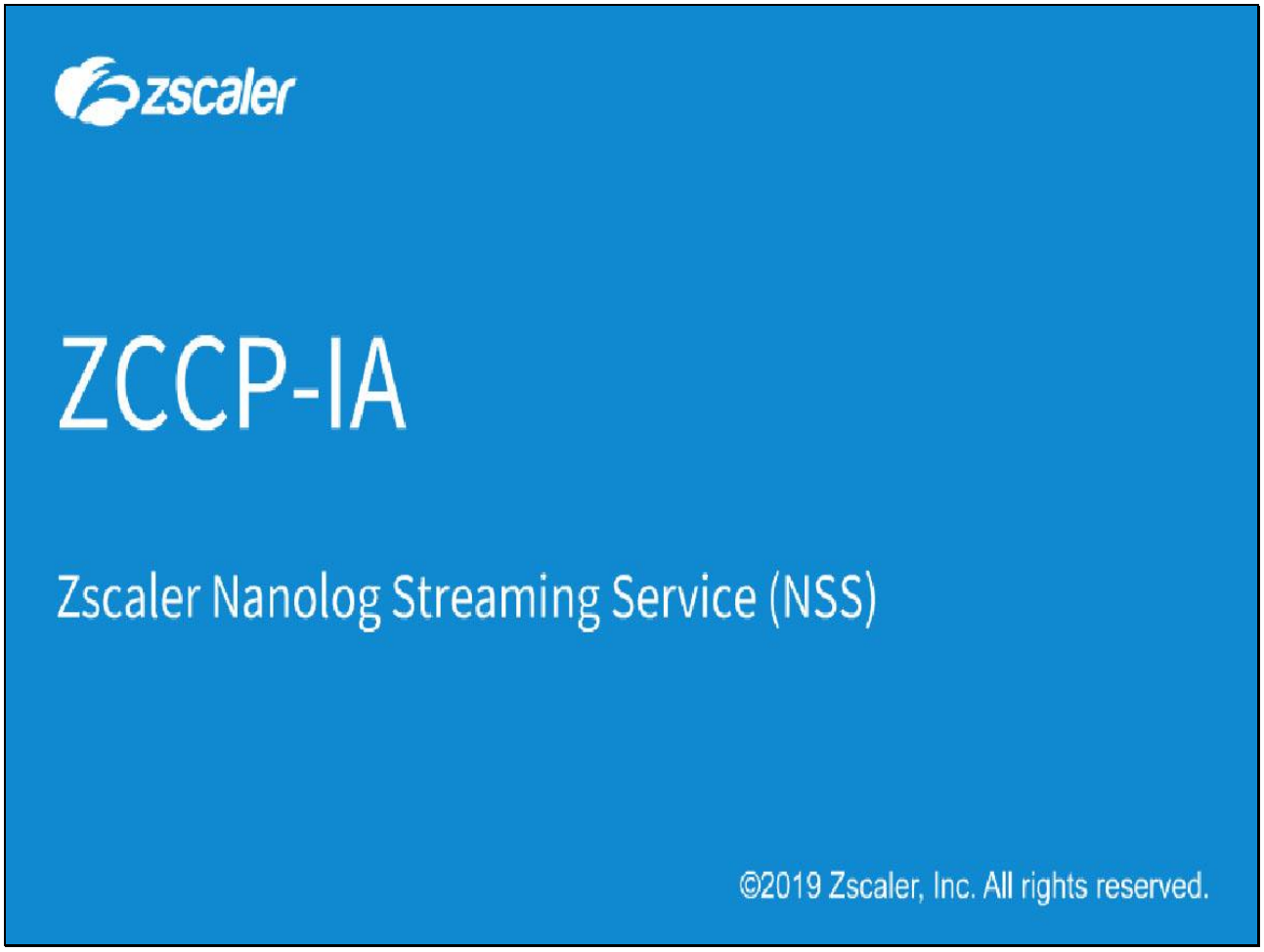
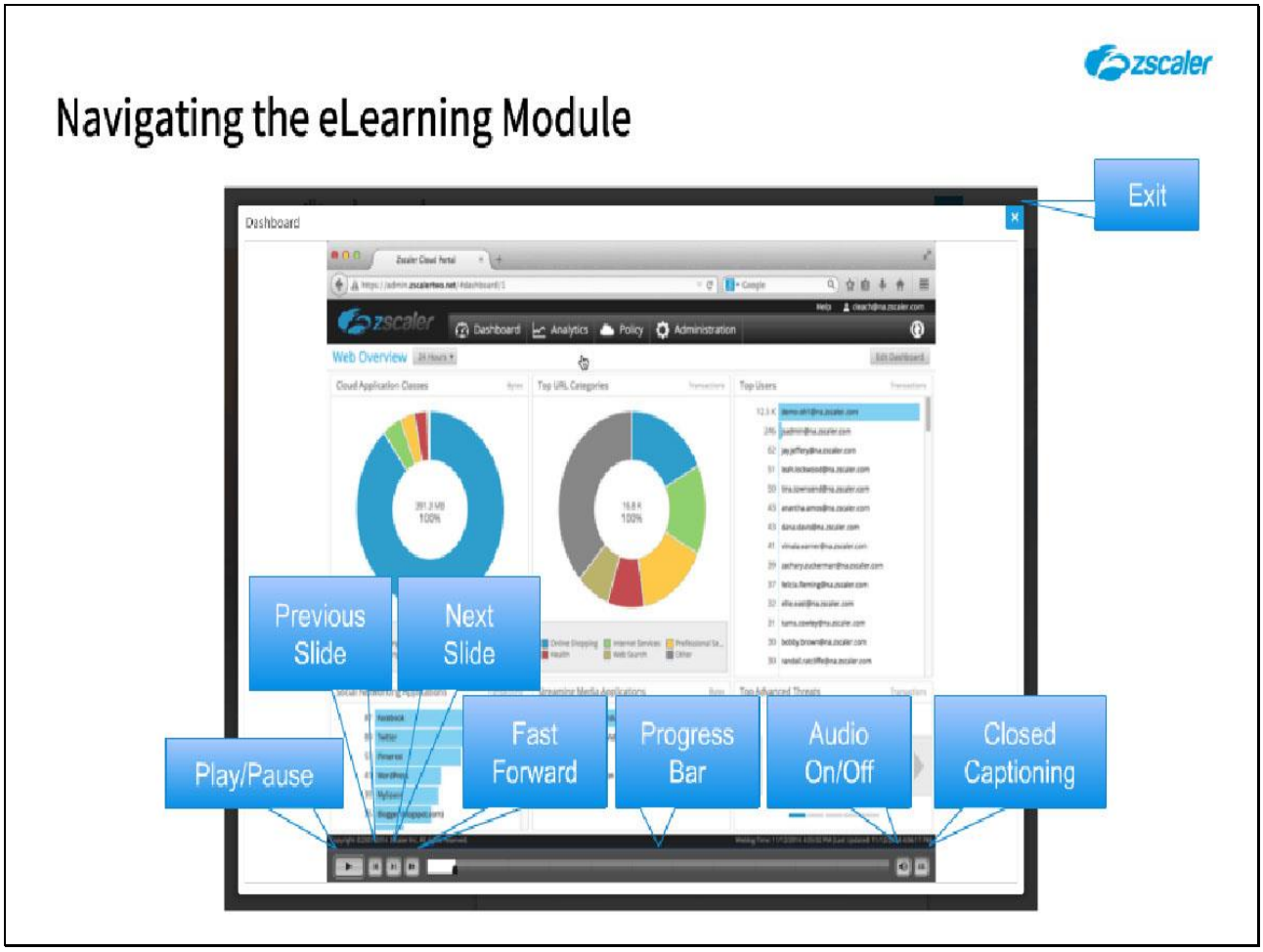
Slide 1 - ZCCP-IA



Slide notes

Welcome to the Zscaler Nanolog Streaming Service module.

