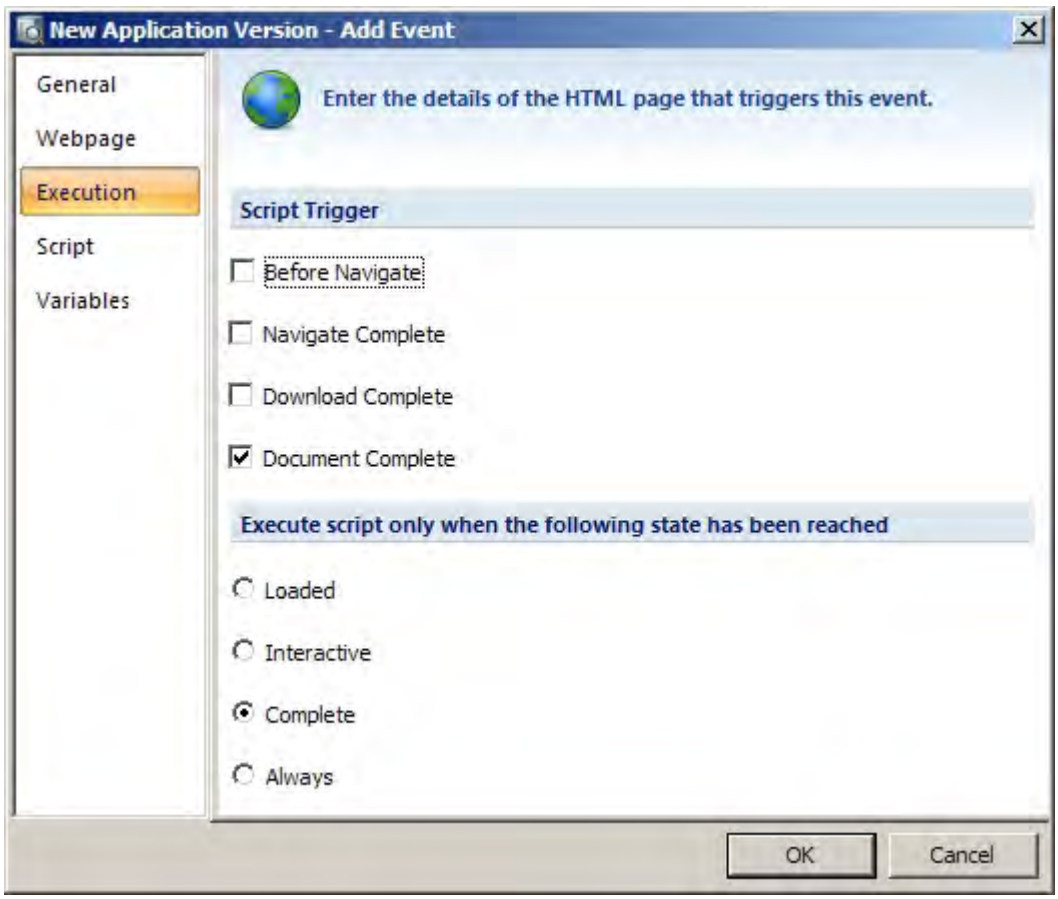
A 'HTML - Internet Explorer' application version type is used to perform Single Sign On on web sites that are loaded using Microsoft Internet Explorer or FireFox.

4.2.1. Web Page Event

A web page event is triggered when web page with a specific address is loaded. To configure a web page event, enter the address of the webpage on which the event must trigger. Click on the browse button (The ... button) to navigate to a page for the correct address.

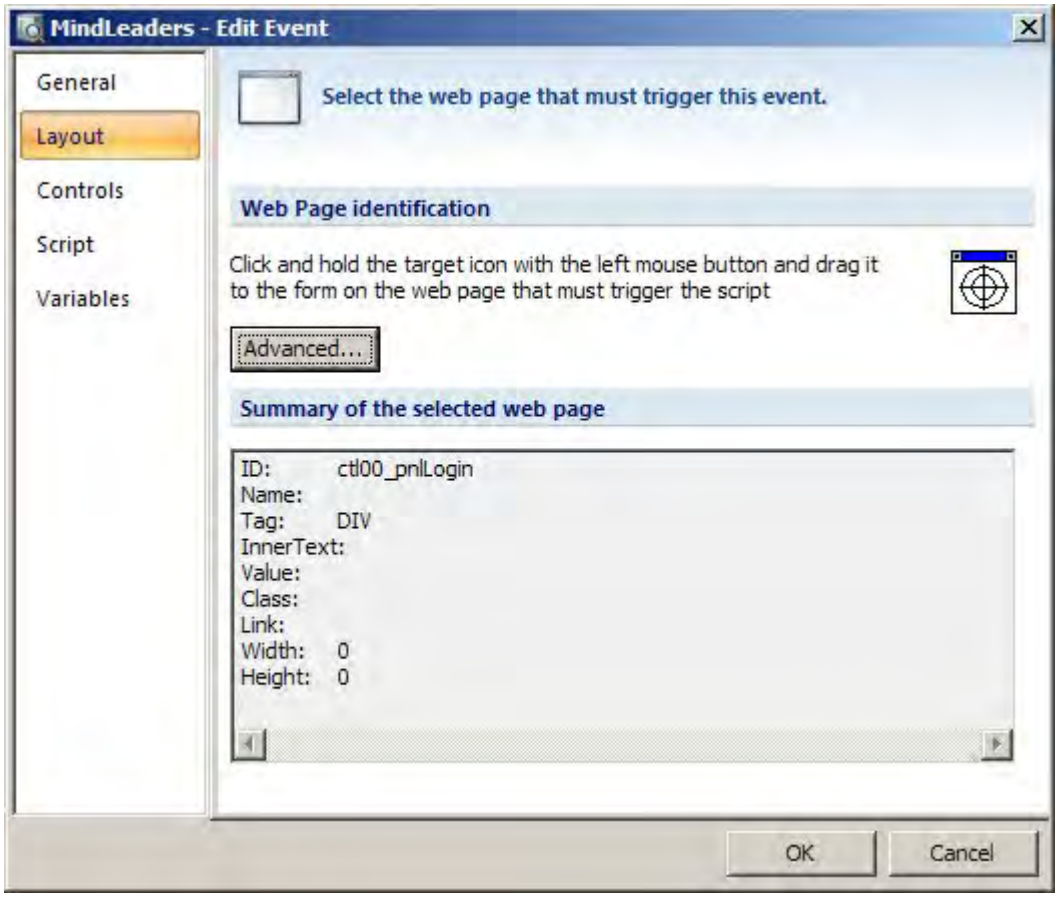


When a web page is loaded, it passes through several different stages. E-SSOM can be configured to trigger on one or more of these stages in the 'Execution' tab. In general scripts that want to get credentials from the 'POST' data must be triggered in the 'Before Navigate' event. Scripts that want to enter logon data must be executed in the 'Document Complete' event.

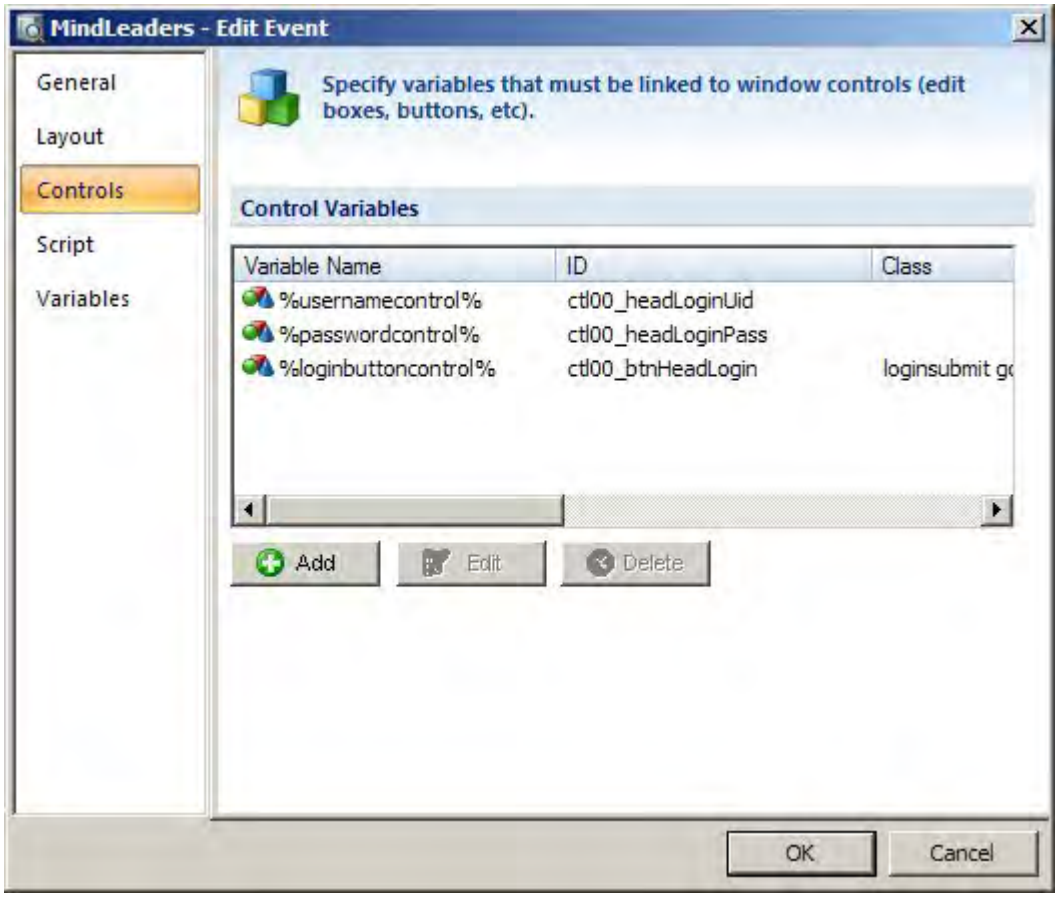


4.2.2. Web Layout Event

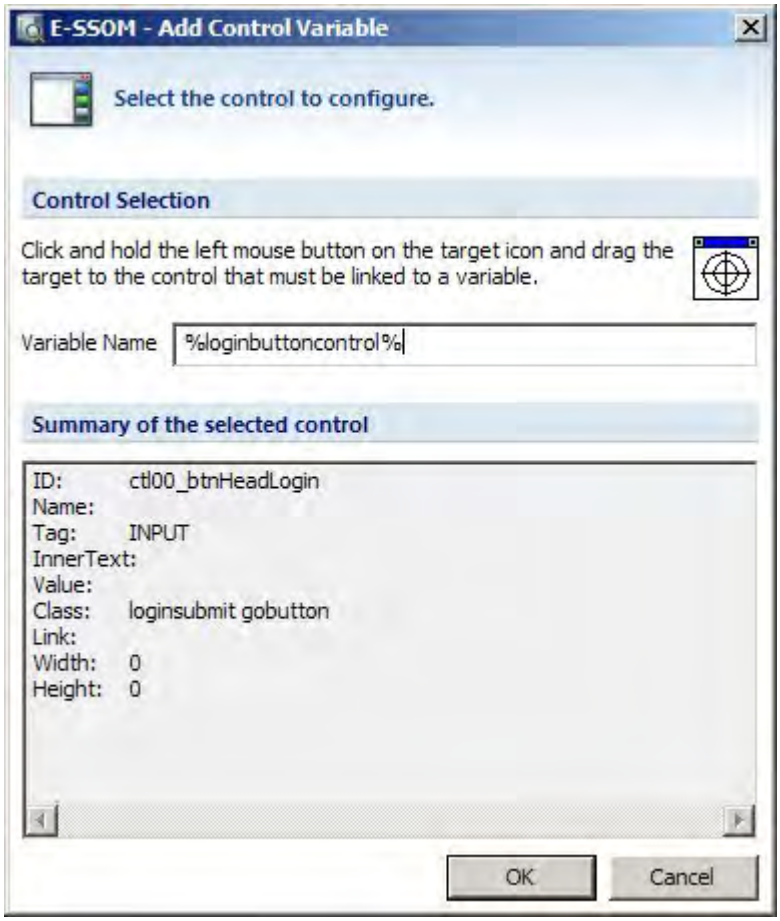
A Web Layout event is triggered when a specific layout of a webpage is detected. To configure the event, click and hold the target icon in the 'Layout' tab of the 'Edit Event' dialog and drag it to the portion of a webpage that must trigger this event.



The 'Controls' tab can be used to select controls so that they can be used in the script that is executed when this event is triggered.



Click on 'Add' to add a control to the list.

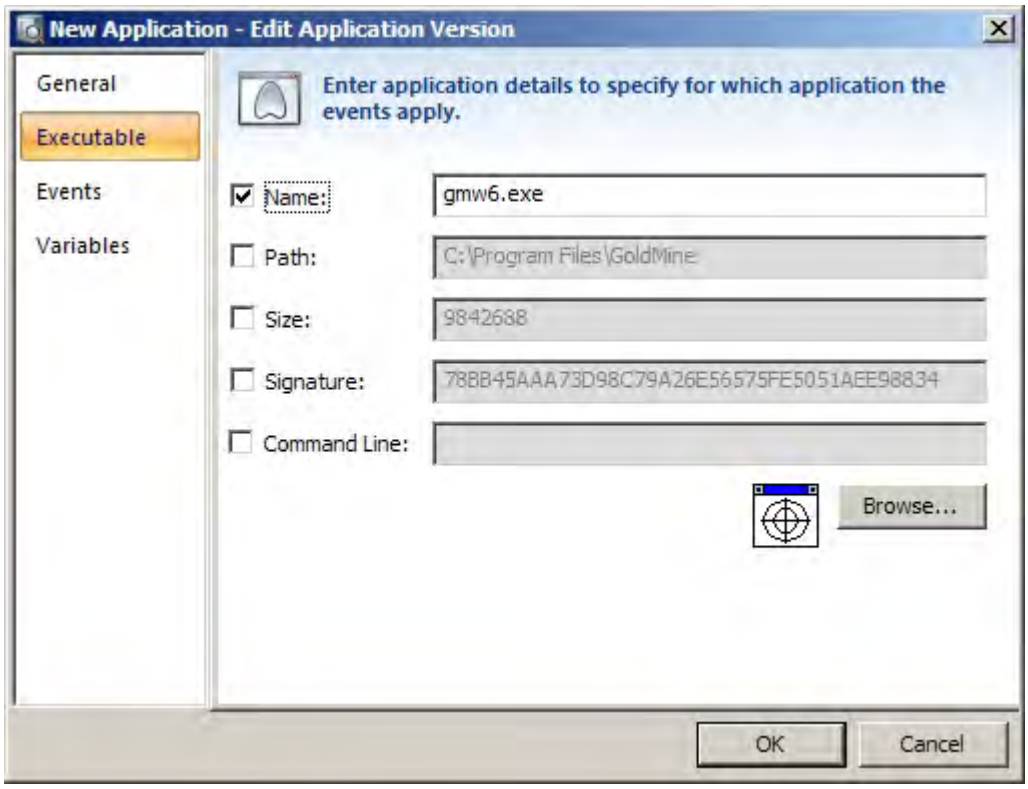


Click and hold the target icon and drag it to the control that must be configured and enter the name of the variable. This variable can be used to identify the control in the script that is executed by this event.

Please note that the control must be inside the part of the webpage that is configured in the 'Layout' tab.

4.3. CLI / Telnet

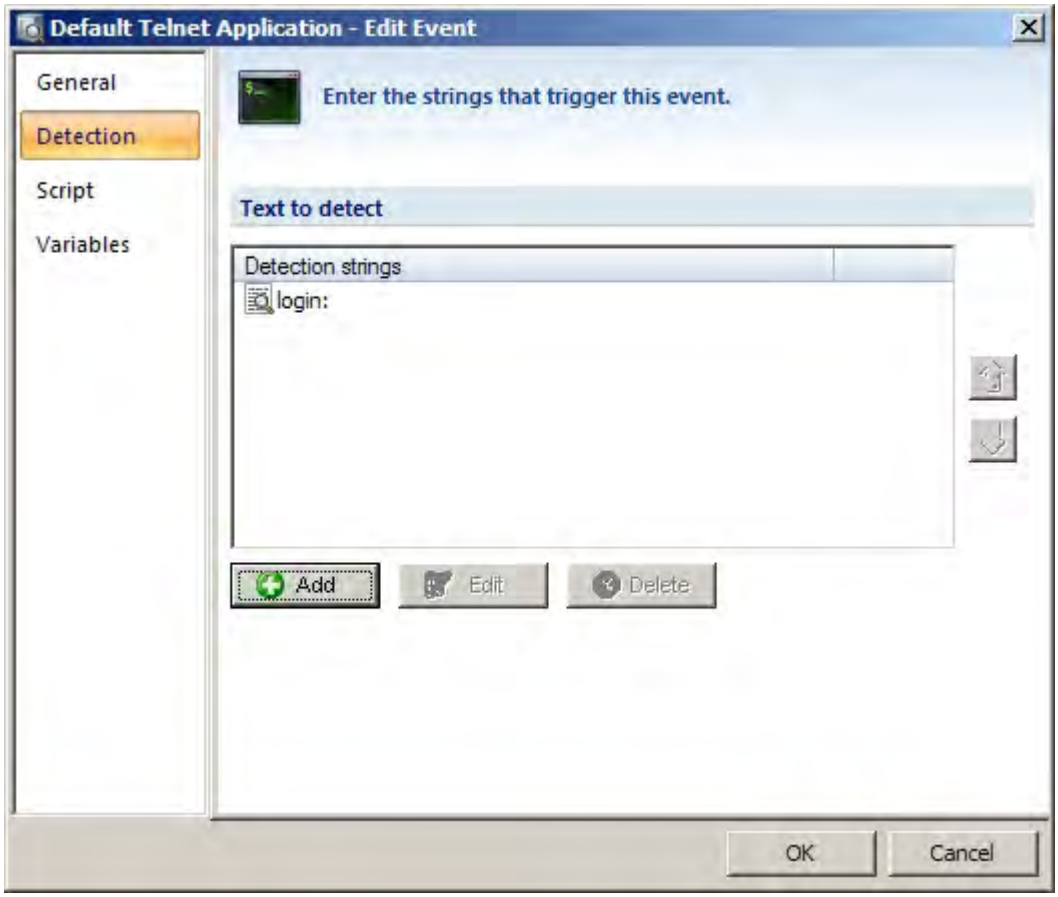
A CLI / Telnet application version type is an application that uses a windows console window. (For instance the Windows Command Line Interface or Windows Telnet)



The application can be detected using several restrictions. By default only the name of the executable is used to identify the application.

