Security – Group Level Domain Synchronization

APPLICATIONS NOTE

April 2010

Description: Guide to integrating specific groups of users in an NT Domain into ICONICS Security Server.
OS Requirement: Win 2000, XP Pro, Server 2003, Vista, Server 2008, Windows 7
General Requirement: Installation of either GENESIS32 or BizViz version 9.x. You should also be in an NT domain on a Windows Server operating System (NT 4.0 or higher). We recommend that you have some knowledge about the Windows NT system administration, access rights, and tools.

Introduction

Since the release of version 8.0, the ICONICS Security Server has the ability to synchronize users and groups with Windows NT Security by simply specifying a domain. The Security Server can then import all of the users and groups and which allows you to apply ICONICS security features on a user or group level. The Security Server also synchronizes periodically with the NT domain to detect any changes in user or group membership. While an excellent solution for linking ICONICS users with existing NT users, synchronizing with a domain can become cumbersome when dealing with very large domains, possibly with thousands of users. To ease the strain of large domains, ICONICS has introduced group-specified NT Domain synchronization.

The idea behind group-specified integrated NT security is to have a specific group in the domain set-aside only for users that will be involved in operations with ICONICS software. In other words, one NT domain group should contain a superset of all of the domain users that should be imported into the ICONICS Security Server. In the ICONICS Security Server, the user can then specify this particular group, and the Security Server will add only these users, and the collection of all groups occupied by this set of users. This limited set of domain users, along with their group membership is initially and periodically synchronized with the domain, just as the set of all users and groups is synchronized when no group is specified. The difference here is that we are dealing with a smaller set of users, rather than the whole list. This should greatly speed up synchronization with the domain.

Specifying a Group for Security

1. Launch the ICONICS Security Server by going to Start → Programs → ICONICS Tools → Security Configurator
2. Select File → New
3. In the Security Server dialog, Select Advanced Mode.
4. Check to Use integrated NT Security
5. select the Domain radio button and enter the name of your Domain
6. Check the option to Specify Group and enter the name of the Group from which you would like to import the users.

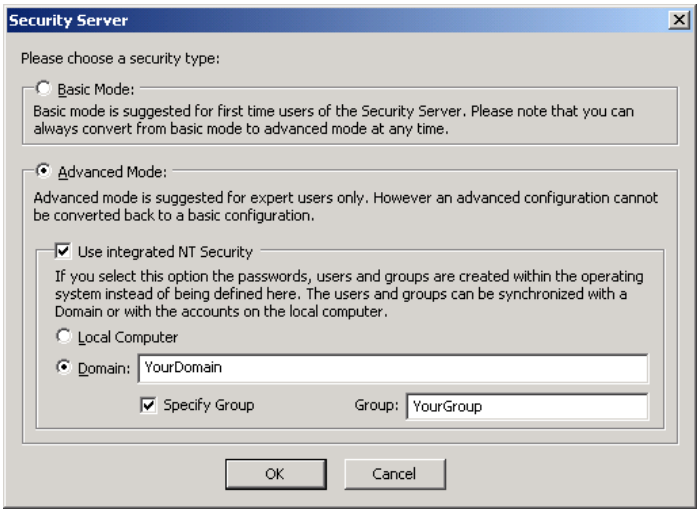

Figure 1 - Using Advanced Mode to Import Users from A Domain Group

7. Click on "OK"
8. The Save As dialog will appear asking you to save the security configuration. Give the configuration a name and a location and click on "Save".
9. You should see all of the users in the specified Group in the right-hand pane and the groups to which these users belong to in the left-hand pane.
10. You can now edit ICONICS permissions for the users or user groups as you would normally.

Functionality Explained

If the Specify Group option in step 6 is left unchecked, then NT synchronization will continue across the entire specified domain. If, however, the checkbox is selected and a valid group is specified then synchronization will continue on a group level. All of the users in the specified group will be added to the Security Server along with the cumulative set of all groups occupied by the list of users.

As an example, assume that user A is in groups Group1 and Group2, user B is in Group1, and user C is only in Group2. If you choose to synchronize your security configuration with Group1 you will get all of the users in Group1 (A and B). You will also get Group2 since user A is also a member of Group2. You will not, however, get user C. You will never get users who are not members of the group you are synchronizing with.

All associations between this subset of users and groups will persist in the Security Server as they do in the domain. If an invalid group is specified, the user is warned with an appropriate message and required to supply a valid existing group before a new Security configuration file can be created.

Copyright 2010 ICONICS, Inc.