iCM Single Sign On

Contents

Document revision: 1.1

iCM Single Sign On

iCM Single Sign On is handled by a set of 2 customisable scripts. One script to synchronise users with an external authentication provider, and another that handles authentication when users attempt to log in.

This implementation makes it possible to use most authentication providers. For the purpose of this document we will assume that the authentication provider is Microsoft Active Directory with LDAP.

Terminology

Single Sign On (SSO)

Single sign on is a term used to describe that users will log in to iCM using the same user name and password as their domain account.

iCM will authenticate users against an external authentication provider, but the iCM user still sees the iCM login screen and must enter a valid username and password.

Seamless Single Sign On (Seamless SSO)

Seamless SSO is the same as SSO, except that the logon process is deemed to be "seamless" because users are logged in to iCM automatically using their authenticated domain account. As a result users will not see the iCM login screen at all.

How to enable iCM SSO

1. Run the iCM autoconfig.
    a. On the "General Settings" tab enable "Use network authentication".
    b. Complete the autoconfig by clicking next until the last page and then click finish.
2. If your iCM installation is a cluster then repeat step 1 on every iCM server in the cluster.
3. Log in to iCM as the "admin" user.
4. Create iCM user groups and nominate them for synchronisation from Active Directory by checking the option for "network synchronisation" before you save each group.
5. Synchronise nominated iCM user groups with matching user groups against the Active Directory. This is done in a customisable script: */icm/custom/authenticategroup.cfm*
6. When a user logs in to iCM, use their credentials to authenticate with the external authentication provider and if successful they will be logged in to iCM. This is done in a customisable script: */icm/custom/authenticateuser.cfm*

Goss provides examples of both *authenticategroup.cfm* and *authenticateuser.cfm* in */icm/custom/EXAMPLES/* which should fit most Microsoft Active Directory set ups.

See sections; iCM User Group Synchronisation and iCM User Login Process for more details on how this works.

How to deploy the example SSO scripts

1. Copy the following files from <path to>/icm/custom/EXAMPLES/ <path to>/icm/custom/
    a. authenticateuser.cfm
    b. authenticategroup.cfm
    c. ldapFunctions.cfm
    d. ldapConfig.cfm
2. Edit <path to>/icm/custom/ldapConfig.cfm and configure the settings for your environment.

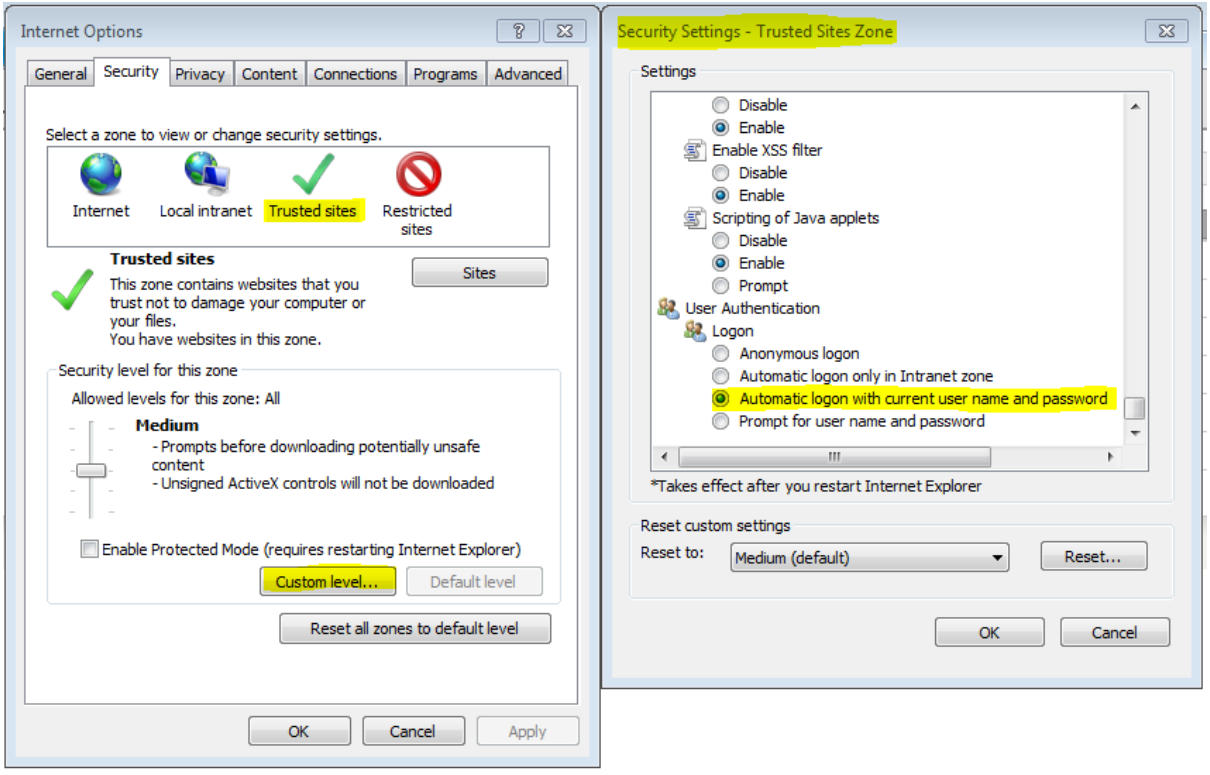
Please note that if your iCM installation is a cluster then the /icm/custom/ directory should be shared across the cluster, therefore there is no need to deploy those files to each cluster node.