Slide 2 - Navigating the eLearning Module



Slide notes

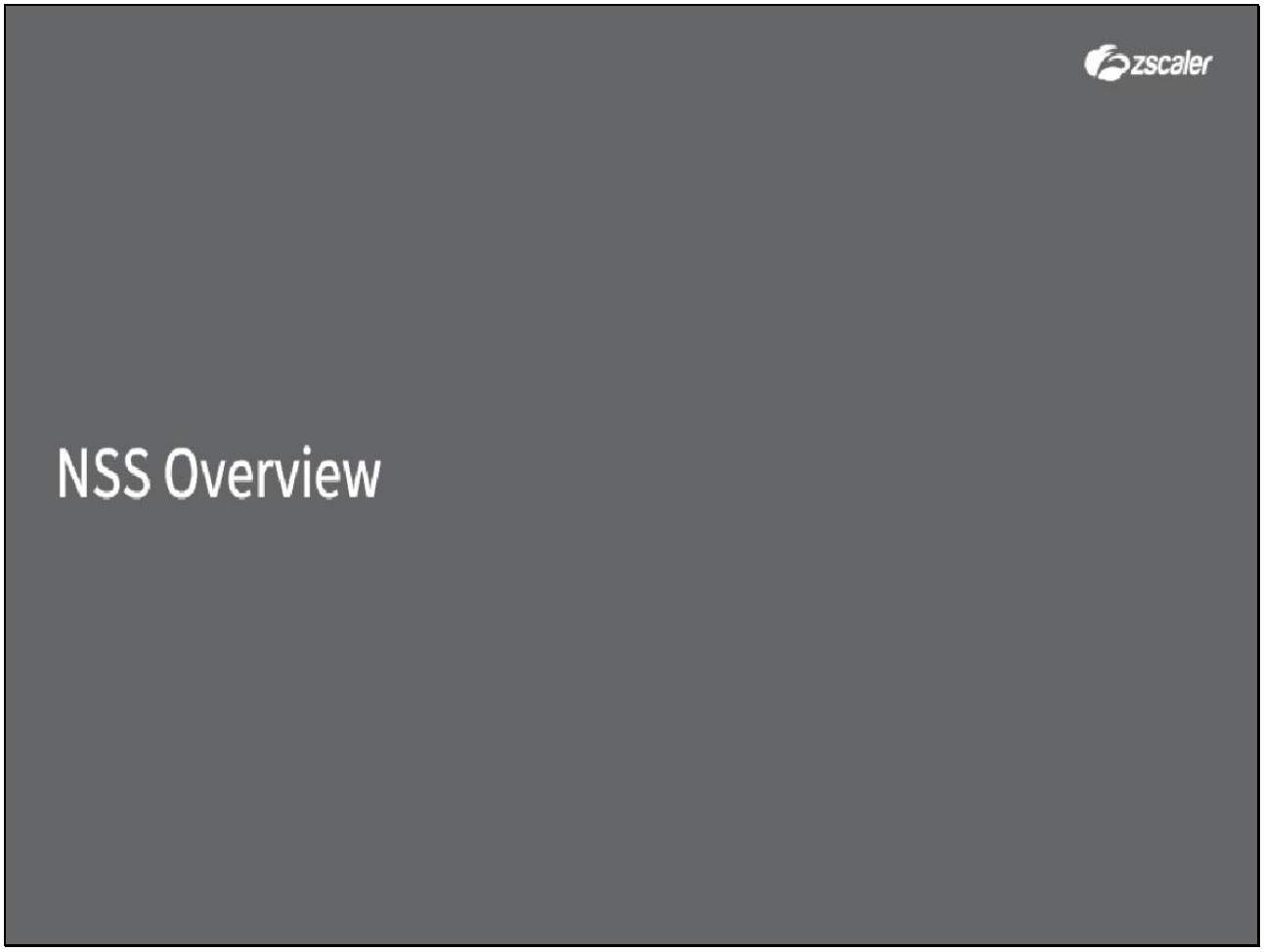
Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and Next Slide, and Fast Forward. You can also mute the Audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the “X” button if you wish to exit.

Slide 3 - Module Agenda

Slide notes

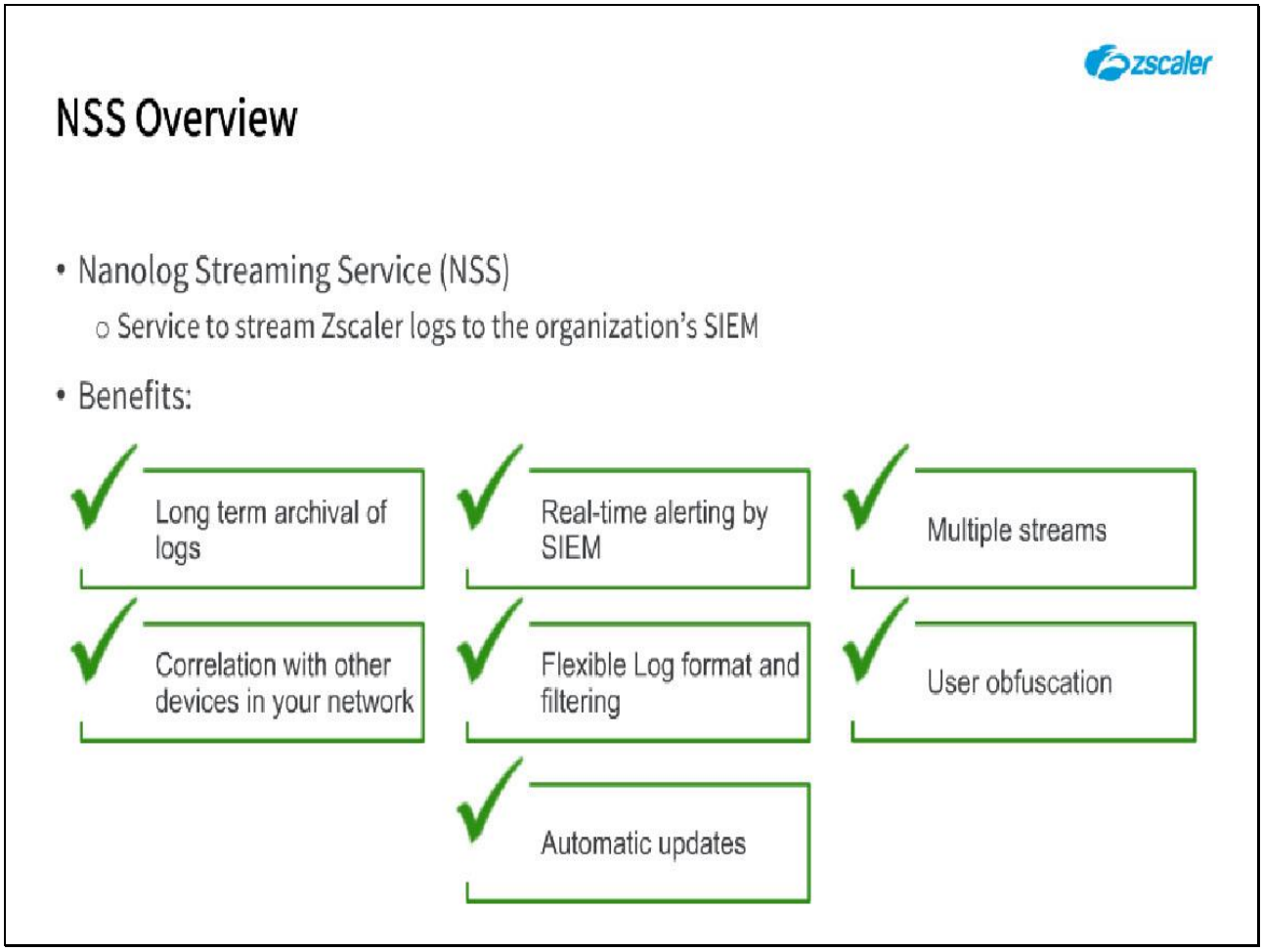
In this module we will cover: an overview of the Nanolog Streaming Service, Requirements for NSS, Deploying NSS, Configuring NSS Feeds and Alerts, and Configuring your SIEM.

