

## When Security Roles Are Security Risks

*Readers of this article will need a Guest security role with view permissions only. (Ah, LMS humor!)*

It's time to put up your defenses and lock down your security roles. It's so common for me to see TotalLMS™ implementations with such astonishing security roles that I feel I must say something about it. And, for the record, no, I don't mean "astonishing" in a good way.

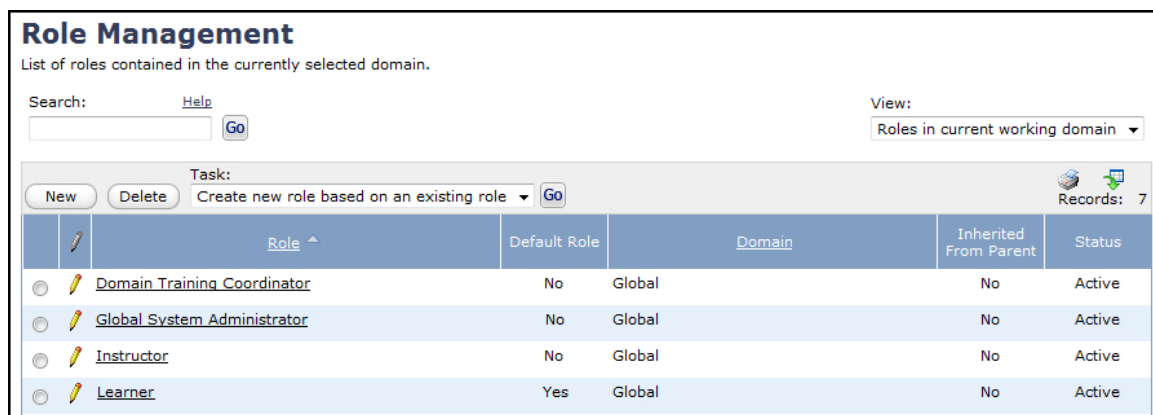
Let's face it: if you are like the majority of TotalLMS™ users, you have created too many roles, you don't know which one does what, and you've likely given too many permissions per role. This means that your LMS security roles are probably much more open than you'd like to think they are, which in turn leaves your organization vulnerable. But never fear! We're here to arm you with the knowledge you'll need to protect your LMS.

It's completely understandable how security roles can get out of control. They're generally set up when the system is first implemented, along with a thousand other things in TotalLMS™, and it can be hard to keep track. And sure, some guidance was likely provided on how to set up your roles but--not knowing what you didn't know--choices had to be made before you had a good sense of TotalLMS™, of how they would be used in practice, or what the repercussions might be.

### **Too Many Roles**

Here's the first question: how many security roles do you currently have? If someone asks your System Administrator how many roles are in your LMS, they should both know the approximate number and be able to tell you the differences between these roles. If your System Administrator can do that--or at least pull out a ready-made documented list--he or she is definitely on top of things and I tip my hat to them. Or at least I would if I wore a hat, but you get the idea.

The rest of us, however, probably have to look it up. To do so, enter Administrator mode and navigate to the Global domain. Now, under the Manage menu, choose Manage Configurations and then Role Management. On the Role Management page, how many records are displayed in the table? 10? 17? Not too bad. But now change the View at the far right to "Roles available in child domains." Now how many do you have? Too many?



**Role Management**  
List of roles contained in the currently selected domain.

Search:  [Help](#)  View: Roles in current working domain

Task:     Records: 7

	Role ^	Default Role	Domain	Inherited From Parent	Status
<input type="radio"/>	<a href="#">Domain Training Coordinator</a>	No	Global	No	Active
<input type="radio"/>	<a href="#">Global System Administrator</a>	No	Global	No	Active
<input type="radio"/>	<a href="#">Instructor</a>	No	Global	No	Active
<input type="radio"/>	<a href="#">Learner</a>	Yes	Global	No	Active

Having too many security roles is not only troublesome, it's a security risk: if you don't know who has permissions to do what in the system, that's a problem. And I'm not just referring to the obvious issues with too-open security roles; giving someone the wrong permissions can lead to

their accidentally doing things they don't mean to and shouldn't be able to do, like deleting a course, a category, or even more. Trust me, I've seen it happen, and it's not pretty.

### ***Describe Current LMS Roles***

The first step in fixing the problem is to get a handle on what you've got: create a list of all the roles in your LMS with short descriptions of each (be sure to note the differences between similar roles), and jot down which ones are inheriting. The goal here is to provide a clear view on the differences between the roles and who can do what, which are really the most important parts of this entire exercise.

### ***Eliminate Similar Roles***

Having just described each role, you have likely found a few that are very similar to one another. As you move to the next step, see if you really need those roles or if you can consolidate them.

### ***Review Each Permission***

Next, review each permission to confirm that those rights are needed and used by people who are given that role. Consider whether any of these roles need to be scaled down. As a rule of thumb, be a bit stingy when doling out permissions and wait till users come to you with specific business needs that require a permission. And remember, just because they ask for it doesn't mean you have to give it to them.

### ***Tales from the Front Lines***

True story: a company using TotalLMS™ created a fairly high-level administrator role that included the ability to delete learning activities. This is okay in and of itself, but deleting learning activities is very permanent, so such a role shouldn't be used by any more than two or three people. Despite strong recommendations otherwise, however, the company gave this role to about a dozen folks. The company reasoned that these were good people who had been trained on the system, so they could be trusted.

Or not. One day, a learning activity was accidentally deleted. And this was not just any learning activity, but their most popular training with about 12,000 completion records on the roster. With no undo button and no recycle bin, the road to recover the data was long and laborious. They managed, but recovery of the completion data took about three months and countless hours. Ouch.

### ***Maintain Security on Your LMS***

As your use of your LMS changes over time, continue to monitor your security roles. It will serve you well in the long run, allowing you to ensure your security roles are not security risks to your organization. We hope this article helps you feel secure in your ability to do that.

*Irene Campbell has been securing security roles and other matters related to SumTotal products for over 15 years. During that time, she has logged in to many client LMS servers using a variety of different security roles. Her favorite role by far is helping clients make the best use of their TotalLMS™ implementations, especially in establishing best practices throughout their organizations.*

*If you have any comments, questions, or suggestions on this article, please secure your thoughts then email them with view and reply permissions to [articles@terrabia.com](mailto:articles@terrabia.com).*

TotalLMS™ is a trademark of SumTotal Systems.