4.3.1. CLI Event

A Command Line event is triggered when one or more specified lines of text are displayed in the console window.

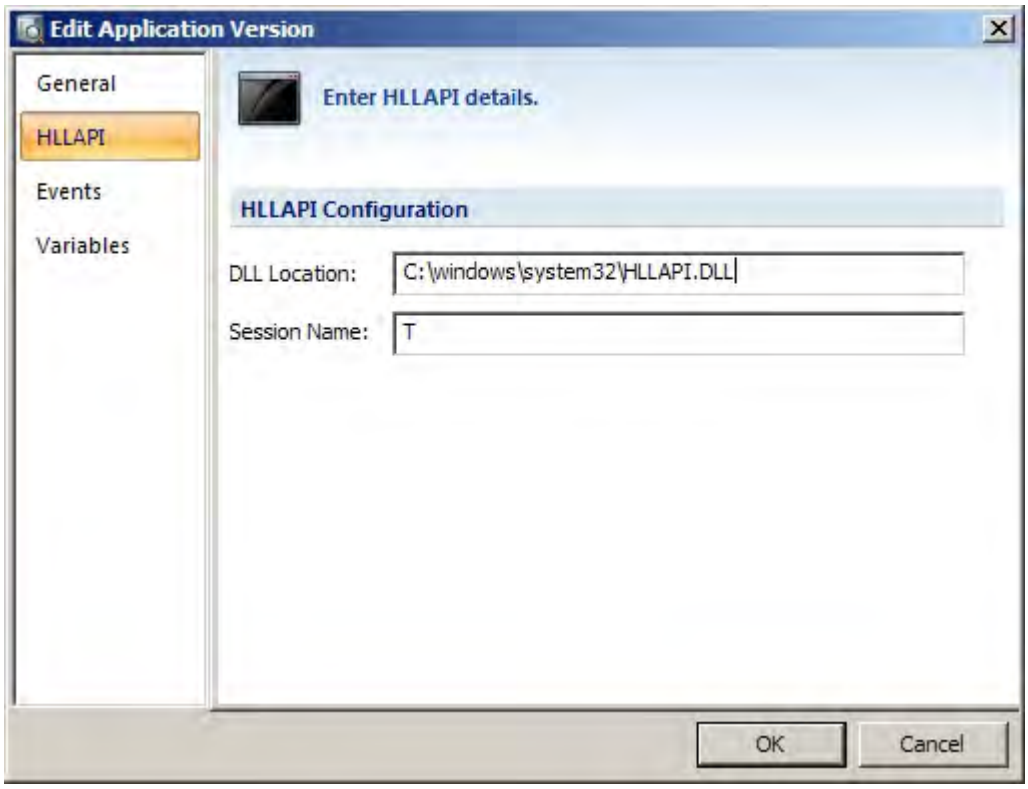


Click on 'Add' to add a string that must cause the script to trigger. The detection strings may contain wildcards.

Please note: The event is only triggered if the detection strings are found at the cursor position.

4.4. HLLAPI Telnet

A HLLAPI application is an application that supports the HLLAPI interface.

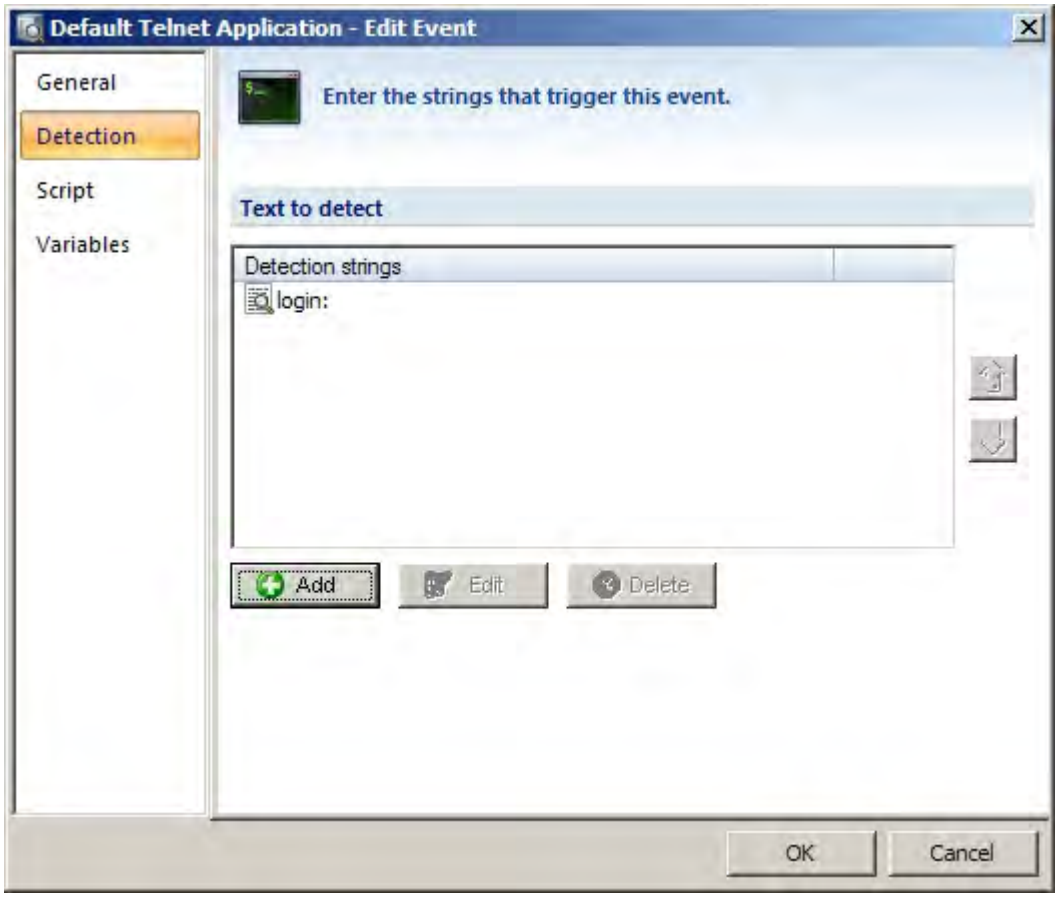


To be able to perform Single Sign On on an application that supports the HLLAPI interface, the name and location of the HLLAPI dll must be entered as well as the name of the session. Enter a '*' to perform SSO on all sessions. The name and location of the HLLAPI dll can be found in the documentation of the product that is being configured.

Please note: The session name may only be one character long.

4.4.1. HLLAPI Event

A HLLAPI event is triggered when one or more specified lines of text are displayed in the console window.

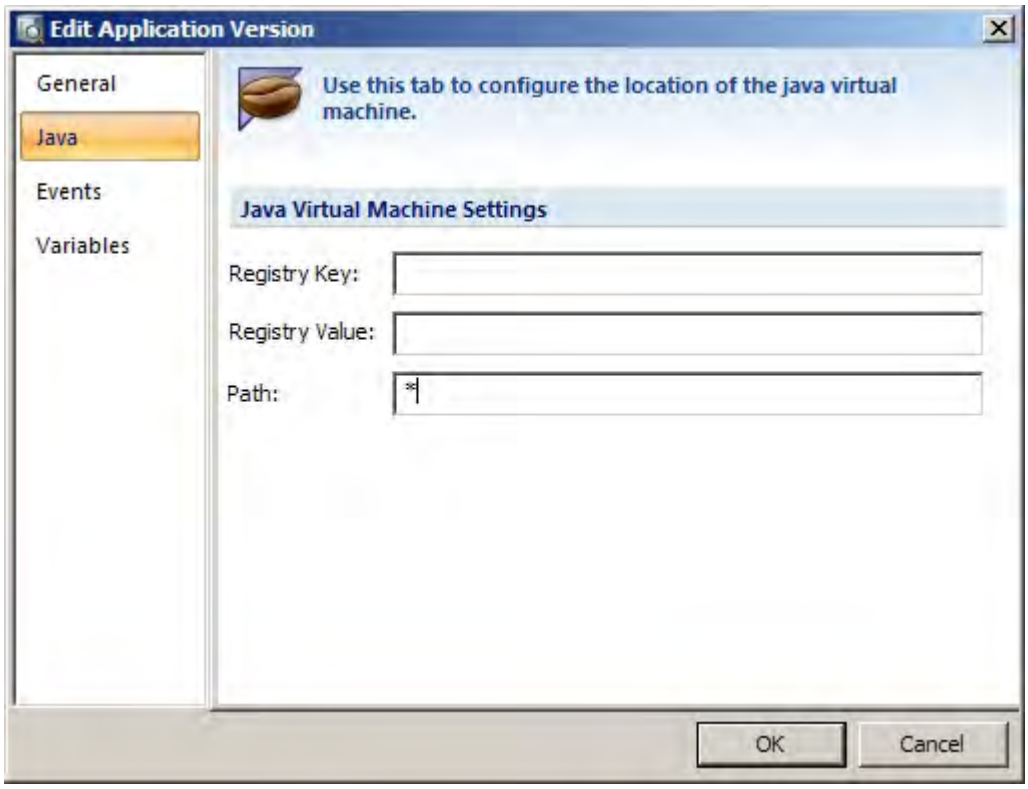


Click on 'Add' to add a string that must cause the script to trigger. The detection strings may contain wildcards.

Please note: The event is only triggered if the detection strings are found at the cursor position.

4.5. Java

A Java application is an application that is written in Java and uses Sun's java virtual machine to run.



To be able to perform Single Sign On on a java application, E-SSOM must know the location of the java virtual machine that the application is using so that it can install a java monitor. E-SSOM can get the location of the java virtual machine from the registry. The path may be a relative path that must be added to the found registry value or a full path to the Java Runtime Environment.

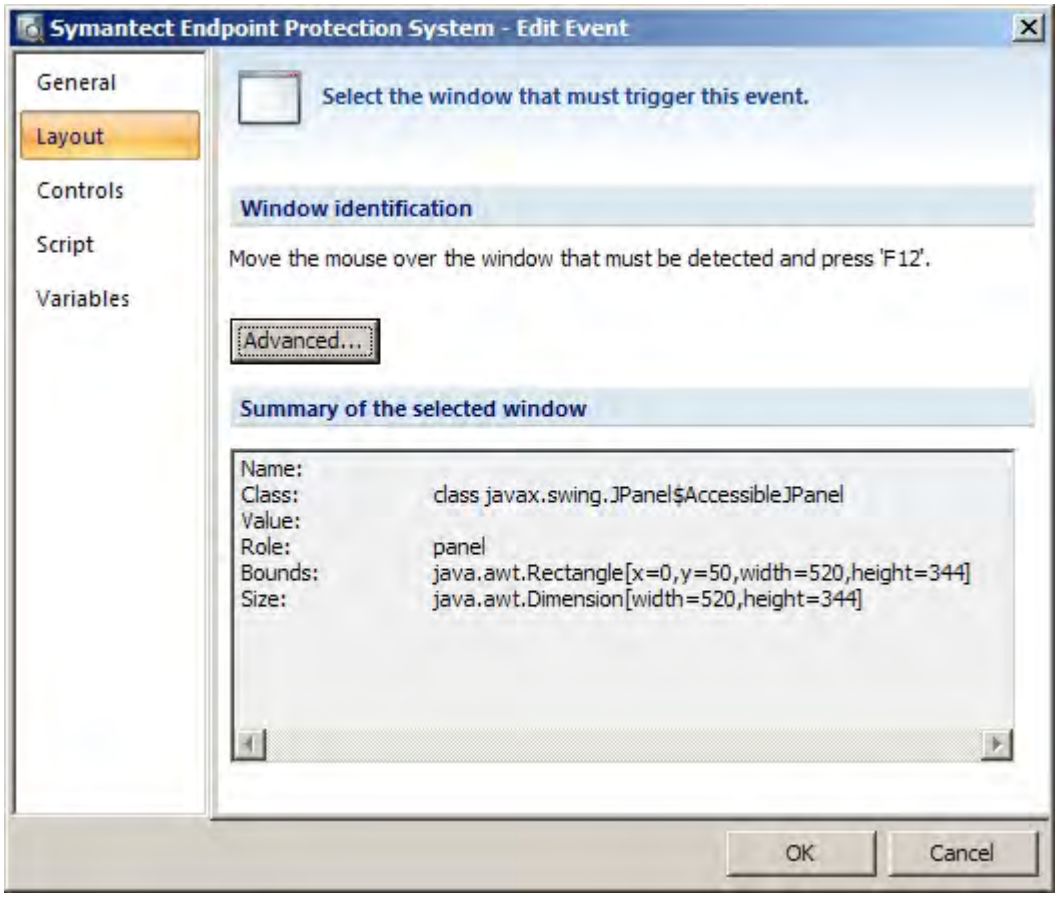
By default the Java Runtime Environment is stored in the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Runtime Environment\JavaVersion where 'JavaVersion' is replaced with the actual version number of the Java Runtime environment. The Registry value is 'JavaHome' by default.

Please note: If a '' is entered in the 'Path' edit box, E-SSOM will search the registry for Java Runtime Environments and install the java monitor for every java runtime environment it finds.*

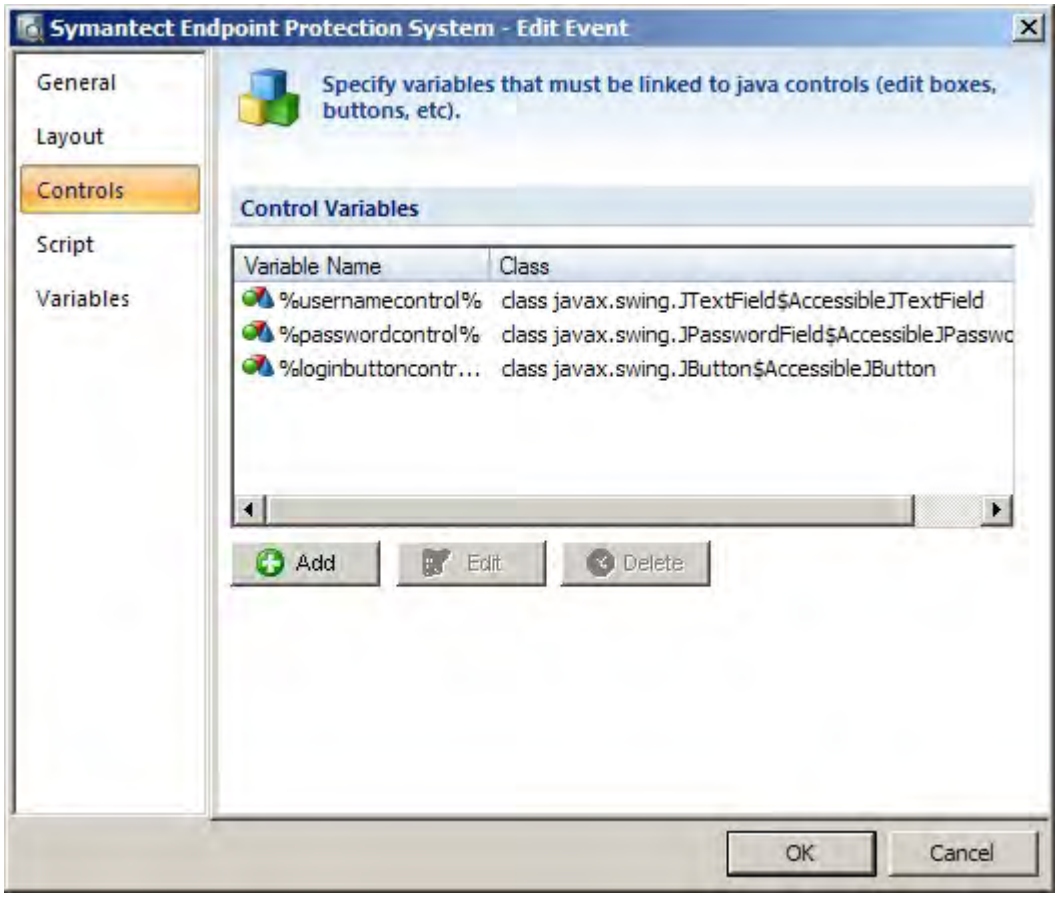
Warning: A java application type can only be configured if the E-SSOM java monitor is already installed. Please refer to the 'Java Monitor Installation' chapter on how to install the Java Monitor.

4.5.1. Java Event

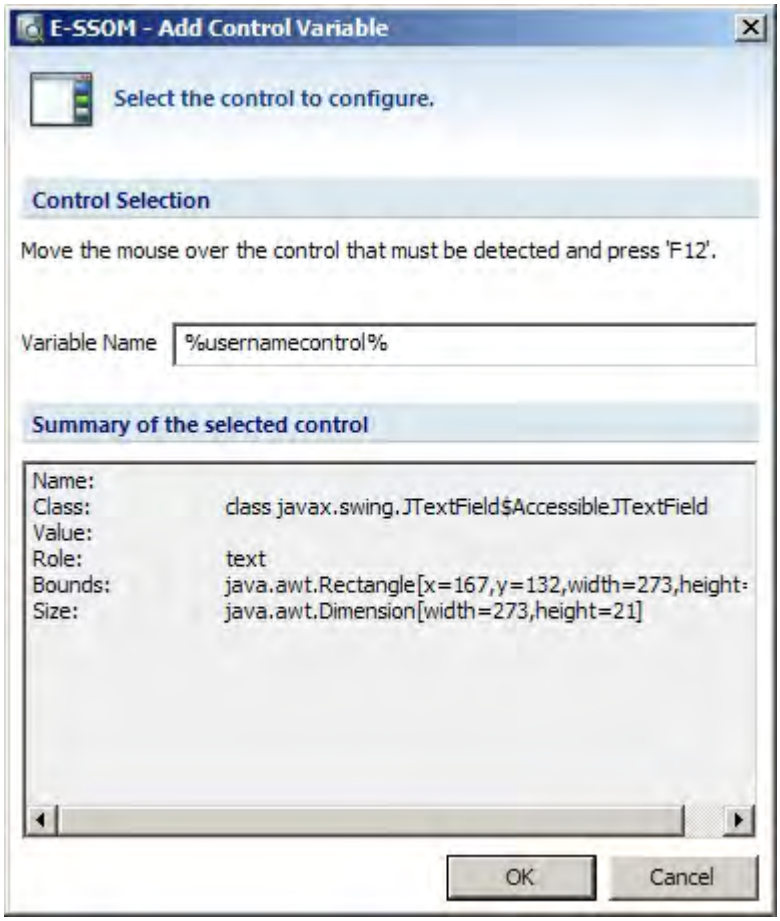
An event in a Java application is triggered when a specific window is displayed. Open the application that must be configured and go to the window that must trigger the event. Press SHIFT-F12 to 'capture' the window. This will store the layout of the window so that it can later be detected by the E-SSOM client.