Slide 4 - NSS Overview



Slide notes

Slide 5 - NSS Overview



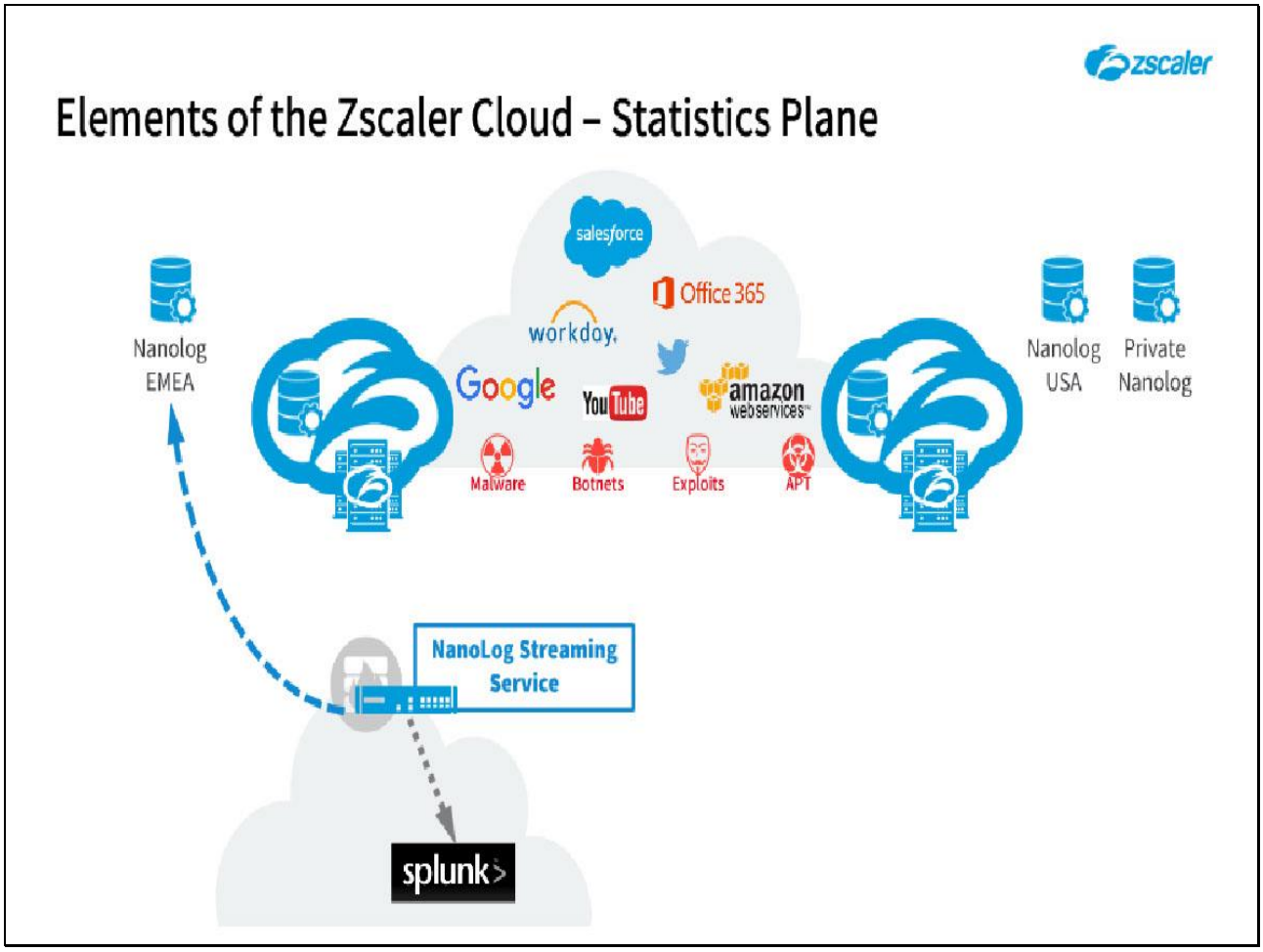
Slide notes

The Nanolog Streaming Service is a mechanism for streaming log data generated by Zscaler into your organization's SIEM. Some of the benefits include: Long term archiving of logs. Zscaler stores logs for a maximum of one year. If you wish to store logs beyond that time you will need NSS to deliver them into your organization where they can be stored locally.

NSS allows real-time alerting by your SIEM as well as allows event correlation with other devices in your network. NSS allows a great deal of control over which logs are sent to your SIEM and the format of those logs. NSS can be configured to deliver multiple streams for redundancy or to separate data like sending URL category violations to a different system than security alerts.

Depending on your regulatory and HR policies you can optionally obfuscate user identities. Finally, once the NSS is configured it is managed by Zscaler and any software updates are automatically applied.