How to enable *seamless* single sign on

The *seamless* part is not an iCM feature; it is domain/ browser configuration. Once single sign on is configured and working you can set up your browser to pass your credentials to the web server.

For *seamless* single sign on to work there are several pre-requisites, as follows;

1. Your web server must be joined to the domain against which you need to authenticate.
2. Your iCM users must on the same domain as the web server.
3. Your iCM users must be using internet explorer.
4. Your iCM user's internet explorer settings must be configured to pass the username and password to the web server. You can achieve this by putting the URL of your website/intranet in the "local intranet zone" of internet explorer, or change the security level settings for the appropriate zone to allow "Automatic logon with current user name and password".



iCM SSO User Group Synchronisation

1. An iCM administrator must nominate some iCM user groups for network authentication. This is done by logging in to iCM, editing an iCM user group and selecting the "Allow network synchronisation" option.
2. iCM permissions can be assigned to the iCM groups you created in order to grant those permissions to all members of that group.
3. iCM synchronises nominated iCM user groups with Active Directory user groups that have exactly the same group name.
4. The group synchronisation is performed by a scheduled task in iCM called "Authenticate groups" which calls to the customisable script: */icm/custom/authenticategroup.cfm*. This task should be scheduled to run several times a day (or as frequently as you see fit) so the iCM groups stay in sync with the authentication provider. The scheduled task works as follows;
    a. The active directory is queried for each nominated iCM user group.
    b. If a group with that name exists in the active directory then each member of that group (domain user) will be created as a user in iCM and then added to that group in iCM.
    c. If the user already exists in iCM then it will be added to the iCM group with no changes to the user account itself.
    d. If a user is no longer a member of any of the nominated group(s) in the Active Directory, the user will be removed from the corresponding group(s) in iCM.
    e. Once all nominated iCM groups have been synchronised then iCM users that are left orphaned with no group membership at all (nominated for SSO or not) will be deleted. To prevent users being deleted from iCM you can add them to any iCM group.
5. The iCM scheduled task "Authenticate groups" can be run manually at any time by iCM users with the correct permissions.

iCM SSO User Authentication

1. The user domainname\username and password are passed to iCM by the browser and used to query the Active Directory.
2. The Active Directory is searched to see if the user exists.
3. If the user exists in Active Directory then iCM attempts to authenticate with the Active Directory using that user's credentials.
4. If iCM successfully authenticated with the Active Directory AND the user exists in iCM then the user is logged in to iCM.
5. If this authentication fails, the user is presented with the iCM log in screen and the user can attempt to log in manually.
6. If the user has the option for "Allow iCM authentication" set in their user profile in iCM then the user is authenticated against the iCM database.
7. If iCM successfully authenticates then the user is logged in to iCM.

Single Sign On flow chart

Note that should authentication fail, then the user is presented with the iCM login screen. If the user has the option “Allow iCM authentication” set in their user profile in iCM then the user can enter their username and password and be authenticated against the iCM database.