The 'Controls' tab can be used to select controls so that they can be used in the script that is executed when this event is triggered.



Click on 'Add' to add a control to the list.



Open the window that contains the control that must be configured and move the mouse over the control. Click on 'SHIFT-F12' to capture the control. Enter the name of the variable. This variable can be used to identify the control in the script that is executed by this event so that the E-SSOM script can interact with the control.

Please note that the control must be inside the window that is configured in the 'Layout' tab.

4.5.2. Java Monitor Installation

To be able to configure java applications, the E-SSOM Java Monitor must be installed on the same machine as the E-SSOM Admin Console. There are two ways of installing the java monitor:

Installing the E-SSOM Java Monitor using an application definition:

1. Install the E-SSOM User Client on the machine that is running the Admin Console
2. Create a new application definition.
3. Add a new java application version to the definition
4. Go to the 'java' tab and enter the correct registry key and/or path
5. Save the application definition
6. Create a new application policy
7. Select the created application definition and assign it to the account that is used to configure E-SSOM with.
8. Save the application policy
9. Refresh the E-SSOM user client

Installing the E-SSOM Java Monitor manually:

1. Install the E-SSOM User Client on the machine that is running the Admin Console
2. Browse to the folder 'C:\Program Files\Tools4ever\SSO\SSO Client Service\SSOJava'.
3. Copy the file 'SSOJavaMon.jar' and 'SSOJava.dll' to the \lib\etc directory in the Java runtime environment directory. (For instance c:\program files\java\jre6\lib\ext)
4. Copy the file 'SSOJava.dll' to the \bin directory in the Java runtime environment directory. (For instance c:\program files\java\jre6\bin)
5. If it does not exist, create a text file called 'accessibility.properties' in the \lib directory in the Java runtime environment directory. (For instance c:\program files\java\jre6\lib\ext)
6. Open the file and add the following line: 'assistive_technologies=SSOJavaMonitor'. (without the single quotes)
7. Close the file.

5. Scripts

5.1. Overview

E-SSOM uses scripts to handle events (Events such as 'login' or 'change password') that occur in applications. E-SSOM uses a custom scripting language with powerful script actions to control dialogs and web pages. These scripts tell the E-SSOM Client Software, in detail, how to handle these events.

A script in E-SSOM consists of one or more script actions. These script actions can be used to perform all kinds of operations. A script action can place text into an edit box or press a button in a window. Other types of script actions can display messages to the user or jump to other parts of the script.

Scripts are executed when a pre-configured event occurs. In applications a script can be executed when a window is shown or when a window is hidden. In web pages a script can be executed after a page has finished loading.

Script Action
A script action can perform one specific task. It can for instance display a message box, press a button in a window or read the text from a control. All script actions have a label and most actions have one or more properties. Examples of how to configure a script action can be found in the 'Examples' chapter.

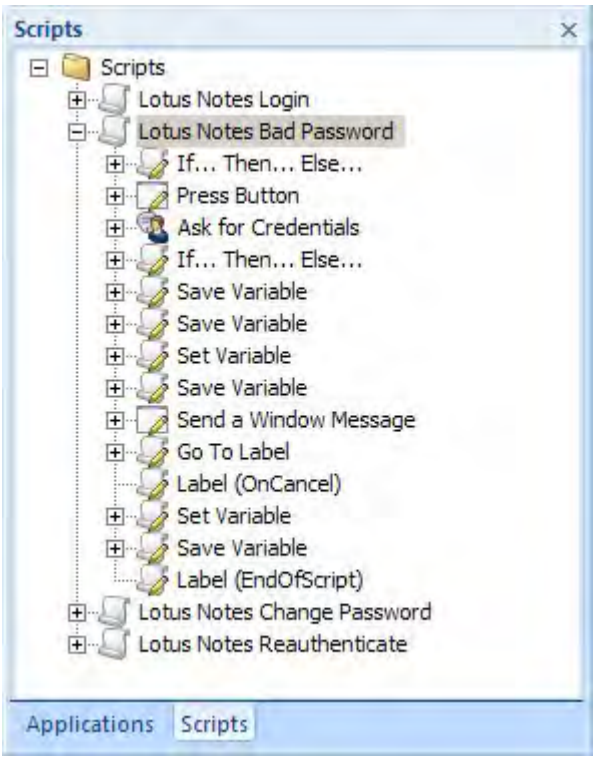
Label
A label uniquely identifies a script action in a script. Actions like the 'Go To' action or the 'If..Then..Else..' action can jump to a script action with a specific label.

Properties
Most script actions contain one or more properties that are used to configure the action.

Please note: The E-SSOM scripting guide explains in depth how to create and edit scripts in E-SSOM.

5.2. Configuring

Scripts can be created and edited using the Admin Console. Select the 'Scripts' tab in the main overview window:



Creating a new script
Right click in the scripts tree and select 'Add Script...' from the menu.

Editing an existing script

- Double click on the script in the tree that you want to edit.
- Select the script that you want to edit. Right click and select 'Edit Script...' from the menu.

Copying an existing script
Right click on the script that you want to copy and select 'Copy Script...' from the menu.

Importing and Exporting
Scripts can be imported and exported. E-SSOM is shipped with several pre-configured scripts that can be imported. These scripts can be found by default at: 'C:\Program Files\Tools4ever\SSO\Admin Console\Scripts'.

Please note: The E-SSOM scripting guide explains in depth how to create and edit scripts in E-SSOM.

6. Application Policies

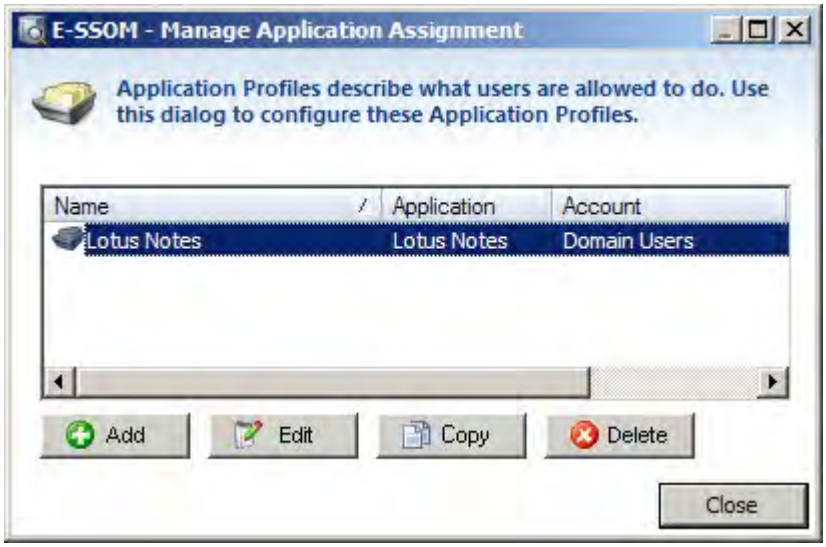
6.1. Overview

Application Policies are used to assign an application to a group of users. Application Policies are also used to control what users are allowed to do with the assigned application.

6.2. Configuring

Managing Application Policies

Application Policies can be configured in the 'Manage Application Assignment' dialog.



This dialog can be opened by selecting 'Management --> Application Assignment...' from the main menu. It allows you to add, edit, copy and delete Application Policies.

Adding or Editing an Application Policy

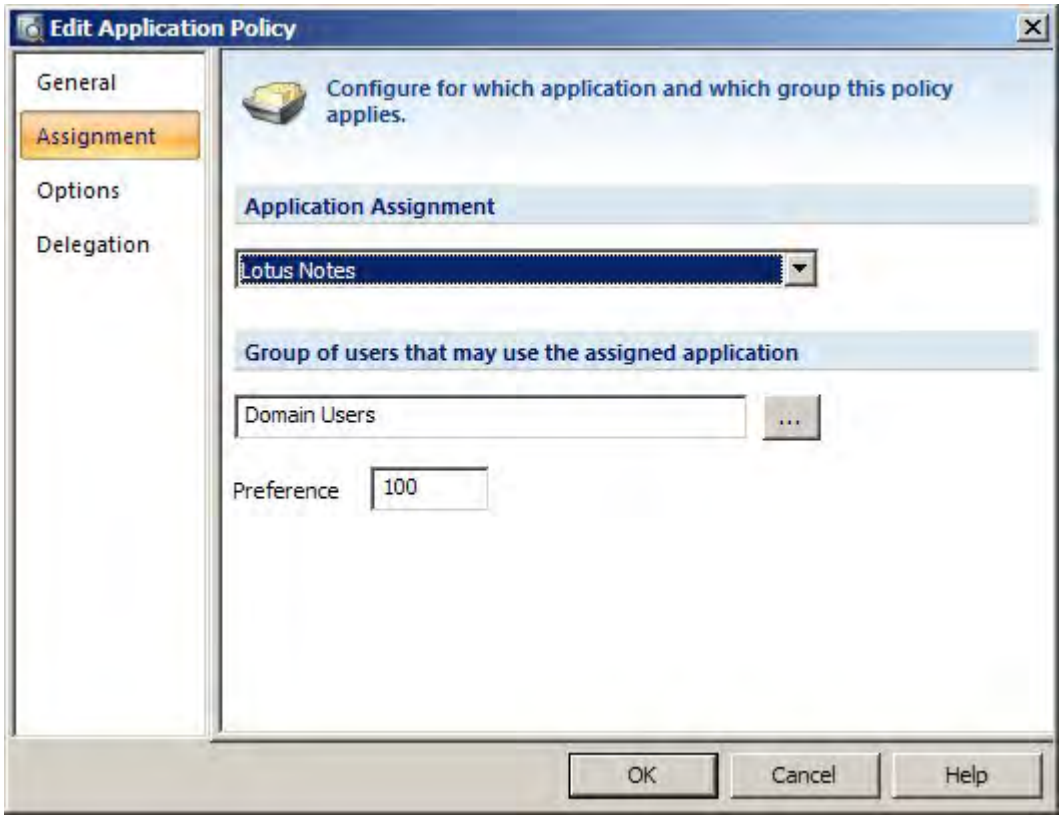
Click on 'Add' or select an Application Policy from the list and click on 'Edit' to open the 'Edit Application Policy' dialog.

General

The 'General' tab allows you to change the name of the Application Policy and to add an optional description. This tab also allows you to disable the policy, removing it from the E-SSOM User Client.

Assignment

The 'Assignment' tab allows you to select the application that you want to assign and select the group to which the application must be assigned.



Preference
If more than one Application Policy is created for the same application, it is possible that a user will receive two different application policies for the same application. These policies can have conflicting options. The E-SSOM Clients will use the first policy that they encounter. To prevent this issue, a preference number can be set. If a user receives two application policies for the same application and the first policy has a preference of 50 while the second has a preference of 100, the first policy will supersede the second.

Options

Offline Mode: When offline mode is enabled, the configuration and user data for the assigned application are stored locally on the end user's computer. This allows the user to automatically log on to the application even when the user is not connected to the E-SSOM Central Service. For instance this could occur when the user is at home or at a customer's site.
Generate passwords automatically: When an application requests that the user changes his or her password, E-SSOM can automatically generate and enter a new (strong) password. This has several benefits: the user no longer knows the password and can no longer log on to the application manually and the new password is guaranteed to be as strong as needed. (Password Policies can be created to configure the strength of a generated password.)
Do not allow users to delete their logon credentials: Enable this setting to prevent users from deleting their credentials.
Ask users to create multiple credential sets: If this setting is enabled, users will be asked to create additional sets of credentials when they log on to the application.
Allow users to add new credential sets using the client: Enable this setting to allow users to create additional sets of credentials using the E-SSOM User Client.

Delegation

When a user goes on leave he or she often has to transfer (some of) his or her responsibilities to a co-worker. To accomplish this, the delegated co-worker will often need to access an application using the absentee's credentials. This can create several security risks:

- The username and password for the application are often written down and left at the desk of the co worker.
- When the original user returns, the co-worker may retain the username and password and can continue to log on to the application.

E-SSOM provides a solution for this security issue and it is called 'Delegation'. Delegation allows a user to assign their logon credentials (stored by E-SSOM) to a co-worker for a specified amount of time. When the co-worker starts the application, he or she will be able to log in as the original user, but will not see the credentials used to complete the login action. When the delegation expires, the co-worker will no longer be able to log in automatically using the original user's credentials.

Run

Applications may be started from the E-SSOM client or automatically when the user logs on. The tab 'Run' can be used to configure how the application must be started.

Fast User Switching

Run logoff scripts after x seconds: When a user log off from the E-SSOM client the scripts flagged as 'logoff' will be ran. This settings causes the execution of these scripts to be delayed by the specified amount of seconds allowing the user to logoff.
Stop running logoff scripts: Enable this setting to stop the execution of logoff scripts after a specified amount of time.
Terminate application: Enable this setting to terminate the application after a specified amount of time. Please note that any unsafed data may be lost.

Please note: The highest number of seconds specified in the application policies assigned to a specific user will determine the time it takes to log off a user. During this time other users can not log on to the E-SSOM Client.

7. User Policies

7.1. Overview

User Policies are used to configure default settings for the user within the E-SSOM User Client. User Policies restrict what the user is allowed to do with the E-SSOM User Client.

-
- **Please note:** When a fast user switching policy is active, the settings from the fast user switching policy are used and not from the user that is logged on in E-SSOM.

7.2. Configuring

Managing User Policies

User Policies can be configured in the 'Manage User Policies' dialog.

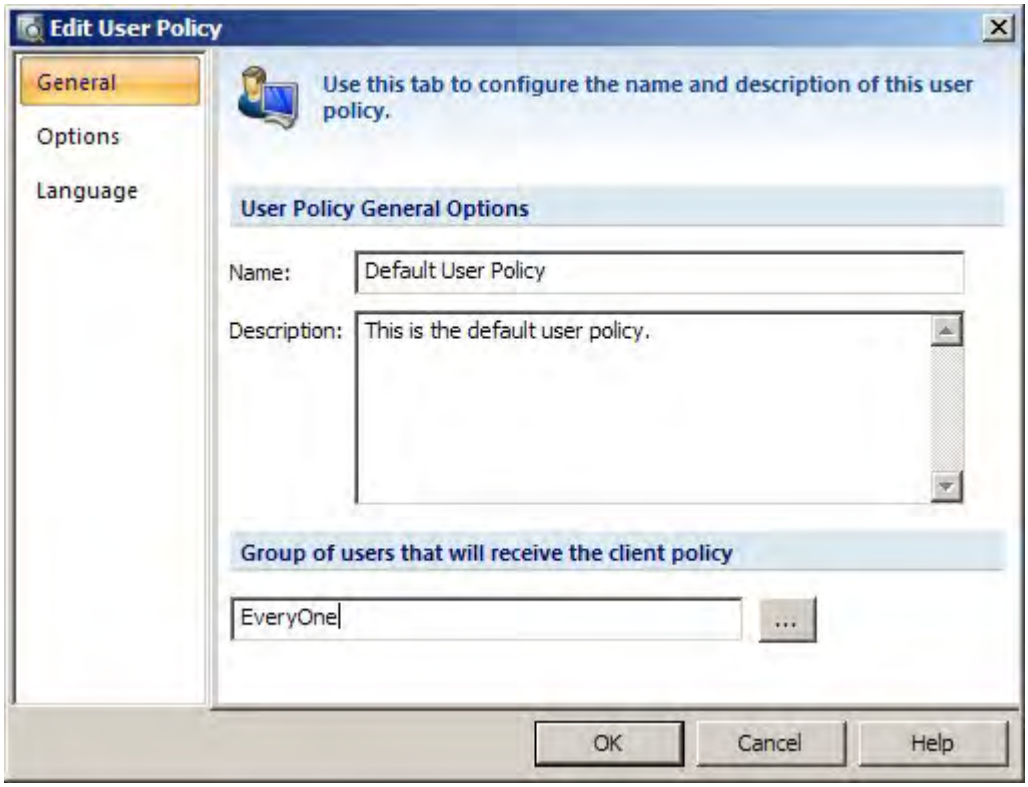
This dialog can be opened by selecting 'Management --> User Policies...' from the main menu. It allows you to add, edit, copy and delete User Policies.

Adding or Editing a User Policy

Click on 'Add' or select an User Policy from the list. Then click on 'Edit' to open the 'Edit User Policy' dialog.

General

The 'General' tab allows you to change the name of the User Policy and to add an optional description.



Assignment

- The assignment tab can be used to assign user policies to a user or a group.
-
- An additional restriction based on the name of the computer can be made. Please note that wildcards are allowed for this setting.
-

Preference

- If more than one User Policy is assigned to the same user. It is possible that a user will receive two different user policies. These policies can have conflicting options. The E-SSOM Clients will use the first policy that they encounter. To prevent this issue, a preference number can be set. If a user receives two user policies and the first policy has a preference of 50 while the second has a preference of 100, the first policy will supersede the second.

Options

Allow exit: Allows the user to exit the E-SSOM User Client. **Please note that this will stop all single sign on operations for this user.**
Allow manual refresh: Allows the user to manually refresh all data on the E-SSOM Central Service.

User Log off actions:
The Log Off actions are performed when the user logs of from the E-SSOM client in fast user switching mode or when the user removes his smartcard in normal mode.

- *Disabled* - Do nothing when the user logs off.
- *Lock Workstation* - Lock the users workstation.
- *Logoff* - Log out of windows. Enable the 'force logoff' setting to terminate any application that does not close. **Please note that this can cause unsaved data to be lost.**

Language

The 'Language' tab allows you to set the default language used by the E-SSOM Client. Please note that it is also possible for the user to change his or her default language in the E-SSOM User Client.

