Link : “ http://docs2x.smartfoxserver.com/AdvancedTopics/privilege-manager ”

**» Trình quản lý đặc quyền người dùng**

Một yêu cầu phổ biến trong các ứng dụng trực tuyến là cung cấp một tập hợp các quyền tùy chỉnh cho các loại người dùng khác nhau. Các trò chơi trực tuyến điển hình có thể xử lý người dùng khách, người dùng đã đăng ký và có thể là người dùng cao cấp. Việc có một hồ sơ cho người kiểm duyệt và/hoặc quản trị viên trang cũng khá phổ biến.

**SmartFoxServer 2X** cung cấp Trình quản lý đặc quyền trong mỗi Vùng có thể được tùy chỉnh để hạn chế tương tác với máy chủ. Mỗi hồ sơ quyền có thể đặt danh sách các lệnh gọi API bị từ chối cho mỗi người dùng từ một danh mục cụ thể. Ví dụ: chúng tôi có thể cấm tạo Phòng và Biến phòng cho người dùng khách và chỉ cho phép chúng đối với người dùng đã đăng ký. Tin nhắn của Người điều hành và Quản trị viên có thể bị từ chối đối với mọi người ngoại trừ hai danh mục đặc quyền đó, v.v.

Mỗi hồ sơ trong Trình quản lý quyền được xác định bằng một số duy nhất. Các ID này có thể được gán tự do, tuy nhiên **4 ID đầu tiên được dành riêng** và có ý nghĩa đặc biệt đối với hệ thống:

* **Id == 0** : Người dùng khách
* **Id == 1** : Người dùng đã đăng ký
* **Id == 2** : Người dùng điều hành
* **Id == 3** : Người dùng quản trị viên

Không có cài đặt mặc định nào được cung cấp cho mỗi cấu hình này. Nhà phát triển được tự do tùy chỉnh các quyền này theo ý thích của mình. Chúng ta chỉ cần lưu ý rằng bốn ID đó luôn được nhận dạng trong hệ thống như trong danh sách trên. Ví dụ: nếu bạn đang sử dụng mã này trong mã của mình:

C# JS AS3

[**?**](http://docs2x.smartfoxserver.com/AdvancedTopics/privilege-manager)

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | User kermit = sfs.UserManager.GetUserByName("KermitTheFrog");    **if** (kermit.IsModerator())  {      // Allow some special action here...  } |

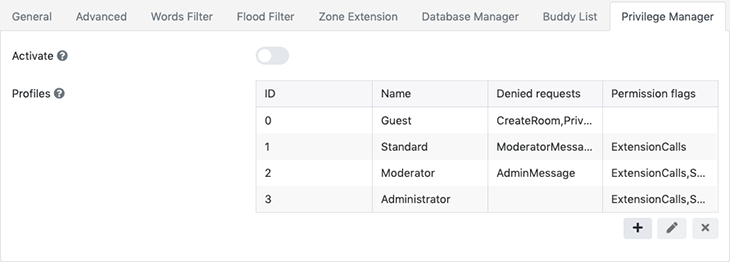
Trong nội bộ, API sẽ thực sự kiểm tra **profileId == 2 đó** .

Bạn cũng có thể tự do thêm bất kỳ số lượng cấu hình bổ sung nào và hoàn toàn bỏ qua những cấu hình mặc định mà chúng tôi đã đề cập.

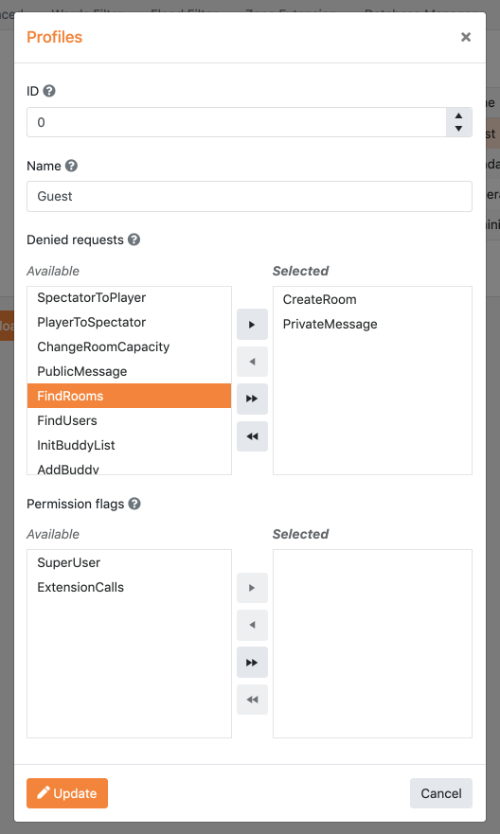
**LƯU Ý**   
ID cấu hình được truyền dưới dạng số nguyên ngắn (16 bit), vì vậy điều này có nghĩa là giới hạn lý thuyết là 2^16 cấu hình quyền đối với mỗi Vùng.

