HP Systems Insight Manager 5.0 and HP OpenView Select Access

Configuring HP Systems Insight Manager 5.0 and HP OpenView Select Access to Use the Same Windows User Groups

Summary

HP Systems Insight Manager (HP SIM) 5.0 and HP OpenView Select Access can use the same Windows user groups for password-based authentication to HP SIM and other HP OpenView Select Access-protected resources. Access can then be managed by membership in or removal from the Windows user group.

HP Systems Insight Manager

Configuration

In HP SIM, add the Windows user group. Sign in as a full-configuration-rights user and from the menu select **Options→Security→Users and Authorizations**. From the **Users** tab, click **New Group**. Enter the desired Windows domain and user group, configure the desired settings, and click **OK**. Members of the user group can sign into HP SIM and have the rights and authorizations configured in HP SIM.

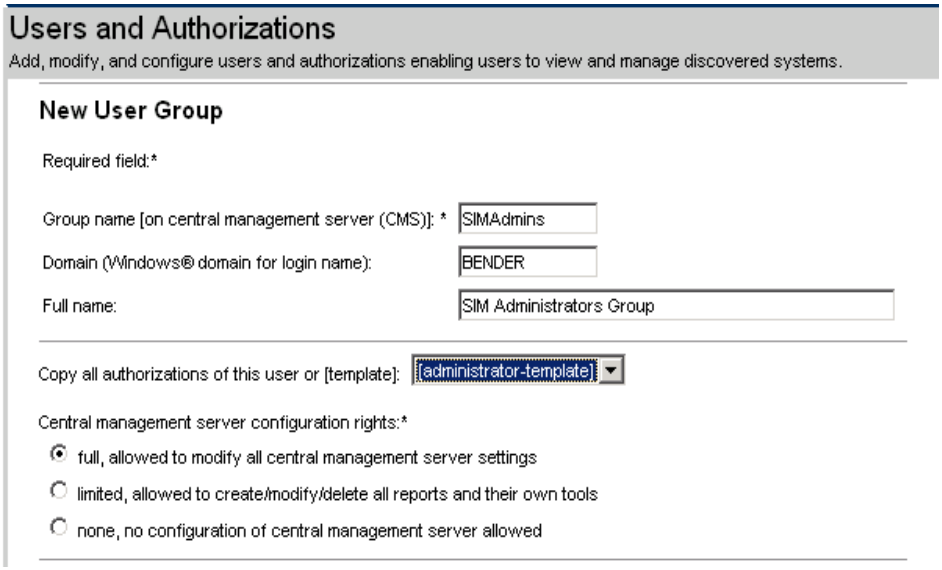

Figure 1: SIM New User Group

HP OpenView Select Access

Note: For more information on these topics, refer to the *HP OpenView Select Access Policy Builder Guide.*

Note: HP OpenView Select Access 6.1 refers to users as identities.

Configuration

In HP OpenView Select Access, add a **User Location** for the same Windows domain used for HP SIM. Log into the HP OpenView Select Access Policy Builder. From the menu, select **Tools→User Location Configuration** to add a user location in the **User location name** field. Specify the Windows domain controller as the directory server. Port 389 is the standard port for LDAP, and 636 is the standard port for LDAP using SSL that ensures the communication is encrypted over the network.

Specify an account and password that can read and write data on the directory server, such as a domain administrator account. Click **Browse** to locate the user tree on the directory server. For example, cn=users, dc=hp, dc=com.