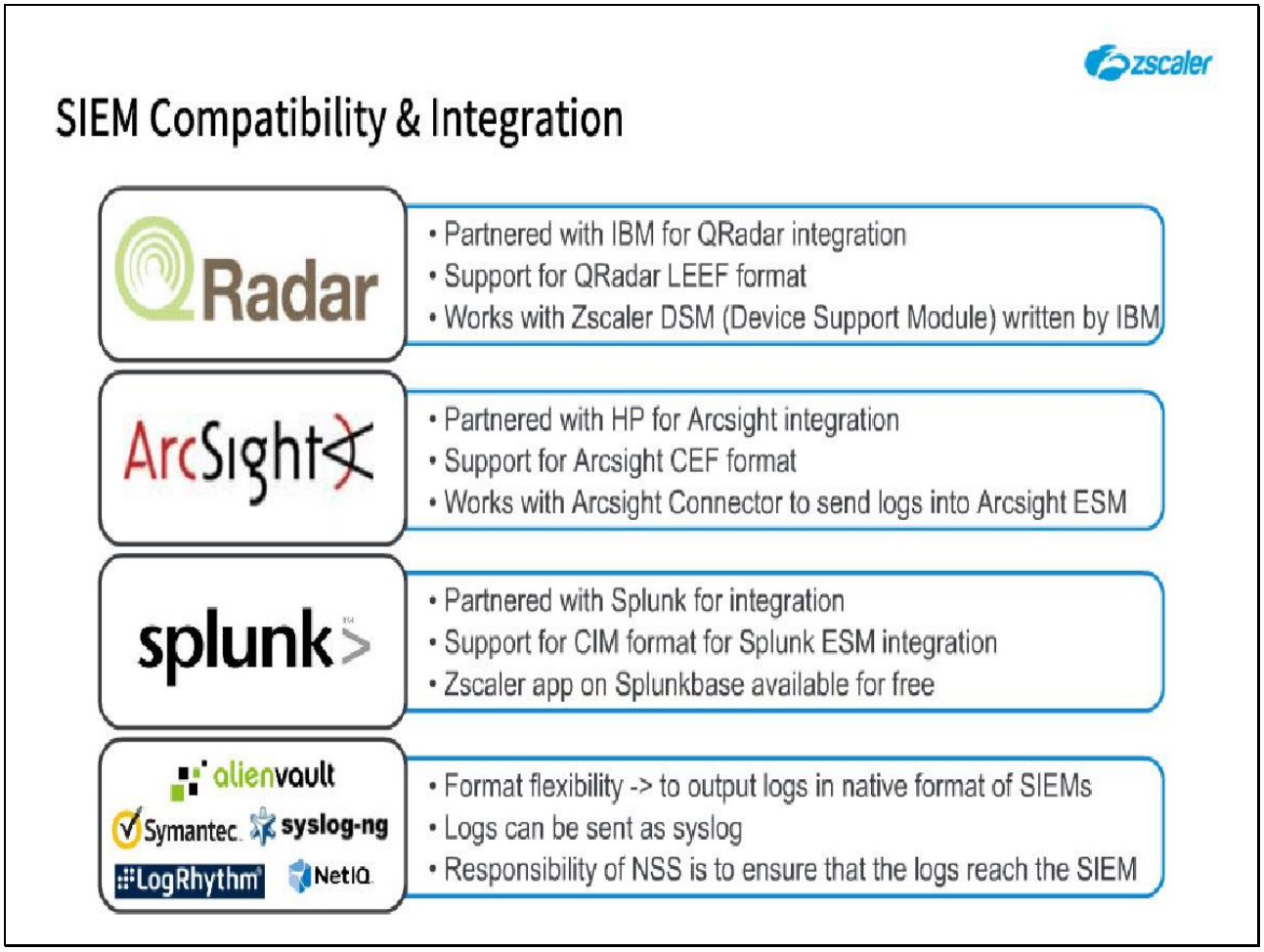
Slide 6 - Elements of the Zscaler Cloud – Statistics Plane



Slide notes

The Nanolog Streaming Service is performed by a virtual machine that is installed inside your network or DMZ. A certificate-based TLS connection is made from the NSS virtual machine to a nanolog cluster. Then, when users are browsing through Zscaler, the logs that you specify are sent down that TLS tunnel into the NSS virtual machine and then on to your SIEM.

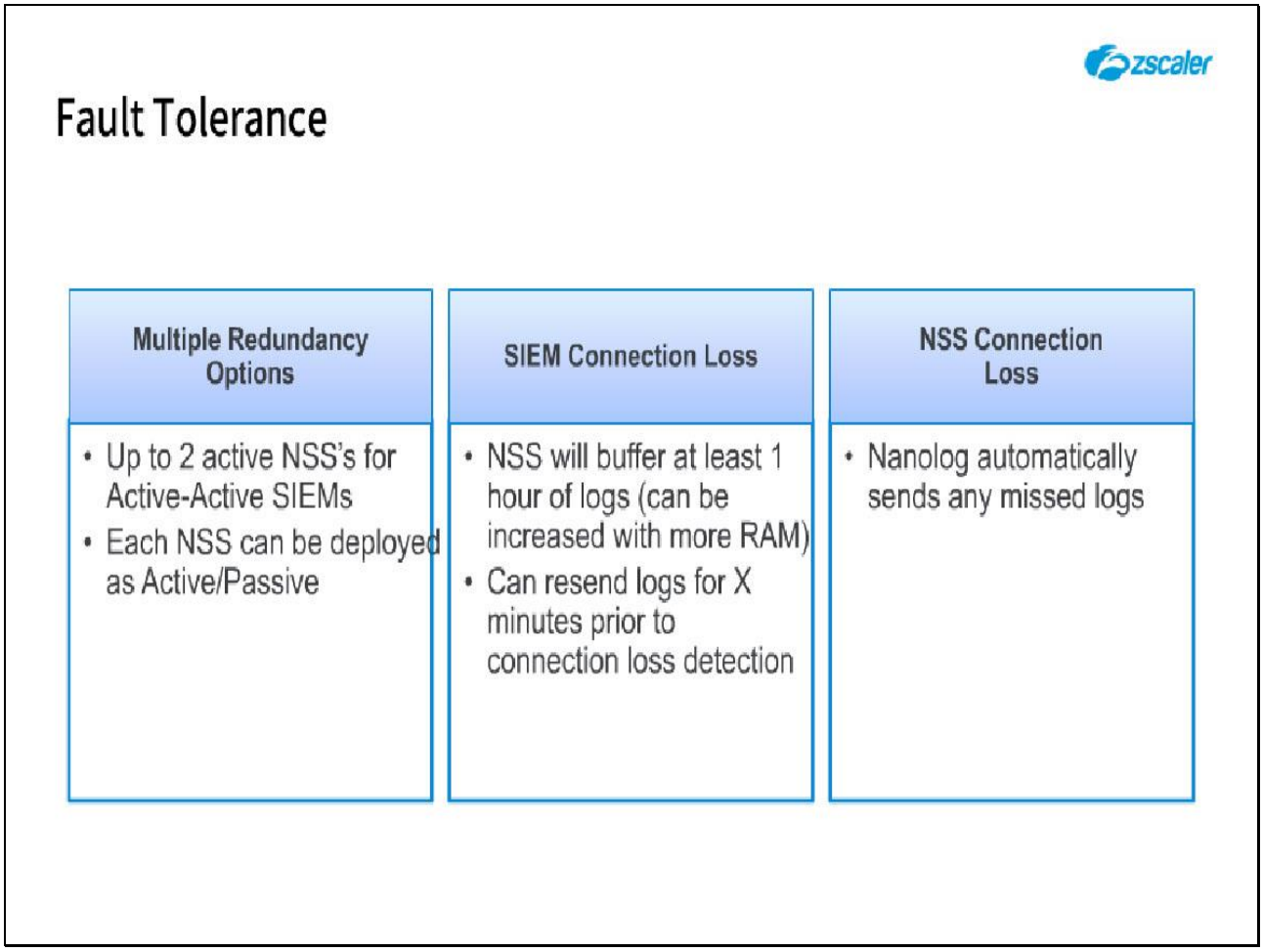
Slide 7 - SIEM Compatibility & Integration



Slide notes

Zscaler provides built-in support for a variety of SIEMs. Logs can also be sent as syslog, CSV, or tab separated

Slide 8 - Fault Tolerance



Slide notes

Zscaler supports multiple redundancy options depending on your SIEM deployment. You can have up to 2 active NSS Virtual Machines at a time for when your SIEMs run Active-Active. You can also deploy additional NSS Virtual Machines as cold standbys by using the same TLS client certificate as the primary. Make sure you do not have both Virtual Machines active at the same time or lost logs may result.