Processes

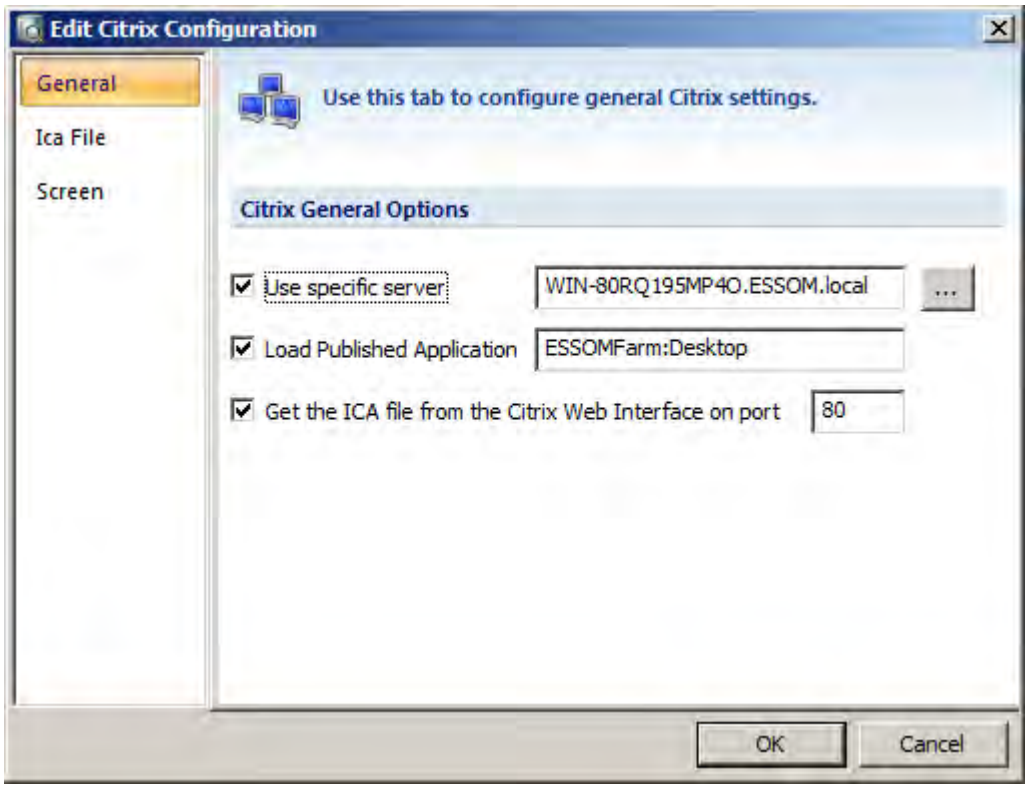
The 'Processes' tab allows you to configure the interval at which processes are monitored. This setting can be used to increase or decrease reaction time of E-SSOM regarding command line interface processes.

Fast User Switching

Enable Fast User Switching: Enable this setting to make the user or group assigned to this policy a fast user switching account.
Require Smartcard: Enable this setting to force users to log on with their smartcard.
Run logoff scripts when the user logs off: Enable this setting to run logoff scripts when the user logs of from the E-SSOM Client. Please note: Disabling this setting will stop log off scripts from running even when the setting in the application policy is enabled.
Resume Citrix Session: When this setting is enabled, the E-SSOM Client will automatically reconnect the user to an existing Citrix session or start a new session.

7.3. Citrix

The Citrix configuration dialog may be used to configure how the Citrix session is established:



Use specific server: Enter the name of a Citrix server that must be used to connect to. (If an ICA file in the ICA File tab is specified that contains the server name, it will override this setting)
Load Published Application: Specify the name of the published application that must be started. **Please note: the name of the Citrix farm containing the published application must be specified also in the following format: Farm:PublishedApp**
Get the ICA file from the Citrix Web Interface on port: Enable this setting to load the ICA file from the Citrix Web Interface so that the correct session is resumed. **Please note: If XenDesktop is used, this setting must be enabled to correctly start/resume sessions.**

8. Password Policies

8.1. Overview

Password Policies contain rules regarding the strength of the passwords used in E-SSOM. These policies can be used for different purposes:

Automatic generation of passwords
The 'Change Password' action can (if enabled in the Application Policy) automatically generate a new password for the user. The password is generated using the rules specified in the Password Policy.

Enforcing password complexity rules
When an application requests a password change, the 'Change Password' action in a script can display a dialog to change the users' password. A password policy can be used to enforce stronger passwords than the application itself.

8.2. Configuring

Managing Password Policies

Password Policies can be configured in the 'Manage Password Policies' dialog.

This dialog can be opened by selecting 'Management --> Password Policies...' from the main menu. It allows you to add, edit, copy and delete Password Policies.

Adding or Editing a Password Policy

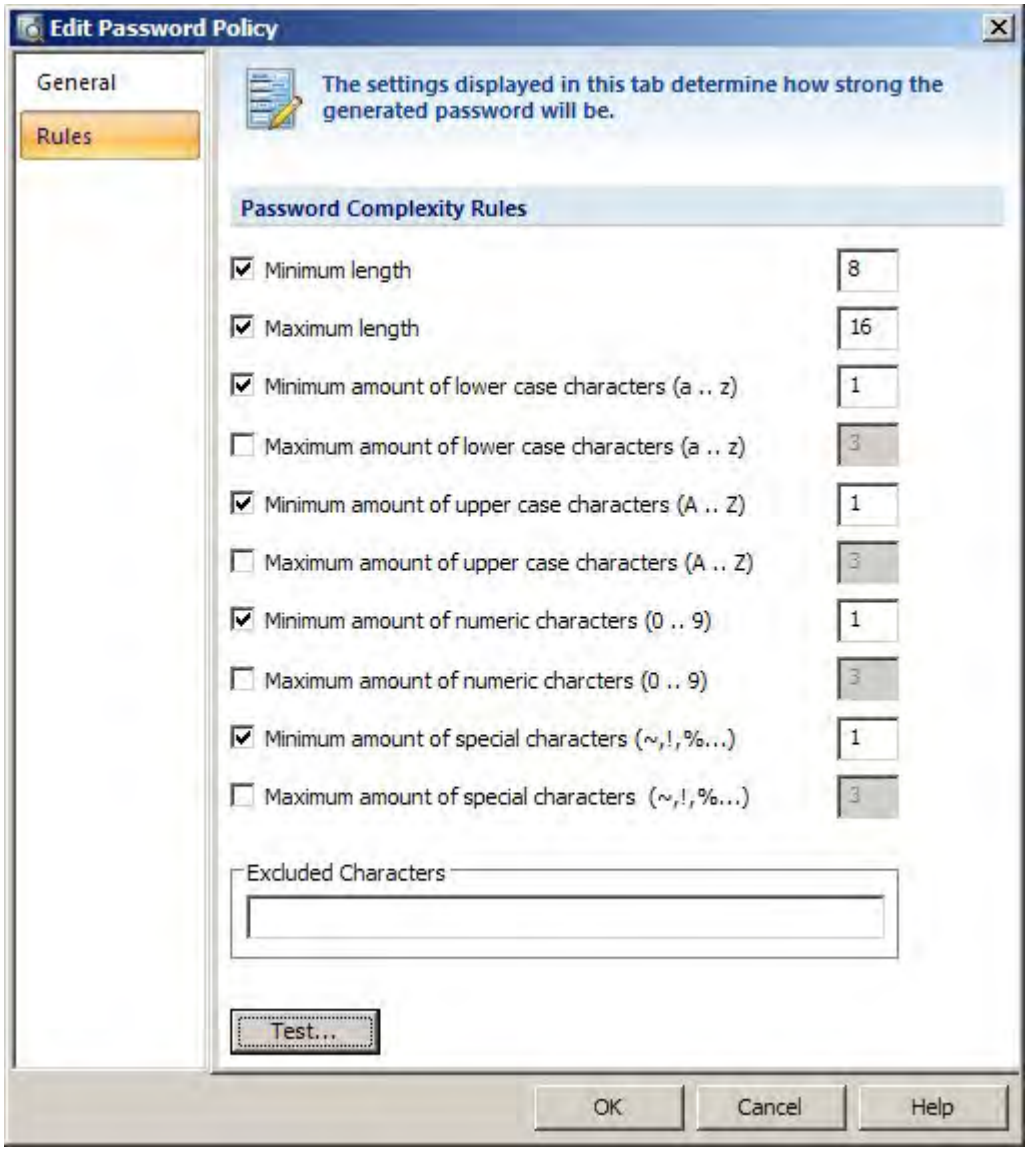
Click on 'Add' or select an Password Policy from the list and click on 'Edit' to open the 'Edit Password Policy' Dialog.

General

The 'General' tab allows you to change the name of the Password Policy and to add an optional description.

Rules

Rules can be enabled and disabled to enforce stronger or weaker passwords. When users change their passwords, they can see if their password meets these requirements.



Excluded characters: Enter characters that may not appear in the password.
Test: Press the 'Test...' button to test the generation of a password.

Please note: If the maximum password length is not specified, automatically generated passwords can become very long. (Maximum 128 characters)

9. Client Service Settings

The Client Service Settings dialog can be used to configure various settings regarding the E-SSOM Client Service. It can be opened from the Admin Console main menu: 'Management->Client Service Settings'.

General

The general tab may be used to specify the refresh rate of the client service. It can be set to a specific interval (Default: 240 minutes) or immediately. The setting 'immediately' should only be used in a test environment. Please note that the new settings will not take effect until the next refresh occurs.

Logging

The logging tab is used to configure the E-SSOM logging options.

Server name(s): The name of the E-SSOM Log Server. If this is left blank, the default E-SSOM Central Service is used.
Port Number: The port number on which the E-SSOM Central Service may be found.

Start Hour: The hour of the day at which the logs should be sent to the Central Service
Time Range: The variation in time on which the logs may be sent to the Central Service
Disable Single Sign On Events: Enable this setting to disable single sign on events all. **Please note: This does not disable logon events or process monitoring.**
Disable Logon events: Enable this setting to disable logon events generated by the authentication management module.
Disable Event Log Caching: Enable this setting to disable all event log caching. All of the log information is immediately sent to the Central Service.

Processes

The process monitoring tab is used to configure if process monitoring on the client is enabled and which processes should be monitored.

Enable Process Monitoring: Enable this setting to start monitoring processes on the client. Processes in all sessions on the client machine will be monitored. The E-SSOM Client does not need to be running to monitor processes.
Processes to monitor: Specify a comma separated list of executables that must be monitored. The E-SSOM Client Service will log the start and end time of the processes specified here.

10. Fast User Switching

Fast User Switching is a method to allow users to quickly switch identity. This feature is mainly used on centralized computers that are used by multiple users during the day. The computer is logged on using an active directory account (For instance 'Accounting' or 'kiosk01') that is known to the users that want to use Fast User Switching. The computer is logged on using this 'kiosk' account. When the computer has been logged on, the users will log on to E-SSOM using their own active directory credentials or a smartcard. After the user has logged on to E-SSOM, he will be able to automatically log on to the required applications.

The kiosk PC may be locked when no one is using it. Users can unlock the desktop of the kiosk user using their own account. This will automatically log them on to the E-SSOM Client.

10.1. Requirements

- An Active Directory user account (a kiosk account) that can be used by multiple users to log on to windows. The account and password are known to the users that need to be able to use the fast user switching functionality.
- The kiosk user account must have access to the applications that users may run.
- The Follow Me functionality requires a Citrix environment.
- For other users to be able to unlock the desktop of the kiosk user, the SSOClientExtensions.msi package must be installed.
- The 'Terminal Services' service must be running.

10.2. Configuration

Fast User Switching may be configured using user policies. A user policy must be created with the settings 'enable fast user switching' enabled. This policy must be assigned to the active directory account (For instance 'Accounting' or 'kiosk01') that is known to the users that want to use FUS. The 'User Policies' section of this document contains more detailed information on how to configure user policies.

Application policies can be configured so that applications are started automatically when a user logs on to the E-SSOM User Client. The application policies can also be used to configure if the application must be closed when the user logs off.

Configuring Fast User Switching Step by Step

Prerequisites:

- E-SSOM Central Service Installed
- E-SSOM Client Installed on a Windows XP/Windows Vista or Windows 7 machine
- SSOClientExtensions.msi installed on the machine running the E-SSOM Client
- A 'kiosk' user account in the Active Directory (For instance 'Kiosk01')

Creating the Fast User Switching User Policy

1. Open the E-SSOM Admin Console and go to 'Management --> User Policies...'.
2. Click on 'Add...'.
3. Change the name of the new policy to 'Fast User Switching Policy' and go to the assignment tab.
4. Set the 'kiosk' user account as the account that will receive the client policy. (For instance: MyDomain\KioskUser01)
5. Set the preference to '90' to make sure that this user policy will be selected for the provided account.
6. Go to the options tab and select the 'Lock Workstation' radio button. This will automatically lock the kiosk PC when a user logs off from E-SSOM.
7. Go to the fast user switching tab and check the 'Enable Fast User Switching' checkbox.
8. Click on 'OK'. The fast user switching policy has been created.

Using Fast User Switching

1. Log on to the client computer using the 'kiosk' account. (The machine will log in and the E-SSOM client will display 'not logged in' in the title bar.)
2. Right click on the E-SSOM client icon in the task and select 'Log In...'.
3. A login dialog will popup. Enter the credentials of a normal user to log in. (If the logon was successfull the username will be displayed in the title bar and the application policies of the user will be displayed in the E-SSOM Client.
4. Right click on the E-SSOM client icon in the task and select 'Log out...' to log out of the E-SSOM Client and to lock the desktop.

10.3. Follow Me

Follow me is a feature that allows users to quickly and automatically reconnect to their Citrix desktop on another machine using their logon credentials. These credentials may be typed manually or a token may be used (for instance a smartcard.) When the user logs of from the client (manually or by removing his token) the Citrix session will automatically disconnect.

11. Authentication Management

The E-SSOM Authentication Management module allows users to assign a smartcard to an Active Directory user account. This allows the user to log on to Windows using a smartcard and a PIN code in stead of a username and a password.

Users will be able to log on to their desktop quickly and will automatically log off or lock their computer when they remove the smartcard from the reader. If a contactless card is used, the user can log off with one card swipe.

11.1. Requirements

- Computers that must be logged on to with a smartcard must have Windows XP or higher installed.
- The SSOClientExtensions.msi package must be installed on client machines.
- The SSOUserClientSoftware.msi package must be installed on the client machines.
- A compatible smartcard reader must be installed.
- Depending on the type of card, the SafeSign middleware must be installed.

11.2. Smartcard Policies

Smartcard policies are used to modify the behaviour of the Authentication Management feature.

Managing Smartcard policies

Smartcard policies can be managed from the 'manage smartcard policies' dialog. This dialog can be opened by selecting 'Management --> Smartcard Policies...' from the main menu. It allows you to add, edit, copy and delete Smartcard Policies.

Adding or Editing a Smartcard Policy

Click on 'Add' or select a smartcard policy from the list. Then click on 'Edit' to open the 'Edit Smartcard Policy' dialog.

General

The 'General' tab allows you to change the name of the smartcard policy and to add an optional description. This tab may also used to (temporarily) disable the smartcard policy.

Assignment

- The assignment tab can be used to assign smartcard policies to a user or a group.
-
- *Global Policy*
- Only one global policy can be configured. This policy is used when an unassigned card is presented to the system during the logon phase. As soon as the enrollment wizard has identified the user, the policy for that user will become effective.
-

Preference
If more than one smartcard policy is assigned to the same user. It is possible that a user will receive two different smartcard policies. These policies can have conflicting options. The E-SSOM Clients will use the first policy that they encounter. To prevent this issue, a preference number can be set. If a user receives two smartcard policies and the first policy has a preference of 50 while the second has a preference of 100, the first policy will supersede the second.

Options

Ask for enrollment: When this setting is enabled, E-SSOM will ask a unenrolled user during the login phase if he wants to enroll a smartcard.
Force enrollment: When this setting is enabled, E-SSOM will force a user to enroll if he has not done so yet. **Please note: this will prevent the user to logon without enrolling first.**
Allow multiple cards: Enable this setting to allow users to assign multiple cards to their user account.
Allow unenroll: Enable this setting to allow users to unassign a smartcard using the enrollment wizard.
Use smartcard PIN code: If this setting is enabled, E-SSOM will verify if the chosen PIN code is the same as the PIN code on the smartcard. Please note that this feature is currently only supperted when using smartcards that support the SafeSign library.

*Force smartcard login:*This setting forces the user to log on using a smartcard. **Please note: This will prevent users from logging on using their credentials entirely.**
Allow unlock without PIN: Enable this setting to allow users to unlock their desktop with their smartcard without using a PIN code. They must have logged on to or unlocked their computer within the specified interval.
Allow login without PIN: Enable this setting to allow users to logon to their desktop with their smartcard without using a PIN code. They must have logged onto their computer before within the specified interval.

11.3. Managing Smartcard Assignments

Smartcard assignments may be viewed from the 'smartcard...' entry in the management menu. The smartcard assignment dialog allows administrators to add and delete smartcards. It also allows administrators to reset the pin code of a smartcard. Please note that a cardreader must be installed on the system running the Admin Console to be able to add smartcards to E-SSOM.

12. Reporting

12.1. Introduction

E-SSOM keeps track of several events that occur on the client machines. These events are logged by the E-SSOM client software and periodically (by default daily) sent to the E-SSOM central service. The Central Service stores these events in the E-SSOM database.

Currently E-SSOM logs the following events:
Script execution: An event is logged every time a script is executed and the 'log event' script action is encountered within that script.
User Logon: When the authentication module is installed, an event is logged every time that a user logs on.
User Unlock: When the authentication module is installed, an event is logged every time that a user unlocks a desktop.

Reports can be generated based on the information that is logged to the database.

12.2. Process Monitoring

E-SSOM can be configured so that it monitors processes on the client machines. The starttime and the endtime of a configured process is stored in the E-SSOM Log database. This allows administrators to view which processes are being used by end users and the maximum amount of concurrent users of a process.

Process monitoring can be configured in the client service settings dialog in the Admin Console.

13. E-SSOM AppInit Client

The E-SSOM client comes in two forms. The normal E-SSOM client called which is installed by the SSOUserClientSoftware.msi file and the 'AppInit' version which is installed using the SSOUserClientSoftwareAppInit.msi file. The AppInit Client is only used in situations where programs run without a desktop or shell. For instance when running a Citrix published application.

Warning: Do not install the SSOUserClientSoftware.msi package and the SSOUserClientSoftwareAppInit.msi on the same machine.

The E-SSOM Appinit Client installs several components and changes registry keys. The source files can be found in the SSO Client Software installation directory.

Win32
The SSOAppI.dll is copied to the c:\windows\system32 directory
The SSOHook.dll is copied to the c:\windows\system32 directory

The value 'SSOAppI.dll' must be added to the 'AppInit_DLLs' registry key in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows If the key already contains a value, separate the new value with a comma.
The 'LoadAppInit_DLLs' registry key in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows must be set to '1'.

x64
The SSOApx64.dll is copied to the c:\windows\system32 directory
The SSOHookx64.dll is copied to the c:\windows\system32 directory

The value 'SSOApx64.dll' must be added to the 'AppInit_DLLs' registry key in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows If the key already contains a value, separate the new value with a comma.
The 'LoadAppInit_DLLs' registry key in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows must be set to '1'.