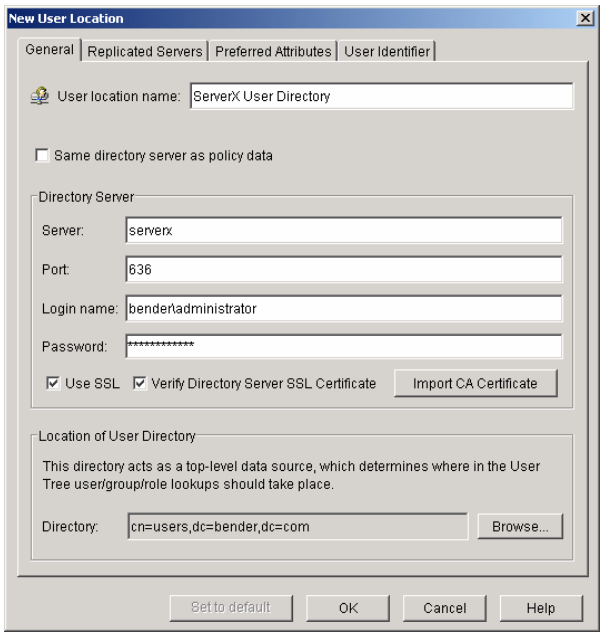

Figure 2: HP OpenView Select Access New User Location

After creating the user location for the Windows domain, it can be added to an Authentication Server in HP OpenView Select Access by selecting **Tools→Authentication Servers**. Select either **Password** or **NTLM** as the authentication method. You can use **Known Users** as the location for user lookups, or a specific user location.

The Authentication Server can now be used for authentication with other HP OpenView Select Access-protected products (not HP SIM) specifying the same Windows user group used for HP SIM. As an example, consider Microsoft Internet Information Services (IIS), for which HP OpenView Select Access provides an enforcer plug-in. After configuring a resource for the IIS server, you could enable **Select ID** using the Authentication Server created above. Using the Policy Matrix, you can then create a policy to enable access to the IIS resource for the Windows user group (available under the user location created for the Windows domain.) Because policies are inherited by default, all members of the user group inherit the allow access policy.

Creating New Users and Groups

Using the HP OpenView Select Access Policy Builder, you can create or modify users and user groups. These users and user groups are available for use by HP SIM because these changes are made directly on the directory server, for example, the Windows domain.

Note: To create and manage user passwords on the directory server (Microsoft Active Directory), SSL must be enabled for the user location.

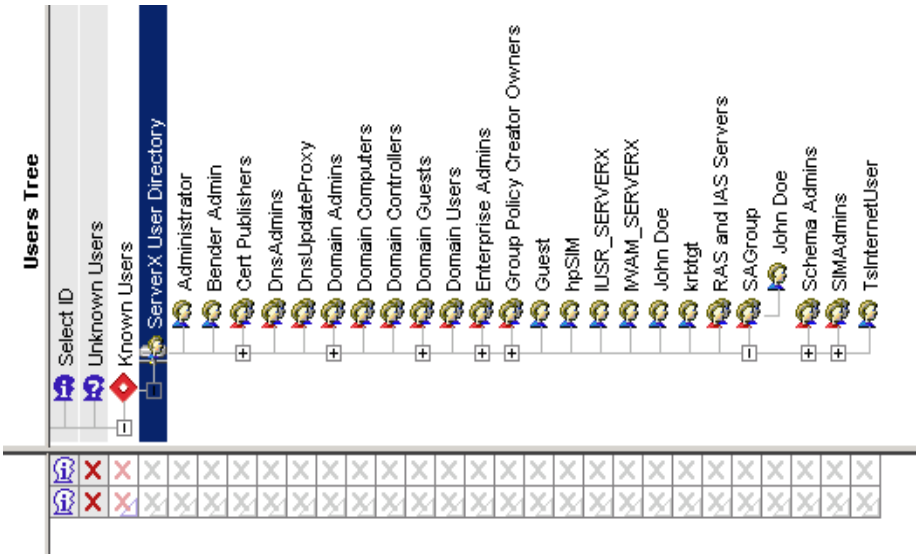

Figure 3: HP OpenView Select Access Users Tree

To create a new user, right-click a user location in the **User Tree**, and select **New→User** To create a new user group, select **New→Group**. Right-click the group or user in the **Users Tree** and select **Properties** to add users to a group. Use the **Group Membership** tab to specify desired group memberships.

Note: Roles created in the Policy Builder cannot be used by HP SIM.

408295-001/September 2005