CONNECTSECURE

Trial Users Welcome – Getting Started - Onboarding Video Transcript

Hi, I'm Ryan Seymour, Education and Consulting Director here at ConnectSecure. If you just signed up for our trial, welcome, we're happy to have you guys. In this video, I'm going to walk you through getting connected, secure setup, get it deployed, so you can start evaluating it using this tool right away. At near the end of the video, I'm going to share with you guys some of the resources that we've got built for you guys to help you get the most out of this product as well.

So, when you first get logged into cyberCNS, you're gonna have a choice here to go PSA or non PSA. Today I'm going to use the non PSA option that can be used by anyone, you don't have to have a PSA to use it. If you do have a PSA and you want to connect it, we can always do that at any point once we get our onboarding wizard completed here so we're gonna start with our non PSA version. And we're gonna go next.

So, the first thing we're going to be doing is creating our first company manually here. So, I would recommend that you guys either use your own internal companies, or you create some type of tests. I'm gonna go ahead and call this one Ryan's sample company for today. Then we've got a description, this is required. We'll go ahead and give this a description. So, this can either be the same thing like Brian sample company, or you can call it something like banking maybe that indicates the industry or market they're in or maybe a location like Tampa, Florida or USA or any other comma separated value that you want to use as a description for that.

Lastly is tags are not required, so we're not going to enter them. There is a great use case for tags. We've got some other content out on our YouTube channel for this so I'd recommend you guys check it out. For Speed sake today, we're going to just leave that blank so it's not required and we're going to create our company going next.

So, this will take us to the deploy probe, an agent screen where you can get the downloads or the PowerShell scripts that we need to install our probes for lightweight. So, the first thing you'll do is choose the operating system that you're going to deploy to so you got Windows you've got Mac Linux Aaron or Raspberry Pi and below you can choose one of the three commands. I'm sorry, one of the three PowerShell commands can be copied using our copies from the corner to deploy different types of agents out. So, we've got a probe, we've got lightweight agent, and then we've got scan without installing anything actually. So, the two most common ones are going to be probes and lightweights are going to get installed on just about everything that you want to scan continuously for vulnerabilities and really use the system. Lightweight agents get deployed to just about every now we've also got a probe the probe and a lightweight work very similarly the only differences is the Pro has the ability to also scan the network for any IP based devices and bring those into the CyberCNS view under your assets so that you know about other devices that are on the network. So, for today we're gonna go ahead and install the probe. We're gonna get that deployed on the machine I'm on generally deploy a probe to a server generally like a domain controller. But I'm going to do this on a workstation today which you can also run.

So, as I mentioned, we've got these nice little copy feature on the corners here. You can tap that, that'll copy the command to your clipboard. And then you're gonna go to PowerShell and you're going to paste in, run that script. So, I've opened my PowerShell there and make sure it's opened as administrator and you're going to run that script. If you do have any type of you know, EDR or an application that might be blocking this download. You can whitelist our agent URLs for communication. We've got those out on our documentation and near the end of this video I will share that with you guys so that you know where to find them. So, we can see when the PowerShell script runs basically it goes out to the internet, perhaps our download from our AWS bucket, pulls environment installs it on your machine, and once it's installed, it'll let us know and we're done with PowerShell so that agent is actually installed and we're ready to proceed to the next screen.

Here the system will go and fetch those agents that we just installed and just confirm that it sees our STL legend that's the name of the machine number. The agent type is probe we can see it's online, local IP address, OS type and version. We're just going to tap Next to proceed. And this is where the Pro will allow us to configure our scanning method and scanning ranges and parameters for what we want to go out and scan the network for and discover assets.