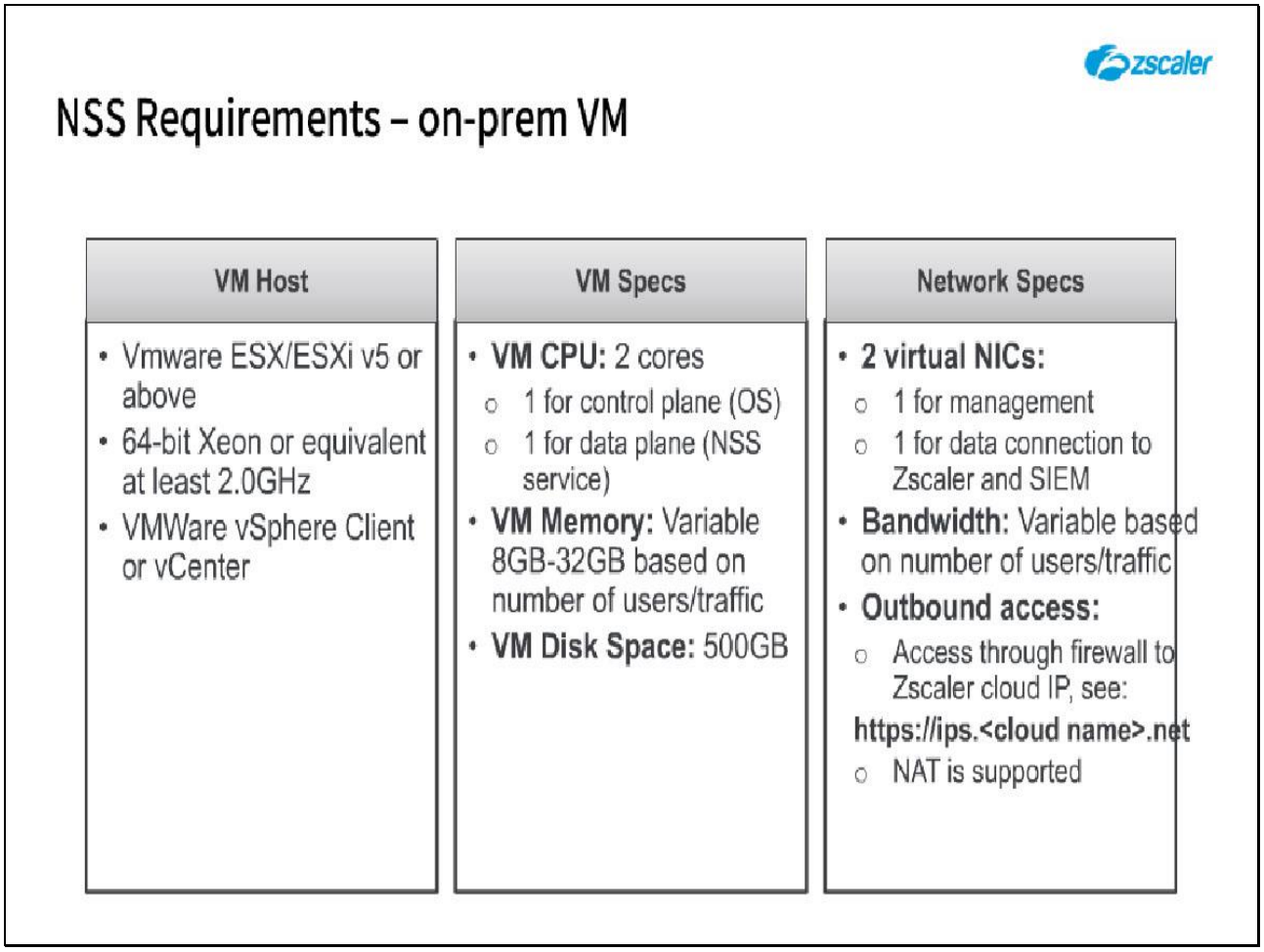
If the NSS Virtual Machine loses connection with your SIEM, the NSS will automatically buffer logs until connectivity is reestablished. If you are using the minimum calculated amount of RAM for the Virtual Machine it will be able to buffer for at least 1 hours of logs. If you allocate more RAM to the Virtual Machine this time will be increased.

Once connectivity is reestablished, you can configure NSS to send logs starting with some number of minutes before the connectivity loss was detected. Each log has a unique record ID so your SIEM can eliminate duplicate logs. In the case that the NSS Virtual Machine loses connectivity with the Nanolog, any missed logs will be automatically sent when connectivity is reestablished.