The SSOAppI.dll is copied to the c:\windows\SysWOW64 directory
The SSOHook.dll is copied to the c:\windows\SysWOW64 directory

The value 'SSOAppI.dll' must be added to the 'AppInit_DLLs' registry key in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows If the key already contains a value, separate the new value with a comma.
The 'LoadAppInit_DLLs' registry key in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows must be set to '1'.

Please note:

- **If files cannot be copied because they are in use, rename them by adding '.bak'. Then copy the new files. Reboot the machine after making these changes.**
- **Windows 7 and Windows Server 2008 R2 have an additional key called 'RequireSignedAppInit_DLLs'. E-SSOM builds up to and including 1074 do not have a signed AppInit dll and require that this registry is set to '0'. Later versions of E-SSOM do not have this requirement.**

14. E-SSOM Anywhere

E-SSOM may be configured so that users can connect to the Central Service from locations outside the company network. This allows users to continue using E-SSOM when they work at home. To be able to create a secure connection over the internet E-SSOM uses a technique called 'RPC over HTTP'.

This chapter describes how to configure E-SSOM and IIS to enable RPC over HTTP for E-SSOM.

14.1. Requirements

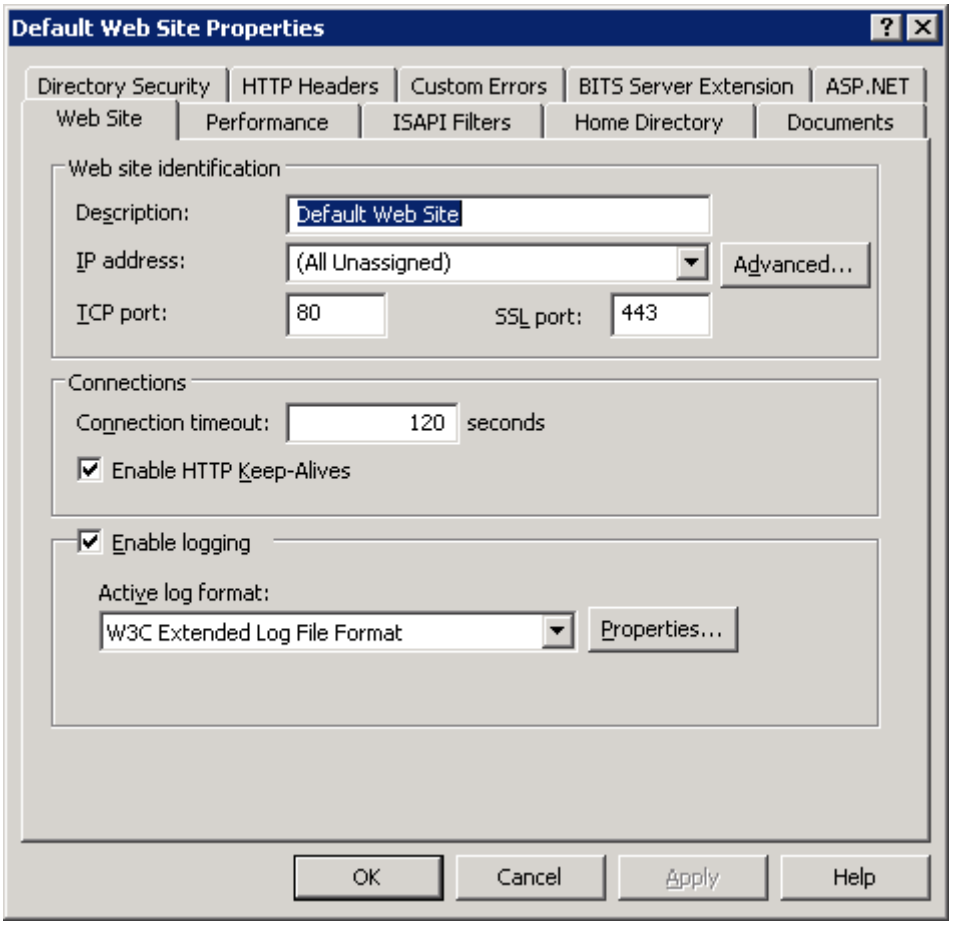
- IIS must be installed on the server running the E-SSOM central service
- RPC over HTTP must be installed on the server running the E-SSOM central service
- A valid SSL Security Certificate is required

14.2. IIS 6 Configuration

Please note: This step by step guide assumes that Windows 2003 is used as the operating system running the E-SSOM Central Service and that the E-SSOM Central Service is already installed on the machine.

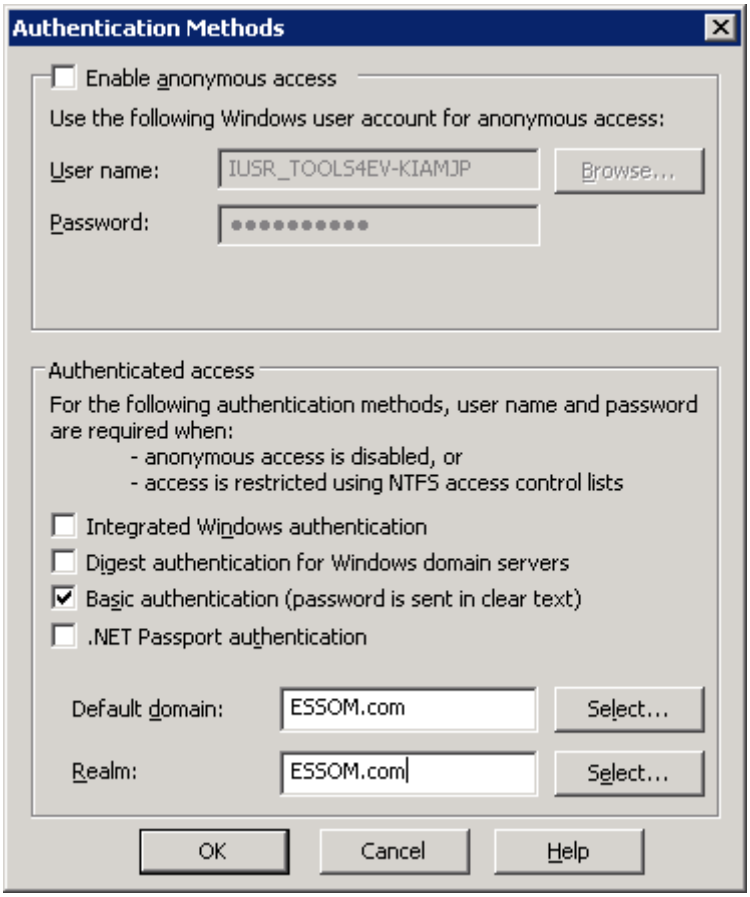
1. Install IIS 6 through the 'add/remove windows components' in the 'add/remove software configuration' screen.
2. Install RPC over HTTP through the 'add/remove windows components' in the 'add/remove software configuration' screen.
3. Open the E-SSOM Admin Console
4. Go to 'Service Management --> Configure...'.
5. Go to the 'Connection' tab.
6. Check the 'Enable HTTP Proxy on port' checkbox.
7. Set the port number to '36786'.
8. Click on 'OK'.
9. Restart the E-SSOM Central Service.
10. Open the IIS Manager.
11. Go to the 'Default Web Site' in 'Internet Information Services--> Computer Name --> Web Sites'.
12. Right click on the 'Default Web Site' and select 'Properties' from the menu.

13. Specify '443' in the 'SSL Port' edit box.



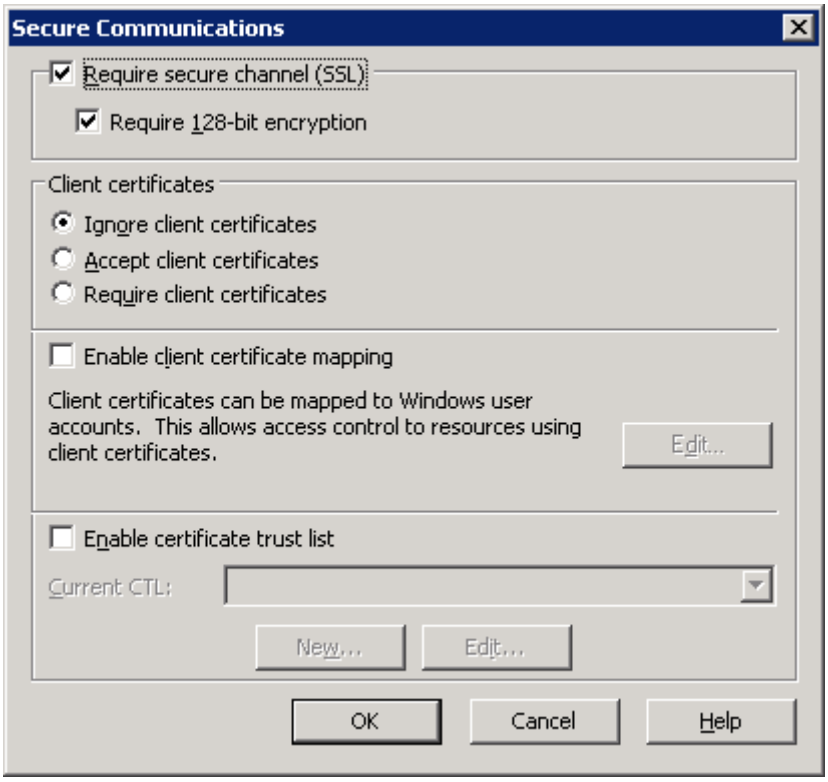
14. Go to the 'Directory Security' tab.
15. Click on 'Edit...' in the 'Authentication and Access control' group box.

16. Disable all checkboxes except for the 'Basic authentication' checkbox.



17. Specify domain name in the 'Default Domain' and the 'Realm' edit box.
18. Click on 'OK'.
19. Click on 'Server Certificate...' and create or import the certificate that must be used.
20. Click on 'Edit...' in the 'Secure Communications' group box.

21. Enable the 'Require secure channel (SSL)' checkbox as well as the 'Require 128-bit encryption' checkbox.



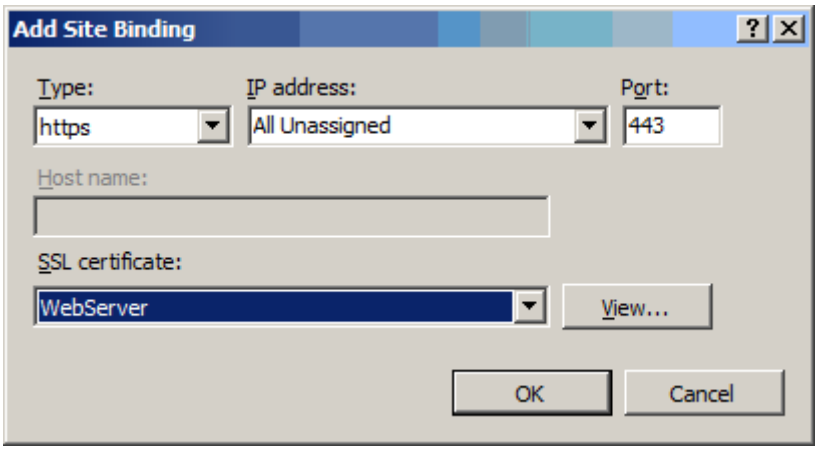
22. Click on 'ok' until all dialogs are closed.
23. Go to 'Start --> Run...'.
24. Type 'regedit' and click on 'ok'.
25. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy
26. Double click on the 'ValidPorts' value.
27. Add 'ESSOMServer.ESSOM.com:36786'. Separate multiple entries by using a semicolon.

28. Click on 'OK' and close the registry editor.
29. Restart IIS.

14.3. IIS 7 Configuration

Please note: This step by step guide assumes that Windows 2008 is used as the operating system running the E-SSOM Central Service and that the E-SSOM Central Service is already installed on the machine.

1. Install IIS 7 through the 'Roles' tab in the Server Manager. **Please note: Enable 'Basic Authentication' in the 'Role Services' tab during installation.**
2. Install RPC over HTTP through the 'Features' tab in the Server Manager.
3. Open the E-SSOM Admin Console
4. Go to 'Service Management --> Configure...'.
5. Go to the 'Connection' tab.
6. Check the 'Enable HTTP Proxy on port' checkbox.
7. Set the port number to '36786'.
8. Click on 'OK'.
9. Restart the E-SSOM Central Service.
10. Open the IIS Manager.
11. Go to 'Computer Name' and double click on 'Server Certificates' in the right pane.
12. Import or create a valid SSL certificate. **Please note: The certificate must be valid at the client workstation.**
13. Right click on 'Default Web Site' in 'Computer Name --> Sites' and select 'Edit Bindings...' from the menu.
14. Click on 'Add...'.
15. Select 'https' as the type to use and select the SSL certificate to use.



16. Click on OK. Click on 'Close'.
17. Go to the 'Default Web Site' in 'Computer Name --> Sites'.
18. Double click on 'Authentication' in the right pane.
19. Enable 'Basic Authentication' and disable all other authentication methods.
20. Click on 'Back'.
21. Double Click on 'SSL Settings'.
22. Select the 'Require SSL' and if the checkbox exists 'Require 128-bit SSL' checkboxes. **Warning: If available set the client certificates radio button to 'Ignore'.**

23. Click on 'Apply' in the rightmost pane.
24. Close the IIS Manager.
25. Go to 'Start --> Run...'.
26. Type 'regedit' and click on 'ok'.
27. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy
28. Double click on the 'ValidPorts' value.
29. Add 'ESSOMServer.ESSOM.com:36786'. Separate multiple entries by using a semicolon.

30. Click on 'OK' and close the registry editor.
31. **Restart the server.**

15. High availability / Fail Over

E-SSOM can be configured for high availability. In the event of server failure, other server can take over. If clients are configured in offline mode, the clients can continue to work even if it is not possible to make any connection to a Central Service.

This chapter describes the various high availability methods and how to configure them.

15.1. User Client Offline Mode

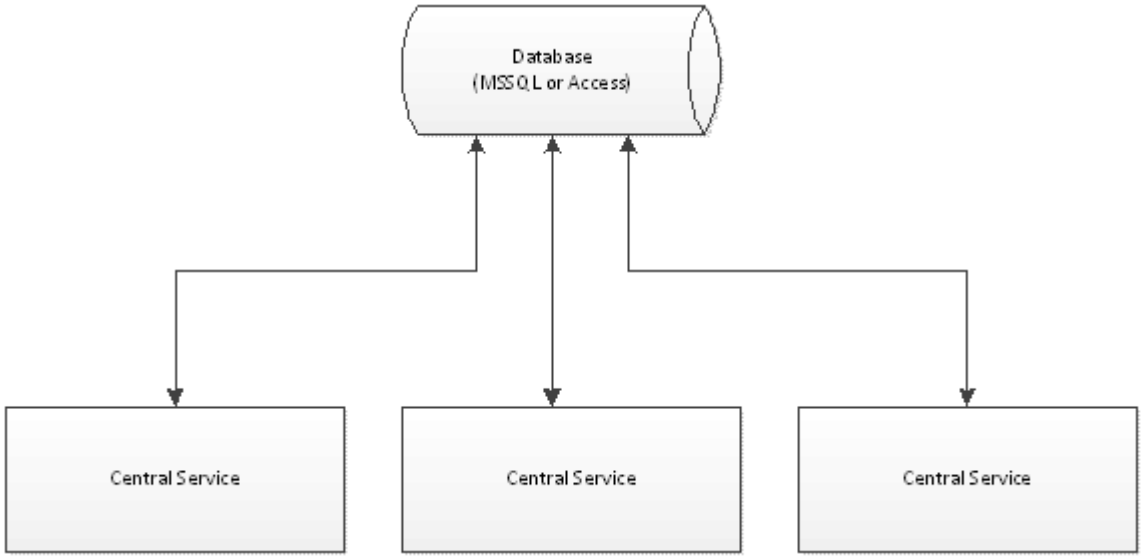
The User Client continues to work properly even when the Central Service is not available. When a client is rebooted, the User Client Software will not be able to retrieve the user data unless offline mode is enabled. This feature allows administrators to configure the user data that must remain available when the Central Service is not available. This can be specified in the application policy of the application that must remain available.

When enabled, the User Client will locally cache the user data on disk. The data is encrypted using triple DES.

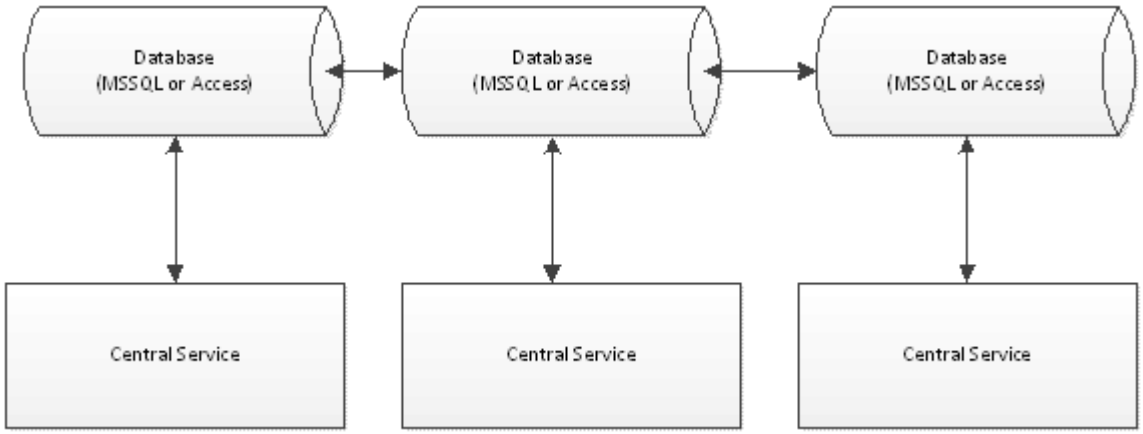
15.2. Multiple Central Services

E-SSOM can be configured to have multiple identical Central Services. Clients can automatically select a Central Service to which to connect. This prevents downtime in the case of hardware failure.

