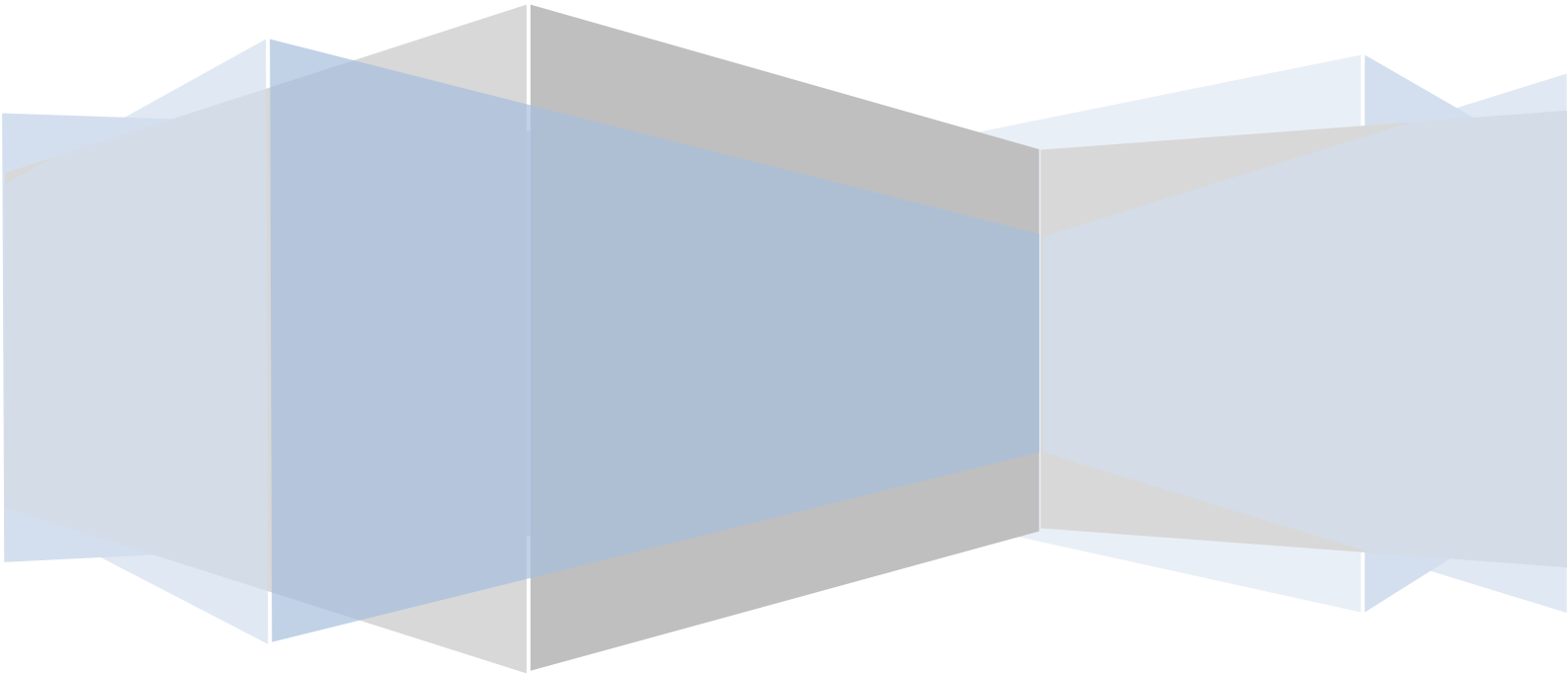
SSO Plug-in

Remote implementations

J System Solutions

http://www.javasystemsolutions.com

Version 3.2



Introduction.....3
Pre-requisite steps.....4
Transparent Windows authentication.....4
IIS front end.....4
SSO Plugin integrates with domain controller.....5

Introduction

This document provides an overview of pre-requisites for a client wishing to receive a remote installation. We would appreciate the client following the instructions in this document in order to ensure the installation is as smooth as possible.

If there are any questions, do not hesitate to contact JSS and remember that our professional services to implement the evaluation are provided at no cost.

Pre-requisite steps

The following will speed up the installation process regardless of the SSO implementation:

1. If you don't already have an account on the JSS website, go to the following URL and create one (select 'Sign up for downloads'):

http://www.javasystemsolutions.com/jss/contact

2. Download the latest stable version of the product.
3. Unpack the SSO Plugin zip file.
4. For Unix operating systems, copy the JSS AREA Plugin to the AR System server. The plugins are located in the installer/sso, under the relevant AR System server Operating System directory. Copy this file to the same directory as the arplugin file. For Windows operating systems, the installer will copy the AREA plugin to the AR System server.
5. Copy the Midtier SSO Plugin files to the server running the Midtier. In the zip file, there's a directory called mt. Copy this directory to the machine running the Midtier.
6. Discover how long it takes to restart the AR System server in the test/development environment. We will need to restart it during installation, so it's useful to know how long this process will take.

Transparent Windows authentication

If you're using a Windows network and you wish users to open up Internet Explorer (or Firefox) and access the Midtier without signing in, this section is relevant.

There are two ways to provide this service:

1. Using an IIS front end, in which case IIS must be able to perform Integrated Windows Authentication.
2. Using the SSO Plugin to integrate with the Domain Controller, in which case a special 'service account' must be created.

Please see the relevant pre-requisite steps below.

IIS front end

When using an IIS front end, it must be capable of performing Integrated Windows Authentication. JSS staff are happy to do this process during the remote installation however the steps are detailed below:

1. Right click on the 'Default website' in the IIS administration console, clicking 'Directory security', disable anonymous and enable Integrated Windows Authentication.
2. Restart IIS.

3. Open IE and navigate to http://host/iisstart.htm.
4. If you can view the iistart.htm page then IWA operated as expected. If the browser keeps prompting for authentication, and your browser is in the Local Intranet zone, the IIS server appears to have an issue performing IWA.
5. Typically, the issue with IIS is because no service principal name (SPN) exists in the Active Directory for the IIS instance and one needs to be present. **This is as per Microsoft design and is outside the bounds of SSO Plugin**. Therefore, ask the Active Directory admin to check the SPN exists, and if one does not, it can be added by running the following command on the Active Directory:

   setspn -A HTTP/hostname domain\computer (where hostname is the hostname of the computer/website, and domain\computer is the computer running IIS).

SSO Plugin integrates with domain controller

When integrating with the domain controller, a service account must be created. The service account must be a Computer Account and we've provided a script to automate this task. It is called set-service-account.cmd.

There are two protocols required by transparent Windows authentication, Kerberos and NTLM. While some organisations may be content with NTLM, the automated script will setup the Computer Account for both protocols.

The primary reason a script is required is because the Active Directory Users and Computers tool does not provide a control to change the password of a Computer Account, hence the recommended Microsoft technique is to use a script. Given we had to provide a script, we decided to automate some other processes, such as the creation of the Computer Account and the creation of service principal names (SPNs) required for setting up Kerberos.

In summary, the script will do everything required to set up an account in the AD to allow SSO Plugin to authenticate IE clients. If your AD administrator does not want to run the script then manual instructions are available in the installation manual (page 29 - “Manually creating a service account”).