Slide 9 - NSS Requirements

Slide notes

Slide 10 - NSS Requirements

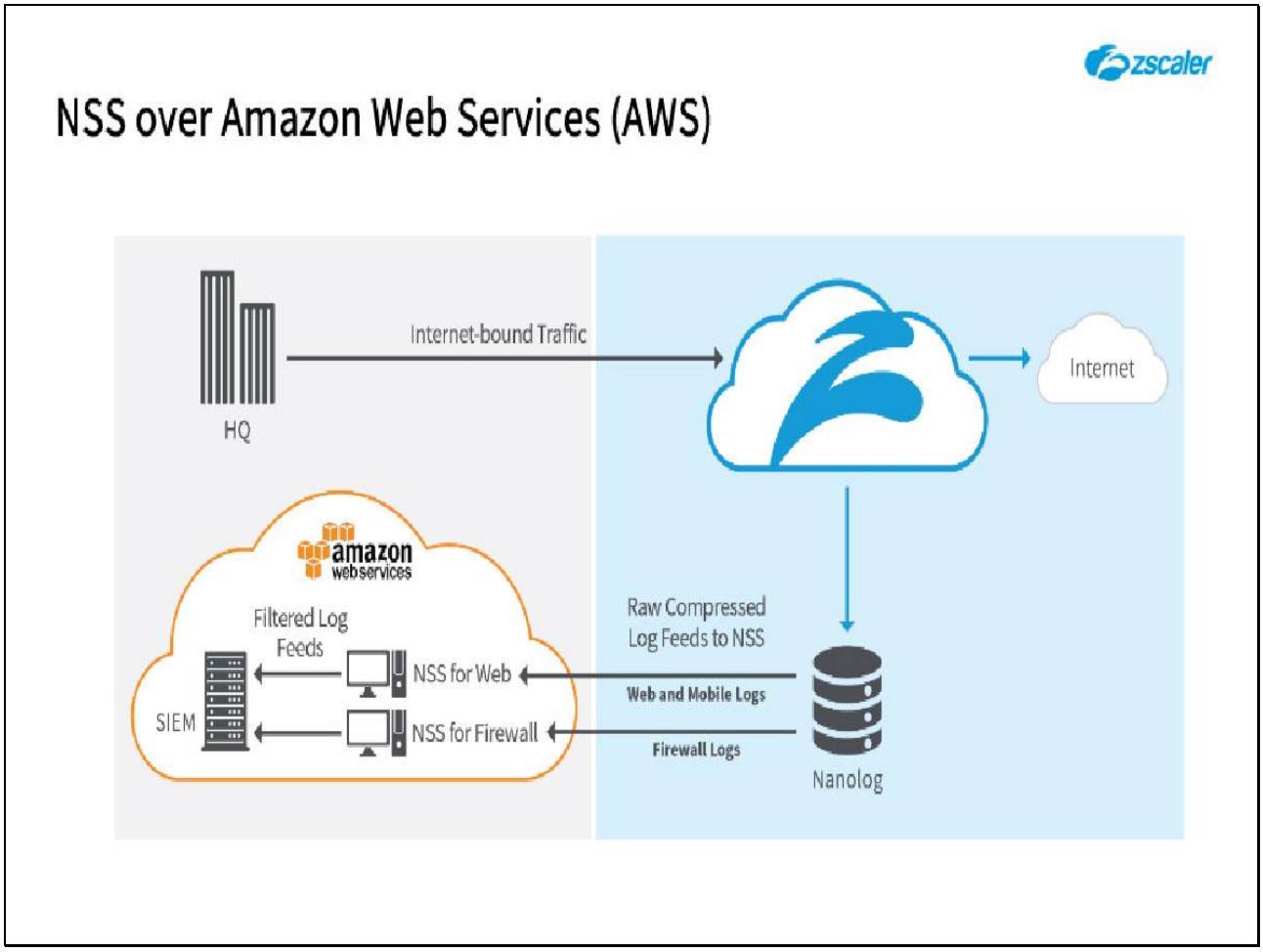


Slide notes

Here are the basic requirements for the NSS virtual machine. The Zscaler Admin UI contains a calculator that will give you more specific recommendations for CPU, memory, disk storage, and bandwidth based on the number of users and expected peak transactions per hour.

We'll walk through that during the demo portion. For the network portion you will need to allocate 2 IP addresses and allow connectivity to the Zscaler Nanolog clusters. You can find a detailed list of IP addresses and ports needed at ips.<cloud name>.net

Slide 11 - NSS over Amazon Web Services (AWS)

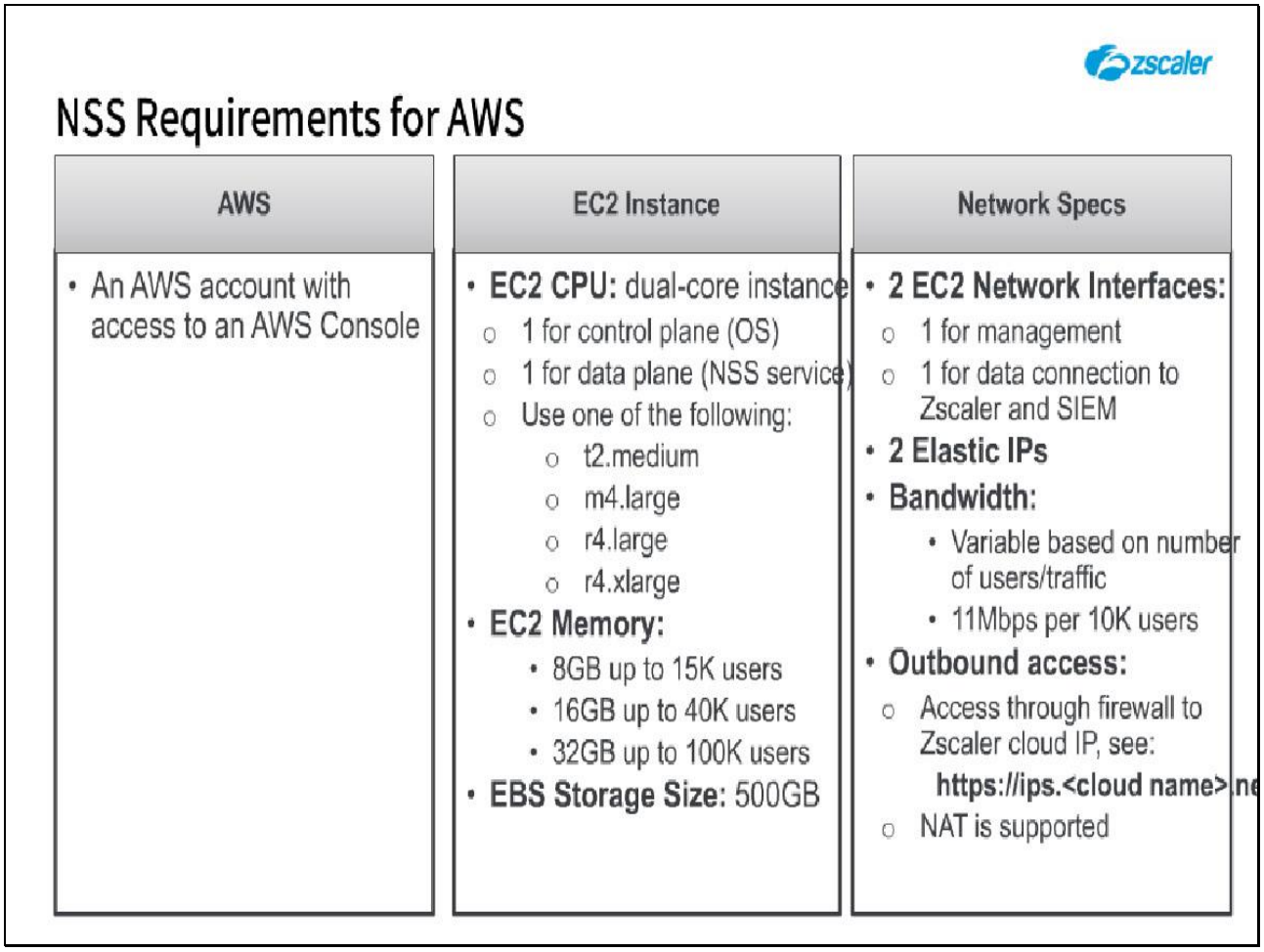


Slide notes

Another option for deploying NSS is on an EC2 Instance on Amazon Web Services. One NSS instance is deployed for web and mobile logs and another NSS instance is deployed for firewall logs. The Nanolog then streams copies of the logs to each NSS in AWS in a highly compressed format to reduce bandwidth footprint. The original logs are retained on the Nanolog for 6 months.