Though when you first load up the screen, the very first field is going to say set one that's our default name. You can change the name of that to whatever you like. You're gonna leave it as set one and feel free. You can put multiple sets of IPs in here to scan so if you had multiple subnets or multiple ranges or multiple static IPs, you can scan all those things. For mine, I'm just going to call this one network since I'm on my home network. You were on your work network you might follow a corporate or work network so on and so next we've got our discovery type. We've got four different ways that you can scan for those assets, last sender, domain, routing, or spiders probably the most popular ones. You've got an IP range where you can set a start and ending range to scan. You can do a static IP or domain oh I'm going to go with the cider most commonly the system will automatically detect the starting IP from the local network that the probe is installed on. So, it automatically picked up and fill this in. If you're on 192 or any other network. It will go ahead and pick those up and fill it in. And then your subnet mask. You can change the notation here if you want to scan different IP ranges. I'm going to go with the most common 24 which will give us 256 addresses that will scan on this particular range. We'll go ahead and save that as our first scan.

So, now if you guys want to expand more than one scanning range there, all you got to do is upon that add button, and then you could add for example set to or maybe this now is going to be your Azure LAN. And you could go ahead and fill in the information and say that you can add as many ranges to the probe as you want for scanning. If you realize that you've made a mistake on one of these, you can always use the three dot action menu on the far right here. This will allow you to edit or remove one of those ranges. And then you'll also notice we have a copy to probe feature so on any range we create. We have multiple probes in an environment we can copy those ranges out to other probes. That way you don't have to rebuild all the networks that you're scanning if you have Okay, so once we get our IP ranges and you're ready to go forward are just going to tap that next button.

Here we've got SNMP support, whether it's be one or two, or the three. This simply toggle to the second line. You tap the ad, you put it in the envelope, so give it its name, tell it what version and your private or public strings you enter. Same thing on v3 except you'll have to put in protocols and author you'll have to fill in the info. If you have any SNMP devices and you want to enter those you can. You don't have to it's not required. You don't have any you can just go with Next to proceed. Otherwise, add those and these screens will all work similar as far as being able to add multiple records and then using our three dot action menu to edit or remove. We'll tap Next.

Next is going to be our asset or master credentials. So, this is where we could add local credentials for a machine. So, if you had, you know most of our partners that we work with will have some type of local administrator accounts that they use to manage and maintain the endpoints they're supporting. So, if you guys have those local admin accounts, you could add in you know that username, what that password is. If there's a domain you could add it not requiring and give that a save. And similarly, you can edit or remove those credentials using that three out action menu. So, if you have different sets of credentials, we can add those and those will be used during scans. Again, they're not required, so I'll remove them today. Just soiled positive confusion when in lifespan, but you guys going to have those credentials. If you have them. Feel free to add as many as you need.

Next, we're going to go to Active Directory credentials. So, unlike them master credentials which are basically local, nice is going to be for Active Directory schemes. So, if you're interacting with a Windows Active Directory environment, you can go ahead and add in you know, for example, the domain admin and give it a domain name. What the name of that server is, maybe it's DCO one username and password give it a save. Similarly, you can add multiple sets of credentials at a delete using a three dot action menu, so I'm going to go ahead and just remove those you'll get messages in the foreigners are noticing and you're doing some of the SES deletes the system public.

We've also got an exclude IP. So, this will allow you to set up an exclusion when you're scanning Active Directory environments. So, again, we'll give you a little note there so if you need to do any exclusions when you're scanning, this is where you can exclude during an ADC and again, we've had documentation for all this stuff out on our conference site. So, you know I'll be sharing it with you guys later. We're gonna go ahead and go next. I don't have any ad creds I'm not in an ad environment on this particular scan, so I don't need to add any and lastly, once we go next, the system will automatically select our Full Scan Type and it will kick off the first scan.

So, that first scan is kicked off. Right now in the active Assets window. What we're going to see is the asset that we've just installed that probe. So, if I go up to the probes and Agent section you can see here we've got one probe. It's online RSL legend. Again, some some basic info about that machine when it was installed. On its last payment communication was with our portal and the last time it was scanned. So, you can see it hasn't scanned yet once this machine completes its first scan. We'll go ahead and get that timestamp in there and know that it's been scanned and then the data is refreshed.

