ScareCrow Message Board Permission System

Document Scope

It is the intention of this document to provide initial understanding of the permission system utilized in the ScareCrow Message Board software. The system can be extremely flexible and powerful, but it can also be dangerous and cumbersome if used without a knowledge of it.

Applicability

This document is accurate through ScareCrow Message Board version 2.12. It should remain applicable for all versions of ScareCrow in the 2.x life cycle.

Background: Binary Operations

To understand the way the permissions system works in detail, the reader must first have a tenuous grasp on binary operations. For our purposes, suffice it to say that *binary* means either 1 or 0. What one must then understand, to a small degree, are the operations that the software performs on binary digits.

First of all, the permissions for ScareCrow are stored as a string of 1's (for a permission that is allowed) and 0's (for a permission that is not explicitly granted). A sample portion of one such string may be the following:

```
00001101
```

There are two basic operations that ScareCrow performs on these strings. The first is called an **AND**. What it means, in particular, is that for the final answer to have a 1

in a specific place, two ones must be present in that position. For example:

String 1: 00001101

String 2: 01100101

If an **AND** were performed on these two strings of binary digits, it would line up the positions and check if the same "place" (think decimal places) has a one in both String 1 and String 2. Example:

String 1: 00001101
String 2: 01100101

FINAL: 00000101

As one can see, only the places in which a 1 was present in both String 1 and String 2 contain a 1 in the final string.

The second operation that is performed on binary strings is the **OR** operation. Similar to **AND**, the **OR** operation has a 1 in the final string if a one is present in String 1 **OR** String 2, or if it is present in both. Using the same strings from above, would arrive at a much different answer:

String 1: 00001101
String 2: 01100101

FINAL: 01101101

Obviously, the two are very different outcomes.

How ScareCrow Uses Binary Operations

ScareCrow has many different sets of permissions. First of all, every single user has their own set of permissions and denies. These are stored as two separate strings of 1's and 0's. Additionally, every group that a member belongs to affects their "effective permissions" -- the ultimate deciding factor in what they can and can not do.

For each group that a user belongs to, ScareCrow **OR**'s the strings together. When that is complete, the user's individual permissions are **OR**'d in. This has the effect of ensuring that if a permission is granted in ANY group the user belongs to, or for that user individually, that they initially have access to the feature. The result of these OR operations will be referred to as the preliminary permissions.

However, before the effective permissions are arrived at, one more step must be done. The denies string for each group is inverted; that is, a deny is stored as a "1" in the file, but it is made a "0" before it is used. When that is complete, the software **AND**'s each set of denies for every group that the user belongs to against the preliminary permissions. When that is complete, the user's individual denies are **AND**'d in. These operations have the effect that if a user is denied a permission by *any group s/he belongs to* or *on their individual account*, that they are **denied** that permission. A deny—anywhere—takes precedence over any number of allows.

What Does All Of This Mean To Me?

The way the message board deals with permissions is an extremely important concept. The most important lessons you should glean from this tutorial is that a deny overrides any number of allows and that the groups a user belongs to have a tremendous effect on their permissions. Therefore, it is *not recommended* to include denies in a group configuration unless the group is meant as a punishment of some sort. If the group does not need access to a feature, mark "Not Set" for the permission rather than deny. Remember: You can *not override a deny* in individual permissions.

On the other hand, you *can* override allowed permissions on a per-user basis, either to give something to them or to deny it. It is recommend that you apply any

restrictions to a user's account directly, rather to a user group.

How Does "Not Set" Factor In?

ScareCrow employs an implicit deny system. What that means is that if a user is not explicitly allowed a permission, it is assumed they can not use it—even if it is not explicitly denied, either. What that means is that "Not Set" is essentially a buffer. If the permission is "Not Set" for every group the user belongs to and their individual permissions, they can not use the feature. However, no matter how many "Not Set"'s may be on a permission for a user (through their account and groups), a single allow will permit the user to give the feature.

"Not Set" is essentially meant to be used for groups, where the group itself may have nothing to do with permissions, but only organization. For instance, if you created a group called "Posting Gods" which users were automatically put into at 1,500 posts, you may want to mark every permission for that group as "Not Set." That is to say, whether or not a user belongs to that group has no effect on their level of power. (It may, for instance, be used to determine access to a forum.)

The best policy is that if you're not sure if you should mark a permission "Not Set" or "Denied," mark it "Not Set."

Conclusions and Important Concepts

- A deny will **always override any allows** on a permission. One single deny in any group a user belongs to, or on their individual permissions, automatically denies the permission for that user regardless of whether or not they are allowed it elsewhere.

- If you are unsure if you should "Deny" a permission or mark it as "Not Set," "Not Set" is the better choice.
- It is recommended that denies not be used on the group level. It is much more effective and expandable to issue all of your denies of a per-user basis.
- Think of a deny as "no way, no how." It is meant to ensure that user *does not ever* have access to that specific feature. On the other hand, "Not Set" can be thought of as "we'll see later." If "Not Set" is the only setting for a permission for a user, they ultimately cannot use it. However, if there are no denies, and at least one allow, "Not Set" is overridden by the allows.
- ScareCrow's permissions system is an **implicit deny**. That is, if the user is not explicitly given access to a feature, through a group's permissions or the user's individual permissions, they will not end up with access to it.
- If it helps you to think of the permissions as a hierarchy, it would be as follows: Not Set -> Allow -> Deny. "Deny" takes precedence over both "Allow" and "Not Set." "Allow" takes precedence over "Not Set." "Not Set" takes no precedence (but see the "implicit deny" explanation above.)
- Whenever you upgrade your version of ScareCrow, be sure to check for new permissions and set them for each group you have created. It is very important that these permissions be set, even if you only set them to "Not Set." Also, you will want to upgrade your user accounts to the reflect the new permissions. A utility is available to aid you that will set all new permissions to "Not Set." It can be found from the ScareCrow Message Board Homepage at http://scarecrow.sourceforge.net.

Hopefully this guide has helped to explain our permission system better, and that it helps you to get the most out of your message board software. Thank you for choosing ScareCrow!