Logs can be retained on the SIEM based on the organization’s needs and SIEM configuration.

Slide 12 - NSS Requirements for AWS



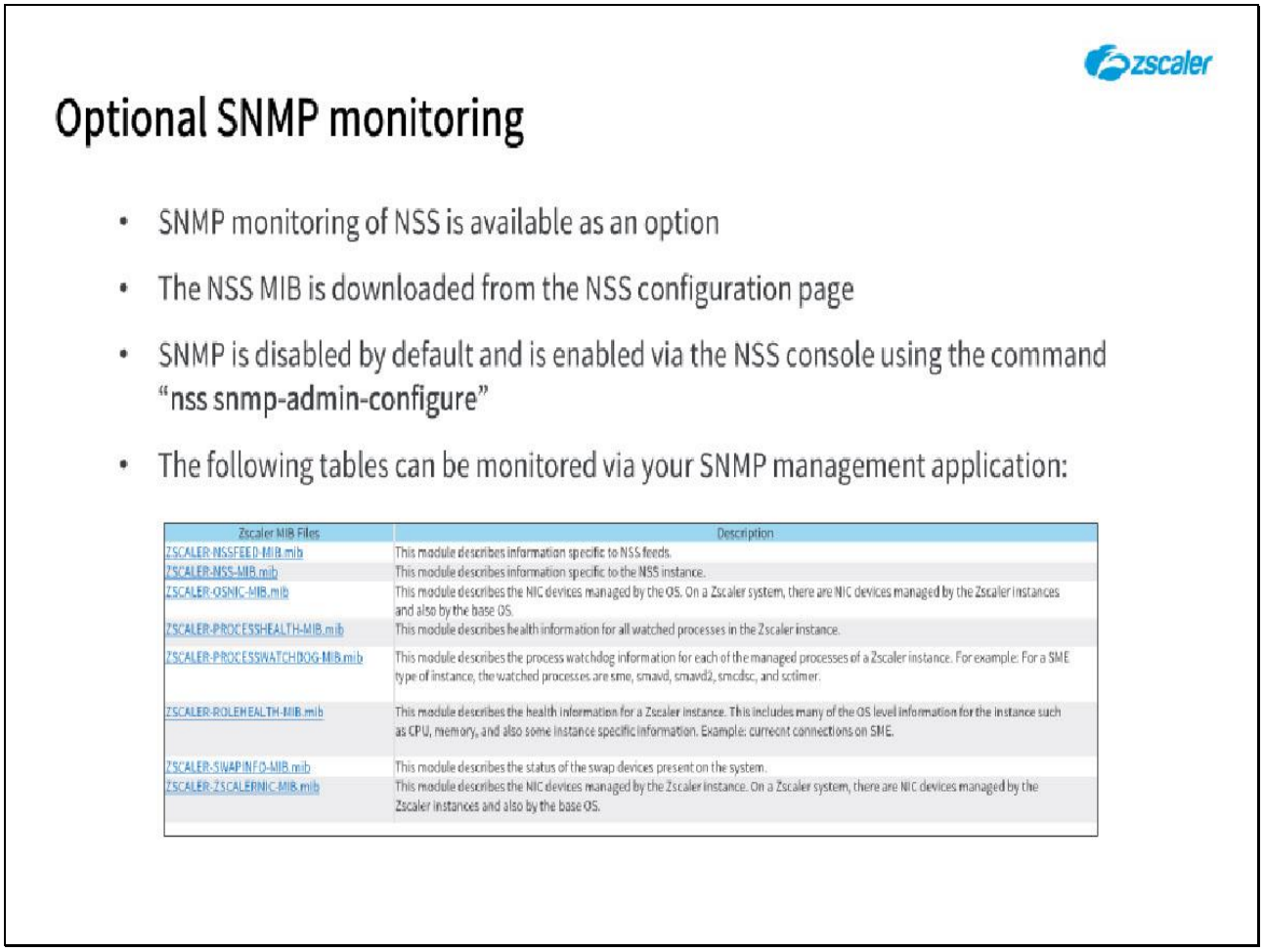
Slide notes

This slide lists the requirements for deploying an NSS instance on AWS. Press pause in the player to review and then press Play when you are ready.

Slide 13 - Optional : Enable SNMP management of NSS

Slide notes

Slide 14 - Optional SNMP monitoring



Zscaler MIB Files	Description
ZSCALER-NSSFEED-MIB.mib	This module describes information specific to NSS feeds.
ZSCALER-NSS-MIB.mib	This module describes information specific to the NSS instance.
ZSCALER-OSNIC-MIB.mib	This module describes the NIC devices managed by the OS. On a Zscaler system, there are NIC devices managed by the Zscaler instances and also by the base OS.
ZSCALER-PROCESSHEALTH-MIB.mib	This module describes health information for all watched processes in the Zscaler instance.
ZSCALER-PROCESSWATCHDOG-MIB.mib	This module describes the process watchdog information for each of the managed processes of a Zscaler instance. For example: For a SME type of instance, the watched processes are sme, smavd, smavd2, smcdsc, and sctimer.
ZSCALER-ROLEHEALTH-MIB.mib	This module describes the health information for a Zscaler instance. This includes many of the OS level information for the instance such as CPU, memory, and also some instance specific information. Example: currecnt connections on SME.
ZSCALER-SWAPINFO-MIB.mib	This module describes the status of the swap devices present on the system.
ZSCALER-ZSCALERNIC-MIB.mib	This module describes the NIC devices managed by the Zscaler instance. On a Zscaler system, there are NIC devices managed by the Zscaler instances and also by the base OS.