Multiple E-SSOM Central Servers with a single database
Multiple E-SSOM Central Servers may be installed to provide high availability in case of hardware failure on one of the servers that is running the E-SSOM Central Service. The clients will automatically connect to another server if the connection to the Central Service fails. The MSSQL database may run on a different machine. *Please note: For high availability the MSSQL database should run on a MSSQL Cluster.*



Multiple E-SSOM databases.
In combination with multiple E-SSOM Central Services multiple E-SSOM Databases may be used. They databases must run on a MSSQL server and replicate the data stored in the database to the other E-SSOM databases.



15.3. MSSQL Replication Configuration

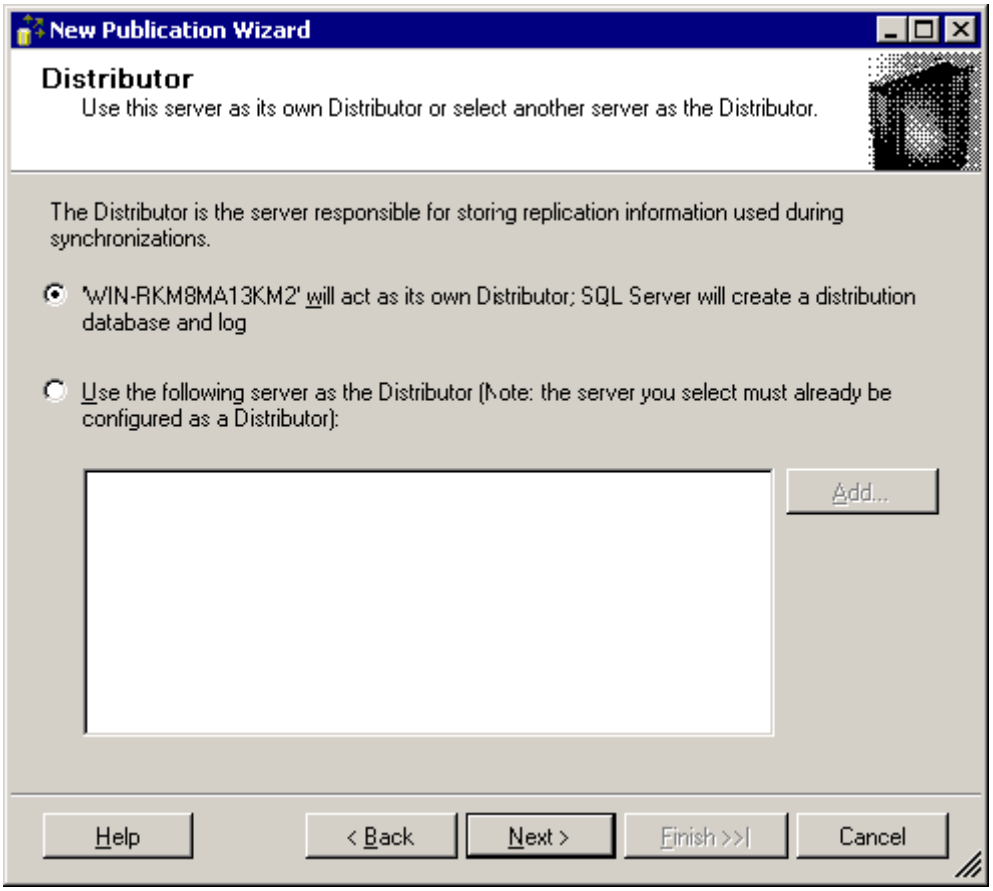
Replication in SQL Server consists of two parts: A publication and one or more subscriptions to that publication. This chapter first describes how to create a publication and then how to create a subscription to that publication.

Please note that multiple E-SSOM Services must be configured in the GPO setting 'Service Location' to be able to use the fail over feature. The Deployment Guide describes step by step how to configure the GPO for E-SSOM.

15.3.1. Publication

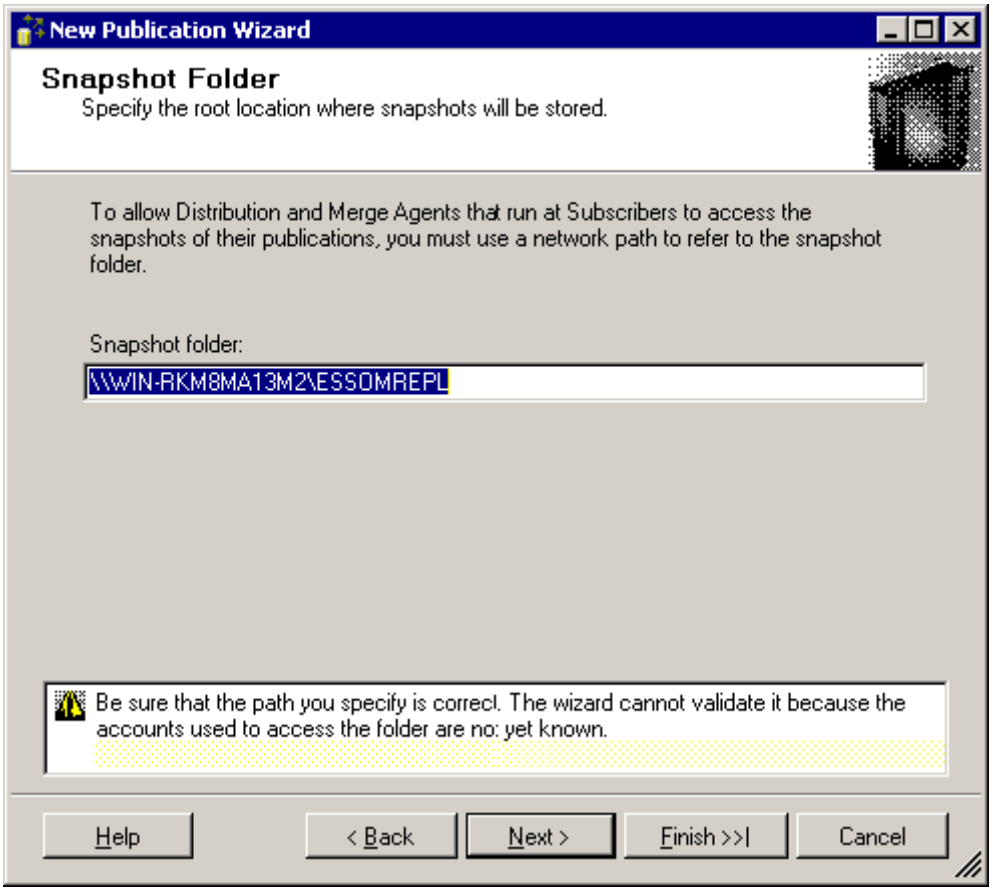
This chapter describes how to create a publication. A publication is made on the first SQL Server. A subscription should be made on all other SQL Servers.

1. Open SQL Server Management Studio
2. Go to Replication --> Local Publications
3. Right click on Local Publications and select 'new publication...'.
4. Click on next. The following page is displayed: ***Please note that this page is not always displayed. If the page is not displayed continue to step 8**



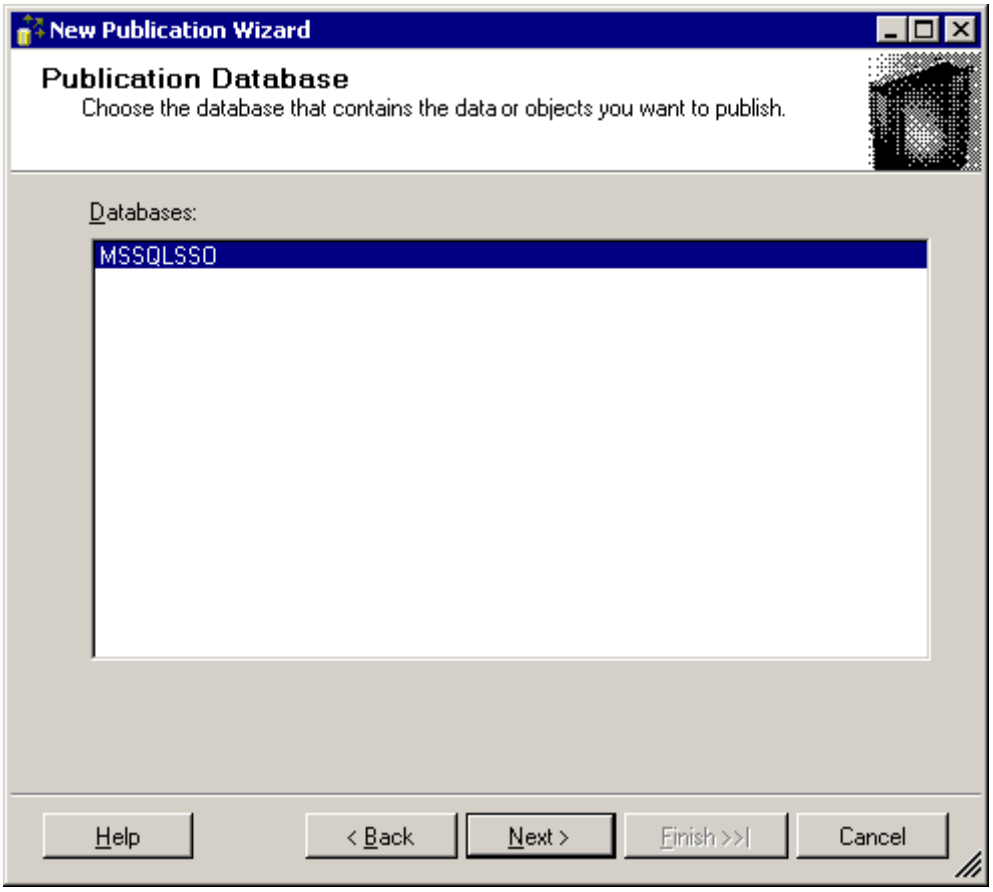
5. Select ''ServerName' will act as its own Distributor; SQL Server will create a distribution database and log'.

6. Click on next. The following page is displayed:



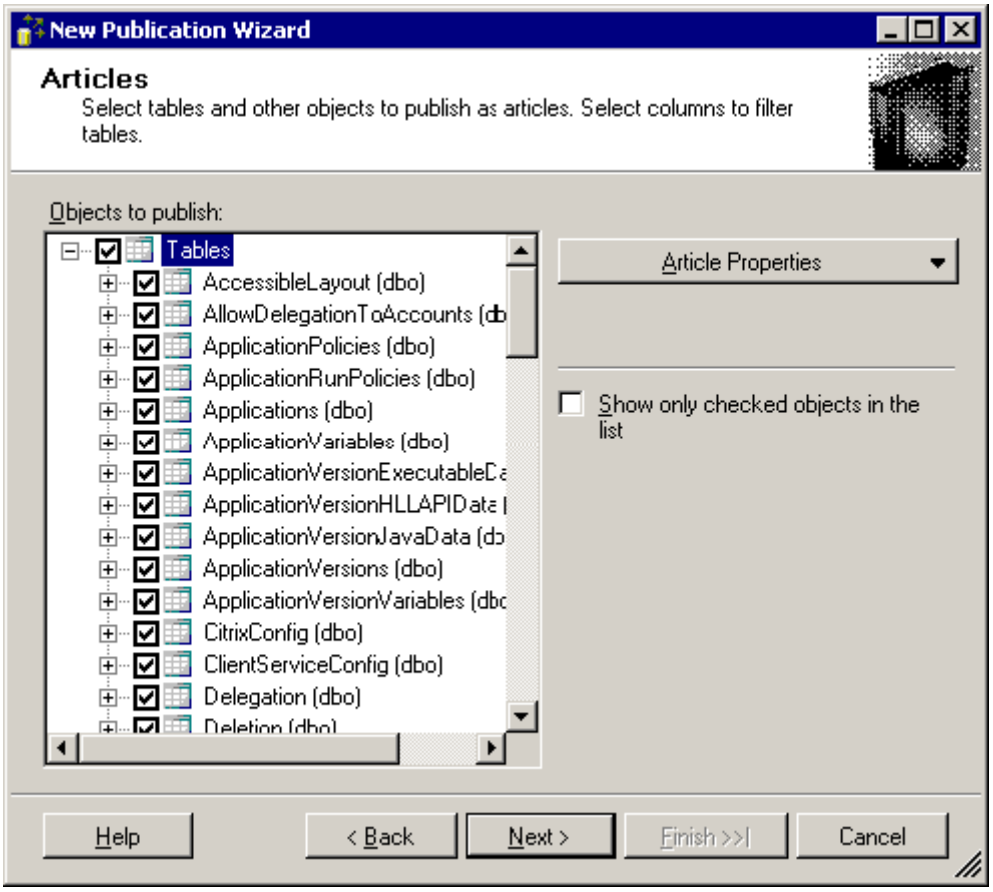
7. Enter the name of the of the share on which the snapshot must be created.

8. Click on next. The following page is displayed:



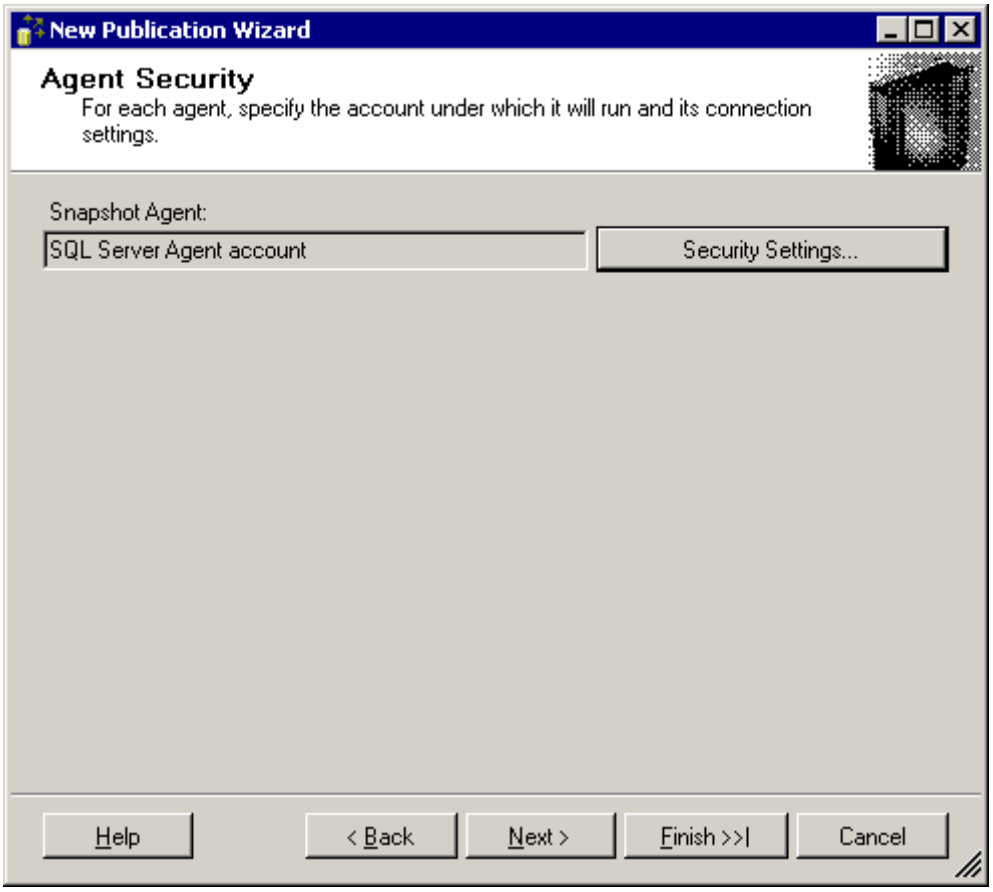
9. Select 'MSSQLSSO' as the database to replicate and click on next. This will display the publication type page.
10. Select 'Merge Publication' as the type of replication.

11. Click on next until the following page is displayed:



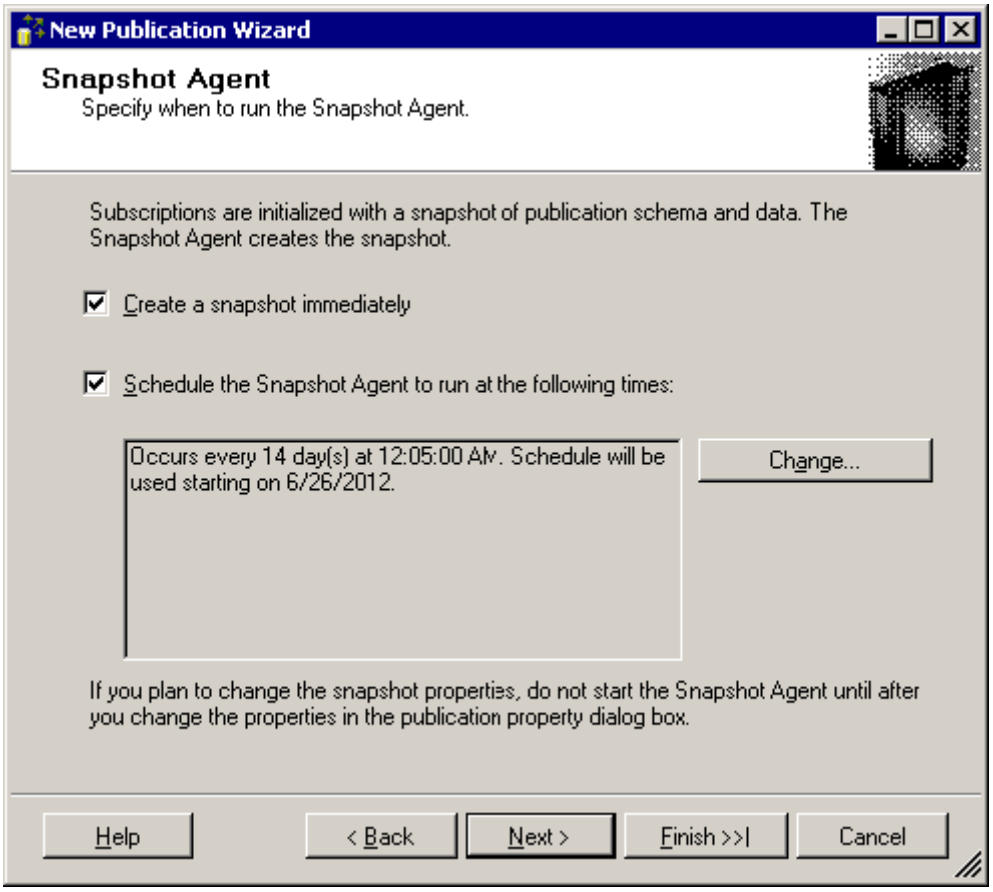
12. Check all tables as displayed in the above picture.