**» Cách cấu hình hồ sơ quyền**

Cấu hình các cấu hình quyền là một hoạt động rất đơn giản. Bạn chỉ cần chạy **AdminTool** , khởi động mô-đun **Zone Configurator** và chọn Zone mà bạn muốn chỉnh sửa quyền. Dưới **Privilege Manager** tab , bạn sẽ tìm thấy bốn cấu hình tiêu chuẩn:



Bạn sẽ có thể chỉnh sửa bất kỳ cái nào trong số này hoặc thêm cái mới:



Danh sách kép sẽ cho phép bạn thêm và xóa bất kỳ yêu cầu nào khỏi danh sách bị từ chối. Ở phần dưới của hộp thoại, bạn sẽ có thể gán hai cờ đặc biệt khác:

* **ExtensionCalls** : kích hoạt quyền truy cập vào bất kỳ Tiện ích mở rộng nào trong Vùng; khi tắt, người dùng có cấu hình đã chọn sẽ không thể sử dụng Tiện ích mở rộng.
* **SuperUser** : khi được bật, nó cho phép người dùng có cấu hình đã chọn sử dụng các chức năng của Người điều hành/Quản trị viên như đá, cấm và gửi tin nhắn mod/quản trị viên.

**» Cách sử dụng hồ sơ quyền**

Chỉ định Hồ sơ quyền thích hợp cho Người dùng cụ thể yêu cầu logic đăng nhập tùy chỉnh. Thông thường , nhà phát triển sẽ quản lý dữ liệu người dùng trong cơ sở dữ liệu hoặc nguồn dữ liệu tương tự. Tại thời điểm đăng nhập, Tiện ích mở rộng của bạn sẽ có thể kiểm tra thông tin đăng nhập của người dùng và cuối cùng đặt Id quyền phù hợp sau khi khách hàng cuối cùng đã đăng nhập vào hệ thống.

Quy trình mà chúng tôi đề xuất là như sau (để biết thêm thông tin , hãy kiểm tra **[Cách đăng nhập tùy chỉnh](http://docs2x.smartfoxserver.com/GettingStarted/howtos" \l "item3)** ):

* Trong phương thức mở rộng **init ( ) của bạn, hãy** đăng ký sự kiện máy chủ **USER\_LOGIN** .
* Khi **USER\_LOGIN** được kích hoạt, bạn có thể kiểm tra thông tin xác thực đối với nguồn dữ liệu của mình và cho phép hoặc từ chối quyền truy cập. Nếu bạn cho phép quyền truy cập , bạn cũng sẽ có thể lưu trữ hồ sơ quyền trong **thuộc tính Phiên** . Theo quy ước, có một thuộc tính dành riêng được gọi là **$permission** được sử dụng để chỉ định ID quyền mà người dùng sẽ được chỉ định. Ví dụ:

Java

[**?**](http://docs2x.smartfoxserver.com/AdvancedTopics/privilege-manager)

|  |  |
| --- | --- |
| 1 | session.setProperty("$permission", DefaultPermissionProfile.MODERATOR); |

Bây giờ các quyền của Người dùng được cấu hình đúng. Mỗi khi một yêu cầu được gửi từ phía máy khách, **Trình quản lý quyền** sẽ xác minh yêu cầu đó đối với hồ sơ người dùng và xác định xem có thể thực hiện hay từ chối yêu cầu đó hay không. Trong trường hợp yêu cầu bị từ chối, một lỗi sẽ được ghi lại cùng với các chi tiết.