Global Settings – User Management Video Transcript

Welcome to the user management review. So, in this video, we're going to cover the basic settings around user management, which include roles, API keys and MFA options.

So, roles in CyberCNS are defined as the security permission that you're going to grant to a user. Those roles can be customized and those roles dictate what one user can see and access across the CyberCNS data points. Most of the permissions are set alongside with these attributes, read, update, save data, delete and create. So, there is a very flexible security layout here, which we'll get into a little more detail later.

API keys again, issued at the user area. These are for use with the CyberCNS API's. And we do have full documentation out on the support site, where you can see some use cases some best practices and methods around invoking and using the API's.

And then MFA options. So, user accounts that you want to have MFA enabled on we'll talk about where you enable this, how to reset it, how to remove it. So, we'll go ahead and get logged in here to our instance so ever seen us and once we log in, we're going to want to tap on the glow to go to global settings. And then here on the left menu is where we'll find our users and roles area.

So, on our user section, this is where we would add or edit existing users from our list. So, adding a user as simple as hitting the add button here, you can also go and find existing users. I'll just go ahead and search from myself here, Ryan. So, here's my account for this tenant. And I can see here, basically first name, last name, email and a role. On this menu. You can also customize what column headers are available. So, in some of the screens will have additional columns available. So, I'll go ahead and add those into this view. And this will then let me see if this user account has access to all companies or specific companies within CyberCNS. And then if MFA is enabled, or not for that user's account. So, these are some additional flags that can be handy if you're auditing the users in the CyberCNS instance.

For existing users, once you see them here under the Actions, the three dot menu, you've got some additional options here where you can edit this user. So, to choose Edit, this is where we can modify first name, last name and also assign a role. As mentioned, the role is what grants security to the user. So, under the role, you're able to tell it you know what role this person is, so for example, if this was using customer all you have the option to specify all company access for specific companies. And so you can either allow or deny specific customers from the CyberCNS instance. If you choose the admin role that will go away and you'll have access to all companies. So, that's the Edit under the existing user.

But then you have to delete this will delete the account the API key. If you've tapped this, this will generate the API keys for us with the CyberCNS API's. If you don't intend to use the API's, nothing needed here, but this is available in case you are going to invoke our work with the API's. And as mentioned, out on the support site, we do got full documentation around the API's.

It got your MFA status here. So, if you tap this, this will tell you about the user's MFA. So, what they're using and when it was created, and then you can remove this MFA account if you needed to if they had multiples or duplicate or whatever. Or you're just replacing it with a new device, you can come in and remove and also reset their MFA account from here. So, if you need to do any user account maintenance that's done right at the users level.

And again, those are on existing users, adding new users as simple as adding users tap on that Add button, and signaling first name, last name, email and a role. And then once you save that users add it so user management, pretty pretty slick, pretty straightforward. As mentioned with users, you've also got roles to consider.

So, these are the roles that are assigned to the users for security. And again, you can customize what these say. So, obviously, you'll have your admin. And then if you want to rename or add some additional rules for your engineers, your technicians, your consultants, your developers, whatever you call your colleagues and staff probably makes more sense. And then you can either again, edit existing ones, you can clone one so if you know if you got one that's pretty close and just want to make a couple edits to it. You can clone it instead of recreate it from scratch, and also delete and then also add, so if I wanted to make a new role here, just got to give it a name, whatever you'd like.

And then down below are all of the options that you can add to this role. They're grouped pretty much by you know, major functions. So, if you notice we've got you know, ad audit, ad computer so everything to do with active directories is going to be starting with AD. So, GPO groups, logs, events, etc. And this is a pretty extensive list. I'm not going to take you guys through every one of these if you'd notice I can scroll on this goes for a while. Good and bad, right? Very flexible. A lot of control over what data points they can that you can access within the system. So, and again, if anyone's done the full scope of permissions, we do have that on our documentation page. So, connectsecure.com, hover over support, and the resources section. We've got the documentation out there for that. So, be happy to help anyone has any specific questions, you can direct those to the support team. And if anyone has any request on content, we'd be happy to you know, make additional videos as always, so that that is it in a nutshell, that is our user management, again, under the global users area, pretty straightforward where you're going to manage your CyberCNS user accounts from so as always, thanks for watching. We've got more content out on our YouTube channel @ConnectSecureEducation and if anyone has any feedback recommendations, want to drop some comments, feel free to or give us an email education@connectsecure.com Thank you.