13. Click on next until the following page is displayed:

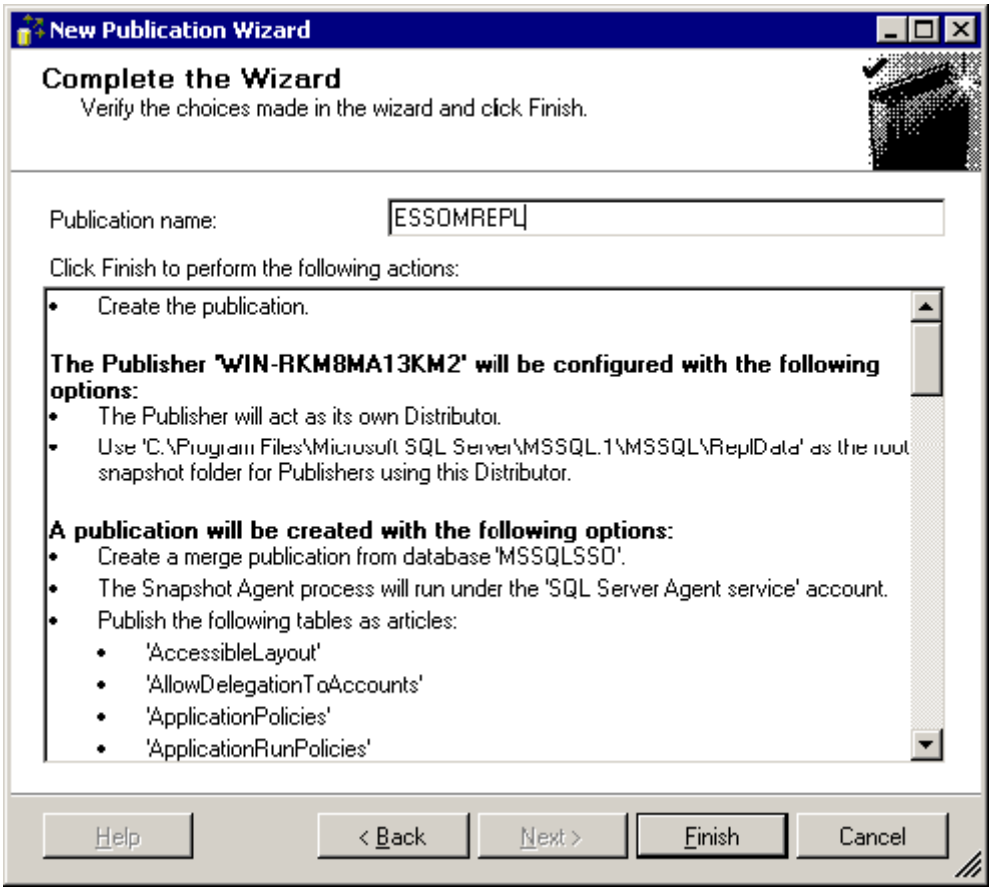


14. Click on 'Security Settings...'.
15. Select the 'Run under the Server Agent service account' option and click on 'OK'.

16. Click on next. The following page may be displayed:



17. Click on next until the 'Complete the Wizard' page is displayed:



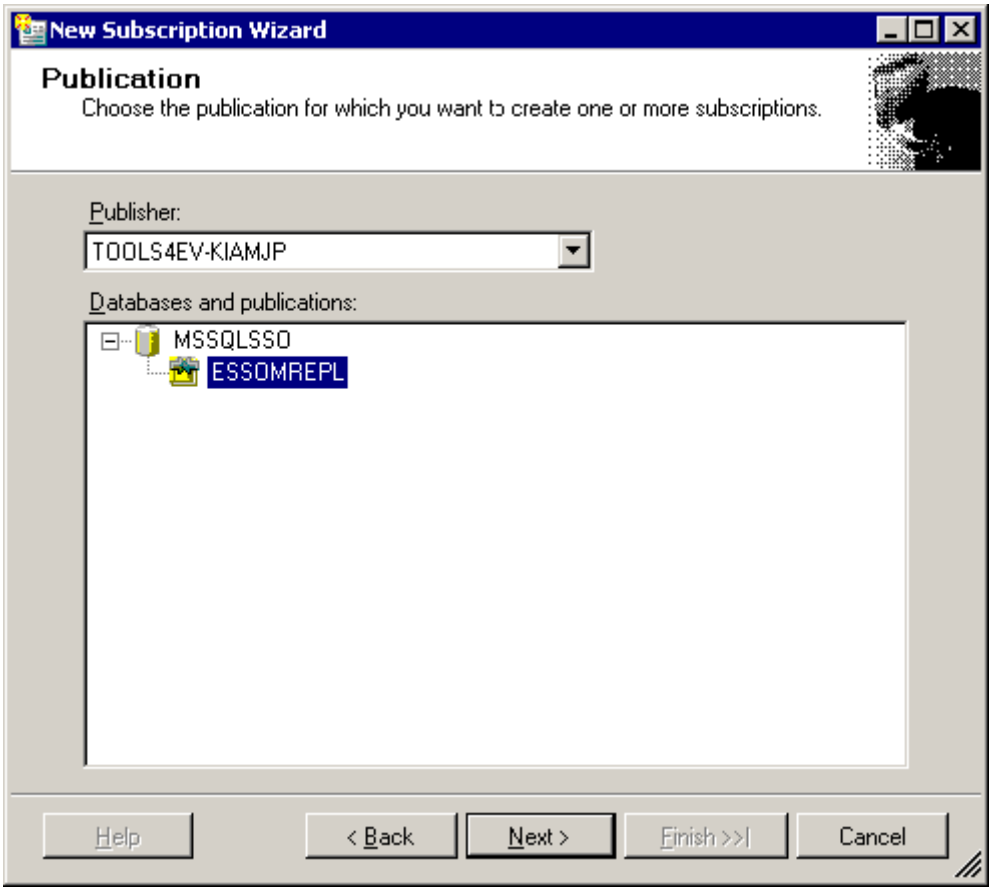
18. Enter a new name for the publication (In this example we used 'ESSOMREPL') and click on finish.

15.3.2. Subscription

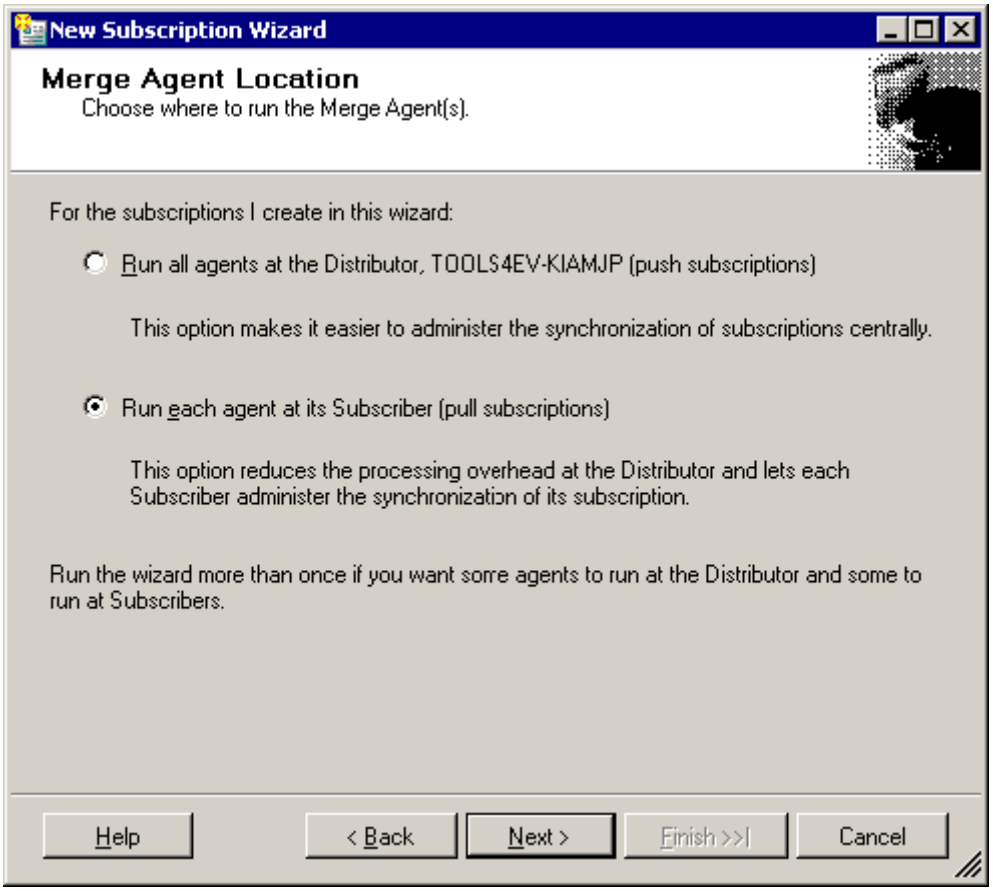
Once the publication is made, subscriptions to that publication can be made on all other SQL Servers.

1. Open SQL Server Management Studio
2. Go to Replication --> Local Subscriptions
3. Right click on Local Subscriptions and select 'new subscription...'.

4. Click on next. The following page is displayed:

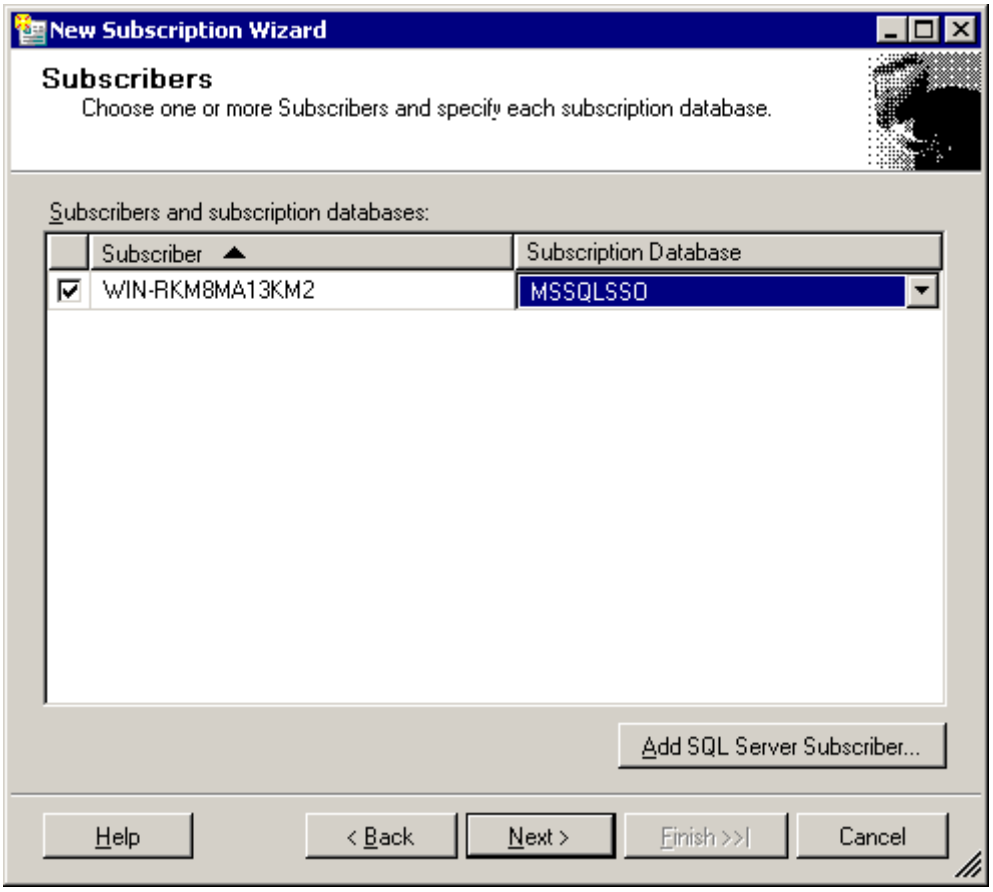


5. Select the server which is running the publication made in the previous chapter. Select the publication 'ESSOMREPL'. Click on next to display the following page:



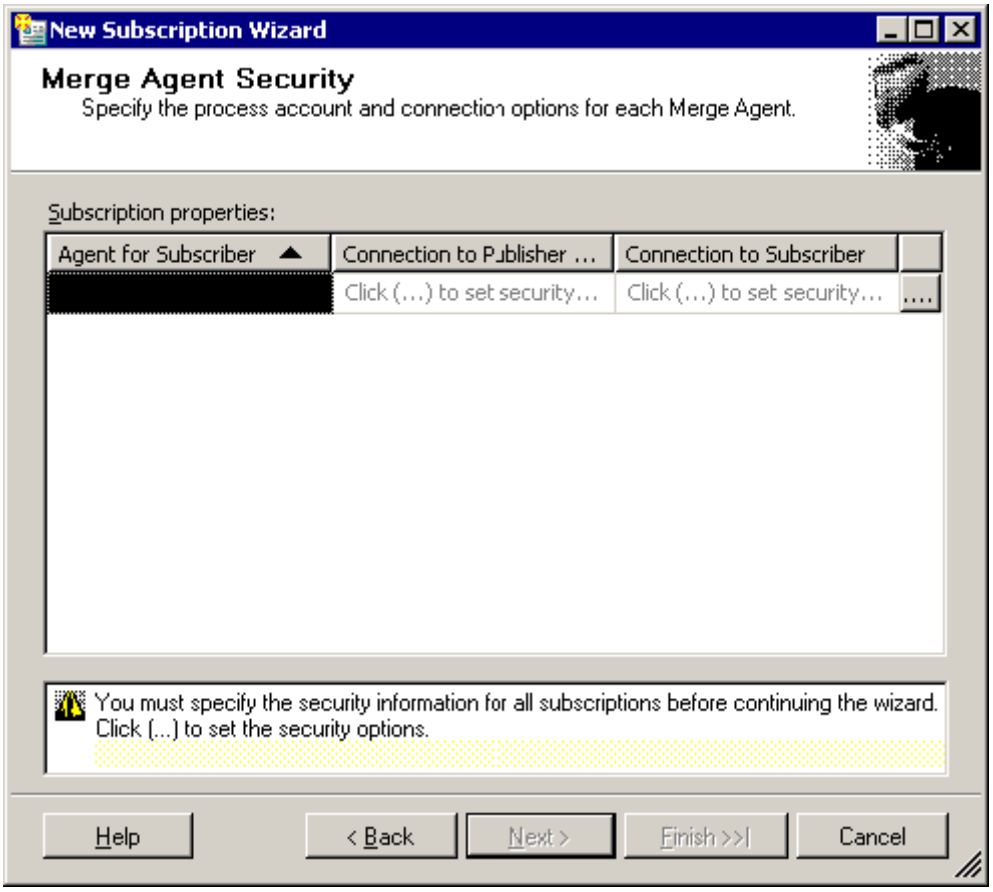
6. Select the option 'Run all agents at its Subscriber'.

7. Click on next. The following page is displayed:

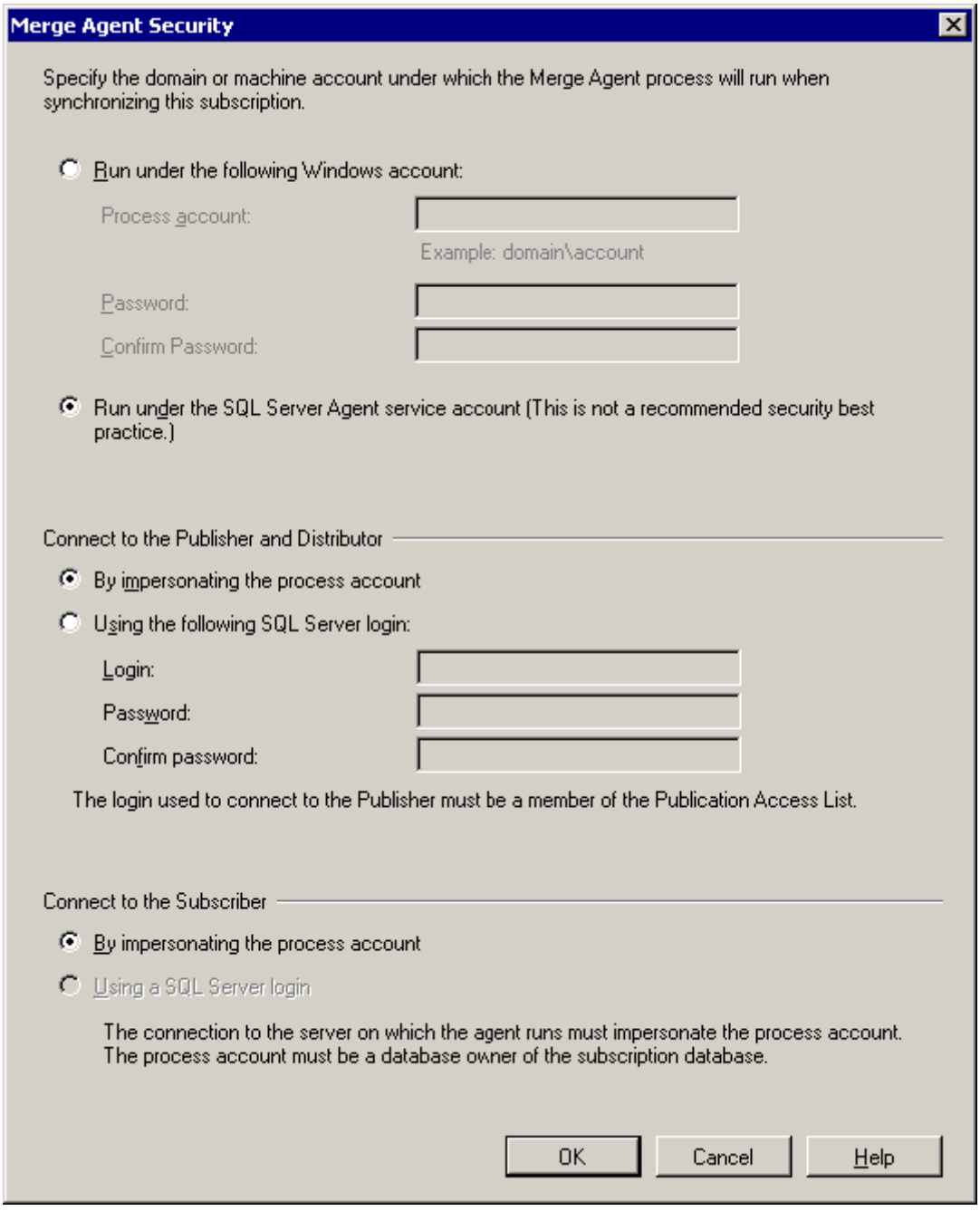


8. Select the server (Subscriber) that contains the created publication and select the correct Subscription Database ('MSSQLSSO')