So, this probe in Asian area is where we're going to. We're going to see any of the probes or agents that get deployed. So, those are the probes in those lightweight agents. So, again, generally one probe out, and then the rest of the machines would get the lightweighting that are active assets view here. This is where as soon as some of those assets come on that we're scanning for get discovered they'll start populating this list right now I've just got the RS skill legend and this one's still scanning.

We can also go over here to our jobs area and actually see what's going on. So, this is where once the sands completed, we will see what was scanned how many assets or devices it found. And we'll build a look at some of that data refreshed in our system. Okay, so we're going to go ahead and let this scan run. And while this is running, I'm going to jump over to our support page documentation. I want to show you guys a couple of key things there to help you out with your trial as you're getting started in case you ran into any issues getting that probe or an agent.

So, our documentation, at connectsecure.com, we're going to go up to that resources and we're gonna tap on support and here we're gonna tap view dot. This will take us to the confluence site where we've got our documentation. You can search this space very easily by just searching the word you're looking for. So, again, if you were interested in those PSA integrations, or you're looking for any type of information about any of the scanning or anything you see in our system, you can find it there in that search.

Now, I want to guide us specifically to some of the prerequisites here. And it's the very first one in that list. And so, the whitelisting URLs for Asian communication. This is where if you have any issues running any of our scripts, when or getting agent updates, you're going to want to make sure that you get these whitelisted inside of your environments. Now, we've got multiple sets here, depending on the region that you're hosted in. So, if you look up when you're logged into our application in your URL, you'll see your region so I can see here us these two. But when I'm looking at that documentation, I'm going to just make sure I'm looking at the appropriate URL stack and then these six URLs will get whitelisted so that our agents don't have any communication issues, and we don't get picked up maybe as any malicious things going. So, out in our documentation site whitelisting URLs want to make sure you guys see that you're about it. If you're having any issues with this stuff, let our support team now. We can help you guys out.

Back on that again, on our connectsecure.com support page. We've got the ability to raise a ticket here. You can also send an email to open a ticket with us just email support at cybercns.com That'll alert our team and this you guys some help if you're having any type of issues or so now we're just going to give our scan here a couple of moments to pick off and finish and then we'll get we'll revisit our active assets view and take a look at what our scan has found.

So, on our jobs menu here we can see now that probe scan has finished. And you can see here the results from the job. So, it's discovered 25 devices out of 256 IP scans that it ran so that was a slash 24 subnet it scanned all 256 addresses. And we picked up 25 devices. So, I'm at active assets view on the left. Again, our STL legend that's our probe that we scanned and then we can start to see all the other assets that it's discovered. On the network. So, bunch of smart switches, couple Apple TVs here, a ring doorbell and Alexa, a Comcast modem so anything on my network with an IP it would have scanned so that's an example just to kind of show you guys how that scanning works and runs.

And again, back upon our probes and agents. That's that probe. We can see it here and you go up to that three dot action menu on your probes and use discovery settings. This is how you guys can get back to that view where we walked you through that onboarding of that probe where you got to set the IP range of the SNMP creds, the ad creds, those local master creds. So, this is where you're going to find that info right on your probes. So, that's as easy as getting a probe deployed element with the scan and scans initiate and kick off and you've got data to work with. So, it's pretty simple. I'm going to jump back over to our support page. We talked about being able to create tickets with our team, go to our documentation site, we've also got a video library that we're starting out on our YouTube channel that can execute education. And if you go out to our website support videos, we've got a collection here on the site. You can also see these old lists in our YouTube channel. And we've got different breakdowns of different modules and different features within our system.

So, if you want to learn you know about the report builder or you want to dive into remediation plans, or you want to learn about the active assets use or application baseline so on and so forth. We've got a collection of videos out on the library. We're going to continue to publish content here for you guys just to help with the learning curves and also share some of the best practices, tips and tricks that we've learned and we've picked up over the years working with all the MSPs that we all been engaged with here at connect secure. So, out on our site, the video library, and again, our documentation, our support team, let us know how we can help we're here to help or listening and we look forward to working with you guys.