# User Mode and Privileged Mode Security

In this lesson, we’ll take a look at how you can secure user mode and privileged (enable) mode. By default, there is no authentication required. If you connect a Cisco console cable to your switch or router, here’s what happens:

Switch con0 is now available

Press RETURN to get started.

Switch>

Once you press the enter button, we end up in user mode right away. There’s no password or anything. The same thing applies to the enable mode:

Switch>**enable**

Switch#

We have full access right away. This is something you might want to change, which is what I’ll explain in this lesson.

## User Mode Security

### Simple Password

The most simple option to protect user mode is to add a password. Here’s how to do this:

Switch(config)#**line console 0**

First, we need to enter the console settings. Here’s where we have to add two commands:

Switch(config-line)#**password cisco**

Switch(config-line)#**login**

We configure a password (cisco) and use the login command to tell Cisco IOS to prompt for this password. Next time you open the console, this will happen:

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Password:

Switch>

The CLI will ask you for the password. At least we have some form of authentication but we can do better…

### Username and Password

Instead of a single password, it’s also possible to use usernames and passwords instead. This is a better option if you have multiple people that need to access your router or switch. Here’s how to do this:

Switch(config)#**line console 0**

Switch(config-line)#**login local**

Switch(config-line)#**exit**

Switch(config)#**username admin password cisco**

Under the console settings, we use the **login local** command to tell the switch to refer to a local database of usernames and passwords for authentication. In the global config, we create a username “admin” with password “cisco”.

Next time you open the console, here’s what you see:

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Username: admin

Password:

Switch>

The switch asks for our username and password.

## Enable Mode Security

What about enable mode / privileged mode? We can also add a password there. You need to do this from the configuration mode:

Switch#**configure terminal**

Now we can set a password for enable mode:

Switch(config)#**enable password cisco**

Let’s see if our password “cisco” works. Let’s get out of enable mode:

Switch#**disable**

And jump right back in:

Switch>**enable**

Password:

The switch now asks for the password.

## Password Encryption

In the examples above, we used passwords but there is one problem…they all show up in clear text in our configuration. Take a look below:

Switch#**show running-config | include password**

no service password-encryption

enable password cisco

username admin password 0 cisco

It’s all clear text. If someone steals one of your switches or routers, they will have your passwords. If you ever backup your configuration and forget to remove the passwords, same problem.

Cisco IOS has a command that lets you encrypt all clear text passwords in your configuration. Here’s how:

Switch(config)#**service password-encryption**

The **service password-encryption** command will encrypt every password that is plain text. Here you can see the result:

Switch#**show running-config | include password**

service password-encryption

enable password 7 13061E010803

username admin password 7 110A1016141D

We need something stronger…

## Secret

Cisco IOS supports something called a secret as an alternative to the password. Let’s try this for the enable mode:

Switch(config)#**enable secret ?**

0 Specifies an UNENCRYPTED password will follow

5 Specifies a MD5 HASHED secret will follow

8 Specifies a PBKDF2 HASHED secret will follow

9 Specifies a SCRYPT HASHED secret will follow

LINE The UNENCRYPTED (cleartext) 'enable' secret

level Set exec level password

Above you can see this switch supports MD5, PBKDF2 and SCRYPT hashes. Older IOS devices only support MD5 authentication.

Let’s give this a try:

Switch(config)#**enable secret cisco**

Our secret will be “cisco”. Let’s see what we find in the configuration:

Switch#**show running-config | include secret**

enable secret 5 $1$CANW$U9Y8O6KeFhrFR4l1Qo07h/

You now find an MD5 hash in the configuration. The “5” that you see behind “enable secret” is the algorithm that we use, 5 means MD5.

Let’s try one of the other algorithms that are considered secure nowadays. Here’s how you can select the algorithm for the enable mode:

Switch(config)#**enable algorithm-type ?**

md5 Encode the password using the MD5 algorithm

scrypt Encode the password using the SCRYPT hashing algorithm

sha256 Encode the password using the PBKDF2 hashing algorithm

Let’s try the PBKDF2 (SHA256) hashing algorithm:

Switch(config)#**enable algorithm-type sha256 secret cisco**

When we look at our configuration, we’ll see the new hash:

Switch#**show running-config | include secret**

enable secret 8 $8$dvX/fx/FJ0Snk2$HhqrOUaEtBgk4zJvG2IQuAJNUicZmmELelC/L6.Fcl2

The “8” behind “enable secret” refers to the PBKDF2 hashing algorithm that we used.

In the example above I changed the hashing algorithm for the enable mode but we can also do this for usernames. Here’s an example:

Switch(config)#**username rene algorithm-type sha256 secret cisco**

My username now uses SHA256 as well for password “cisco”. Here’s what it looks like:

Switch#**show running-config | include rene**

username rene secret 8 $8$dyzsAmZjA3w.aY$YBZn8LBI6CK04ij5ZmqQ/88OrFdc3jzGb6v7SSQI0cw