9. Click on next. The following page is displayed:

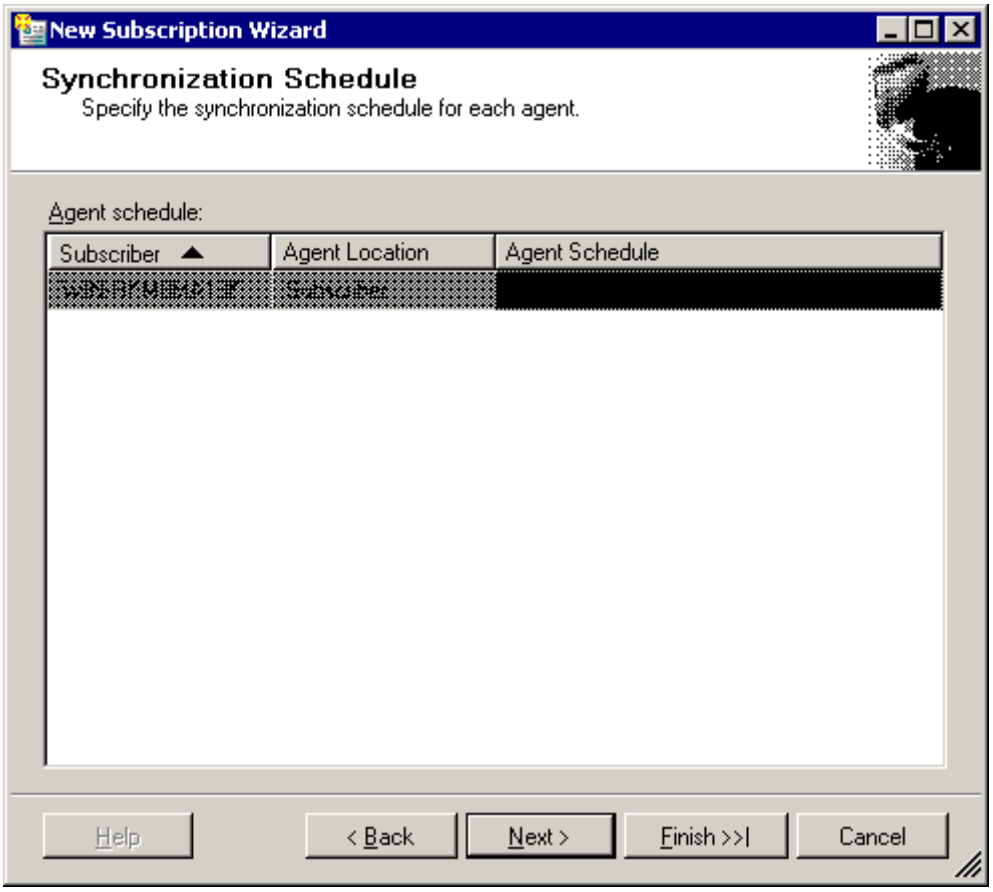


10. Click on the browse button. The following dialog is displayed:



11. Select the 'Run under the SQL Server Agent service account' option and click on OK.

12. Click on next until the following page is displayed:



13. Set the Agent Schedule to 'Run Continuously'.
14. Click on next until the 'Complete the Wizard' page is displayed.
15. Click on Finish.

16. Examples

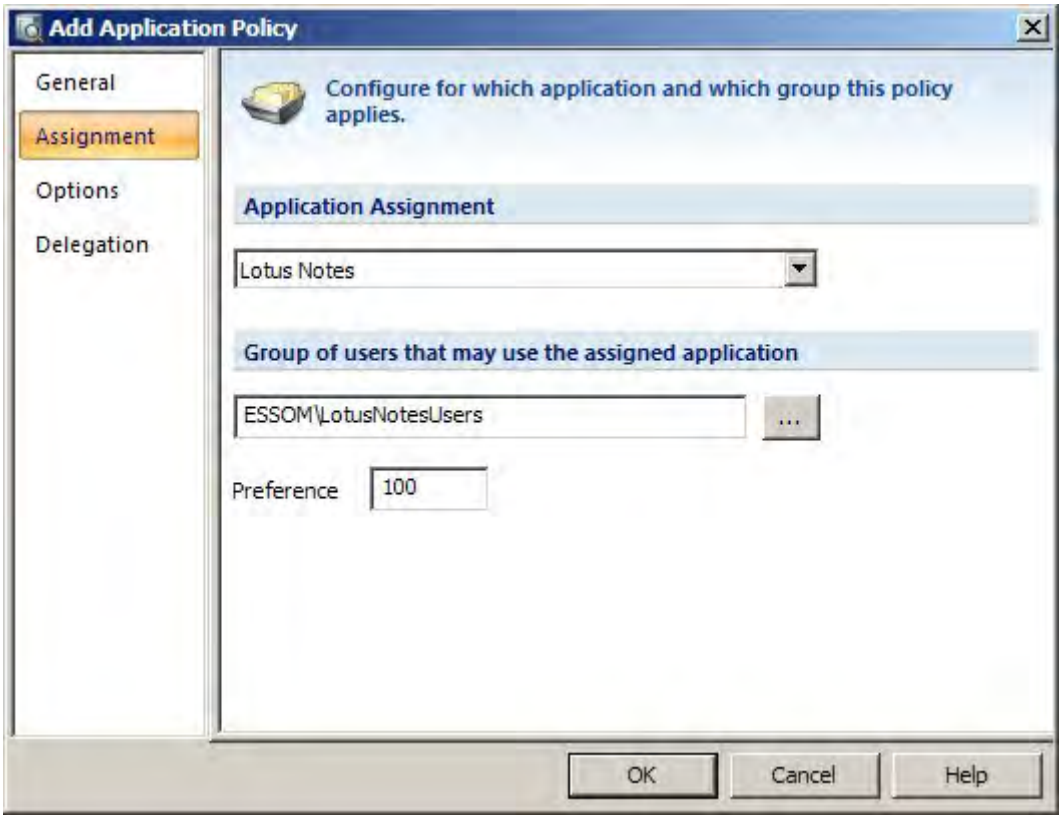
16.1. Importing and assigning an application to a user

This chapter describes how to import and assign an application to a group of users. This guide assumes that all of the E-SSOM software has been installed as described in the 'E-SSOM Installation Guide'.

1. Start the E-SSOM Admin Console
2. Select 'File --> Import --> Application...' from the main menu.
3. Browse to the application that you want to import and click on 'Open'. (E-SSOM is shipped with several applications that can be found by default in: 'C:\Program Files\Tools4ever\SSO\Admin Console\Applications'.)

4. Click on 'OK' to close the notification message.
5. Select 'Management --> Application Assignment...' from the main menu.
6. Click on 'Add' to add a new application assignment.
7. Enter the name of the new assignment and an optional description.

8. Click on the 'Assignment' tab:



9. Select the application that you imported in step 2.
10. Enter the group (or user) to which the application must be assigned.
11. Click on 'OK' to complete the assignment.

Test the assignment

1. Log in as a user that is a member of the specified group.
2. If not already running, start the E-SSO-M User Client.
3. Open the E-SSO-M User Client.
4. Select 'View --> Refresh All' from the main menu.
5. (Re-)Start the specified application.

16.2. Creating a win32 application definition using the default scripts

This chapter describes how to create an application definition using the default scripts called: 'Default - Login', 'Default - Bad Password' and 'Default - Change Password'.

Please note that this example assumes that the application that must be configured is installed on the same machine as the Admin Console and that the three default scripts are already imported.

1. Start the application that must be configured and go the the login window of the application.
2. Start the E-SSOM Admin Console.
3. Right-Click in the 'Applications' tree and select 'Add Application...'.

4. Enter the name of the new application and go to the 'Versions' tab.
5. Click on 'Add' to add a new application version.
6. Select the 'Windows Applications' application type and click on 'OK'.
7. Enter the name of the new application version and go to the 'Executable' tab.
8. Click on the target icon with the left mouse button (the Admin Console will disappear) and drag it to the application that must be configured while holding the left mouse button down.
9. Release the left mouse button when a window of the application had been selected. The Admin Console will reappear and the name of the executable will be displayed in the 'Executable' tab.

Adding the login event.

10. Go to the 'Events' tab and click on 'Add' to add a new event.
11. Select the 'Window Layout detection (default)' method and click on 'OK'.
12. Enter 'Login' as the name of this event and click on the 'Layout' tab.
13. Click on the target icon with the left mouse button (the Admin Console will disappear) and drag it to the **login window** of the application that must be configured while holding the left mouse button down.
14. Release the left mouse button when the correct window has been selected. The Admin Console will reappear.
15. Go to the 'Controls' tab.

The login script requires that three 'controls' are configured. The edit box in which the username must be entered (Variable %usernamecontrol%) , the edit box in which the password must be entered (Variable %passwordcontrol%) and the login button that must be pressed after entering the login credentials (Variable %loginbuttoncontrol%)

16. Click on 'Add' to select the username edit box.
17. Click on the target icon with the left mouse button (the Admin Console will disappear) and drag it to the edit box in which the username must be entered.
18. Release the left mouse button when the edit box is selected. Enter '%usernamecontrol%' in the 'Variable Name' edit box and click on 'OK'.
19. Repeat steps 16-18 for the password edit box and the login button.
20. Go to the 'Scripts' tab and select the 'Default - Login' script.
21. Click on 'OK' to close the 'Add Event' dialog.

Adding the bad password event.

22. Click on 'Add' to add a new event.
23. Select the 'Window Layout detection (default)' method and click on 'OK'.
24. Enter 'Bad Password' as the name of this event and click on the 'Layout' tab.
25. Click on the target icon with the left mouse button (the Admin Console will disappear) and drag it to the **bad password window** of the application that must be configured while holding the left mouse button down.
26. Release the left mouse button when the correct window has been selected. The Admin Console will reappear.
27. Go to the 'Controls' tab.

The bad password script requires that one 'control' is configured. The OK button that must be pressed to close the bad password message box (Variable %okbuttoncontrol%)

28. Click on 'Add' to select the ok button.

29. Click on the target icon with the left mouse button (the Admin Console will disappear) and drag it to the button that must be pressed.
30. Release the left mouse button when the button is selected. Enter '%okbuttoncontrol%' in the 'Variable Name' edit box and click on 'OK'.
31. Go to the 'Scripts' tab and select the 'Default - Bad Password' script.
32. Click on 'OK' to close the 'Add Event' dialog.

Adding the change password event.

33. Click on 'Add' to add a new event.
34. Select the 'Window Layout detection (default)' method and click on 'OK'.
35. Enter 'Change Password' as the name of this event and click on the 'Layout' tab.
36. Click on the target icon with the left mouse button (the Admin Console will disappear) and drag it to the **change password window** of the application that must be configured while holding the left mouse button down.
37. Release the left mouse button when the correct window has been selected. The Admin Console will reappear.
38. Go to the 'Controls' tab.

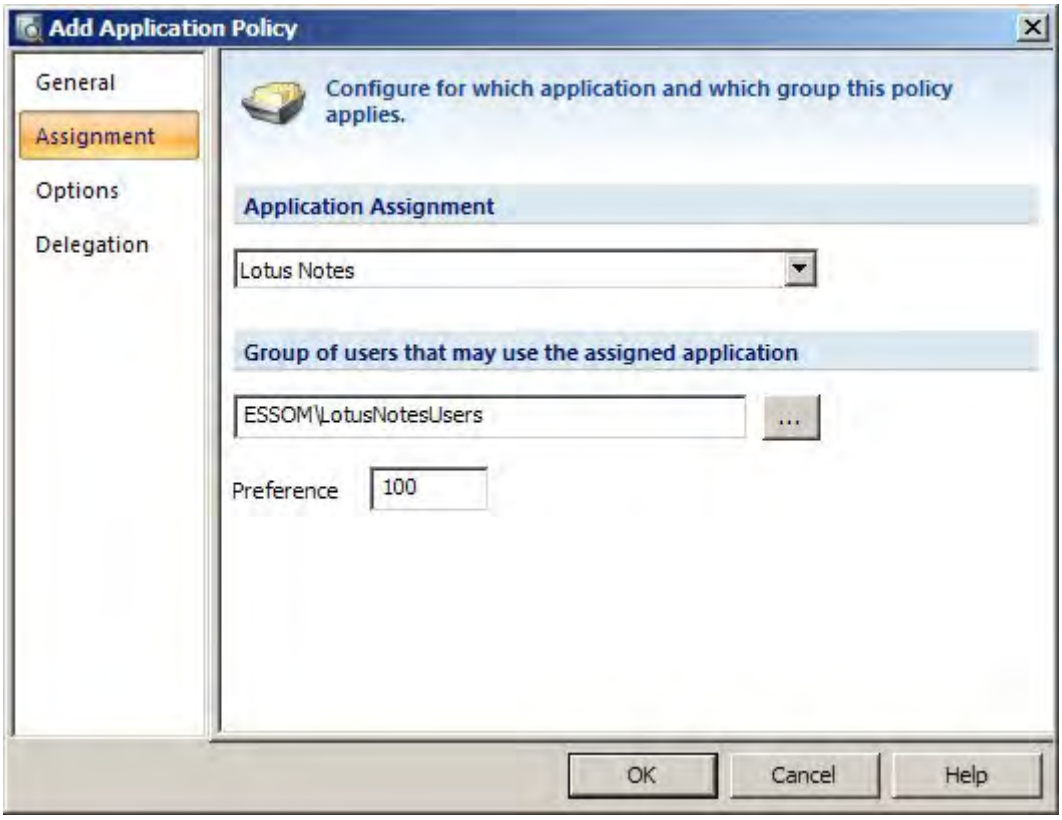
The change password script requires that four 'controls' are configured. The edit box in which the old password must be entered (Variable %oldpasswordcontrol%) , the edit box in which the new password must be entered (Variable %newpasswordcontrol%), the edit box in which the new password must be confirmed (%confirmpasswordcontroL%) and the button that must be pressed after entering the passwords. (Variable %okbuttoncontrol%)

39. Click on 'Add' to select the old password edit box.
40. Click on the target icon with the left mouse button (the Admin Console will disappear) and drag it to the edit box in which the old password must be entered.
41. Release the left mouse button when the edit box is selected. Enter '%oldpasswordcontrol%' in the 'Variable Name' edit box and click on 'OK'.
42. Repeat steps 39-41 for the other controls.
43. Go to the 'Scripts' tab and select the 'Default - Change Password' script.
44. Click on 'OK' to close the 'Add Event' dialog.
45. Click on 'OK' to close the 'Add Application Version' dialog.
46. Click on 'OK' to close the 'Add Application' dialog and store the new application definition in the database.

Assigning the application to one or more users

47. Select 'Management --> Application Assignment...' from the main menu.
48. Click on 'Add' to add a new application assignment.
49. Enter the name of the new assignment and an optional description.

50. Click on the 'Assignment' tab:



51. Select the application that you imported in step 2.
52. Enter the group (or user) to which the application must be assigned.
53. Click on 'OK' to complete the assignment.

17. E-SSOM Error Codes

E-SSOM may display errors from various sources of the operating system as well as internal errors. This chapter describes the error codes.

Win32 error codes (0-15999)
The description regarding Win32 error codes can be found at:
http://msdn.microsoft.com/en-us/library/windows/desktop/ms681381(v=vs.85).aspx

HResult error codes (codes starting with 0x800)
HResult codes can be context specific. The most common HResult error codes can be found at:
http://msdn.microsoft.com/en-us/library/windows/desktop/aa378137(v=vs.85).aspx

Internal E-SSOM error codes (-1 - -50)
-1 General Error
-2 Incorrect client/service version
-3 Operation cancelled
-4 Operation timed out
-5 Unknown archive version
-6 SID invalid
-7 Service unavailable
-8 SMTP communication failed
-9 License Expired
-10 License User Count exceeded
-11 License Application Count exceeded
-12 License Invalid
-13 Module not licensed
-14 Domain or OU not licensed
-15 Server not specified
-16 Service unreachable
-17 Incorrect type
-18 Incorrect size
-19 Pointer is NULL
-20 Error converting name
-21 Detection terminated
-22 License Smartcard Count exceeded
-23 PIN must change
-24 Card not valid now
-25 Already exists
-26 Not included
-27 Excluded
-28 PIN expired
-29 Connection blocked
-30 User does not have enough rights
-31 User has been explicitly been denied access
-32 Wrong user
-33 License key corrupt
-34 No data
-35 Too many recursions
-36 Conversion failed
-37 Error decrypting (decryption key is not correct)
-38 Service needs update
-39 Client needs update
-40 Divide by zero
-41 Delegation not allowed
-42 Service busy
-43 Client not running
-44 User policy not found
-45 Exception caught
-46 Data corruption

-47 Not enrolled
-48 PIN incorrect
-49 PIN does not match complexity rules
-50 Cached credentials not found

18. Index

A

Admin Console Overview • 2
Application Definitions • 3
Application Policies • 27
Application Version Types • 6
Authentication Management • 38

C

Citrix • 33
CLI / Telnet • 16
CLI Event • 17
Client Service Settings • 36
Configuration • 37
Configuring • 5, 26, 27, 30, 34
Creating a win32 application definition using the default scripts • 63

E

E-SSOM Anywhere • 42
E-SSOM AppInit Client • 41
E-SSOM Error Codes • 67
Examples • 62

F

Fast User Switching • 36
Follow Me • 38

H

High availability / Fail Over • 47
HLLAPI Event • 19
HLLAPI Telnet • 18
HTML - Internet Explorer / FireFox • 10

I

IIS 6 Configuration • 42
IIS 7 Configuration • 46
Importing and assigning an application to a user • 62
Introduction • 1, 40

J

Java • 20
Java Event • 21
Java Monitor Installation • 23

M

Managing Smartcard Assignments • 40
MSSQL Replication Configuration • 49
Multiple Central Services • 48

O

Overview • 3, 25, 27, 30, 34

P

Password Policies • 34
Process Monitoring • 40
Publication • 49

R

Reporting • 40
Requirements • 37, 38, 42

S

Scripts • 25
Smartcard Policies • 39
Subscription • 55

U

User Client Offline Mode • 47
User Policies • 30

W

Web Layout Event • 13
Web Page Event • 11
Win32 / x64 • 7
Win32 Window Layout Event • 8