Slide notes

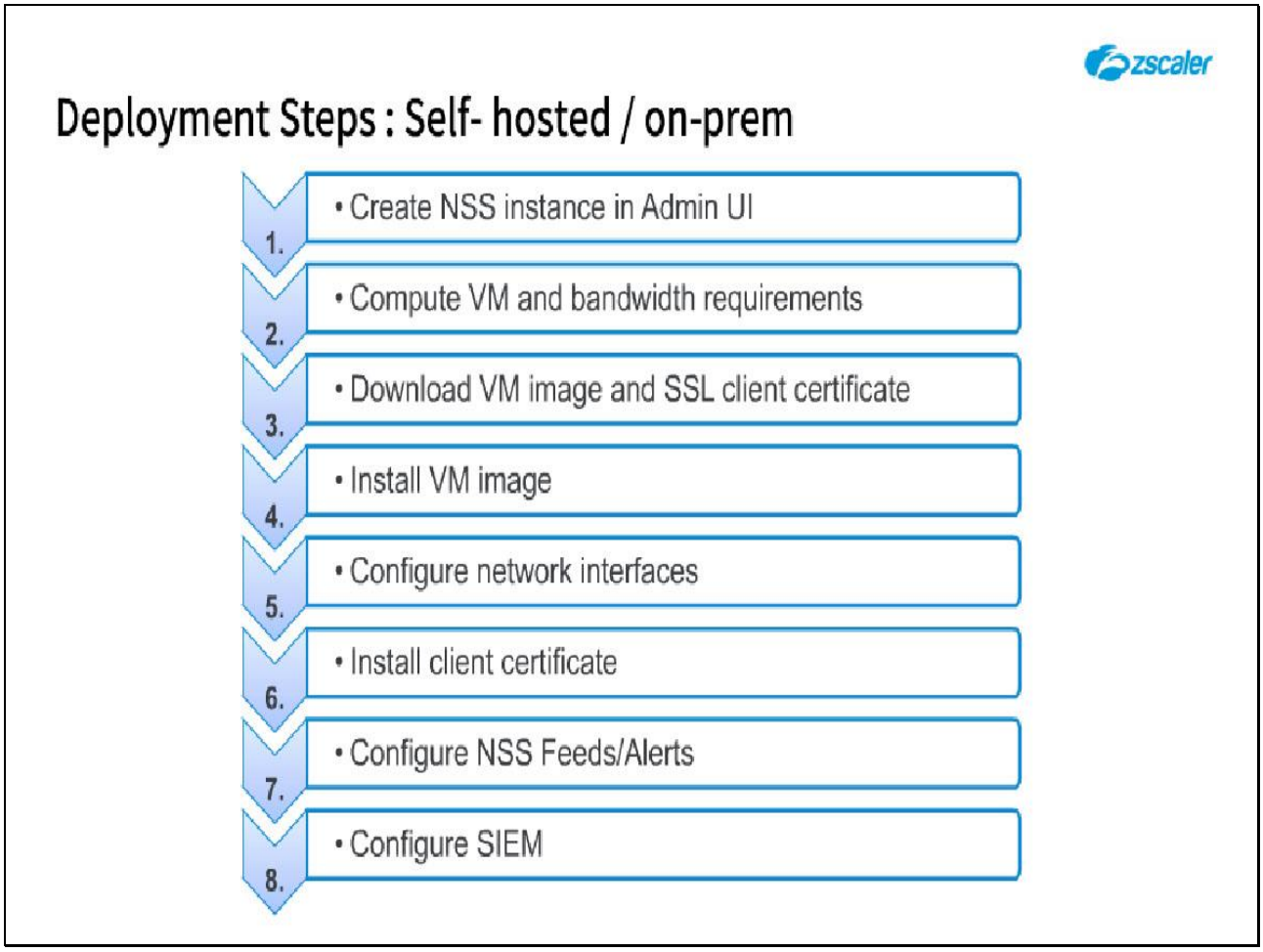
Monitoring of the NSS Virtual Machine may be done via SNMP. A copy of the NSS MIB file can be downloaded from the NSS configuration page in the Zscaler Admin UI and then imported into your own SNMP manager application.

SNMP is disabled by default. It must be enabled from the NSS console using the command “NSS snmp-admin-configure” to configure the SNMP username, password, authentication type, and encryption type for the SNMP manager. Once enabled and configured you can monitor the NSS via your SNMP manager.

Slide 15 - Deploying NSS

Slide notes

Slide 16 - Deployment Steps

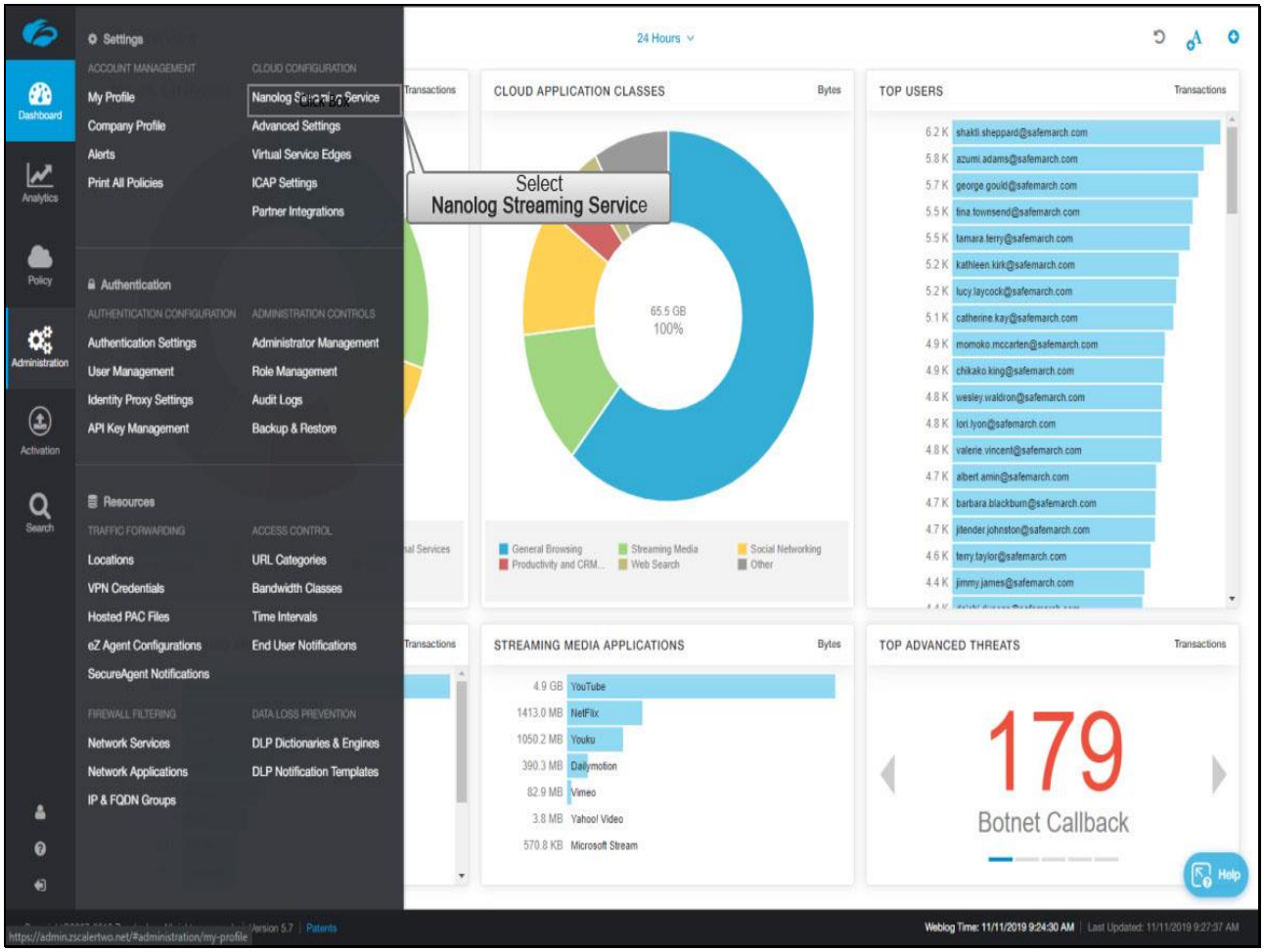


Slide notes

Here are the steps to Deploying NSS. Create an NSS instance in the Admin UI. Compute VM and bandwidth requirements. Download the VM image and SSL client certificate. Install the VM image. Configure network interfaces. Install the SSL client certificate. Configure NSS Feeds and Alerts in the Zscaler Admin UI. And finally, configure your SIEM to receive the logs.

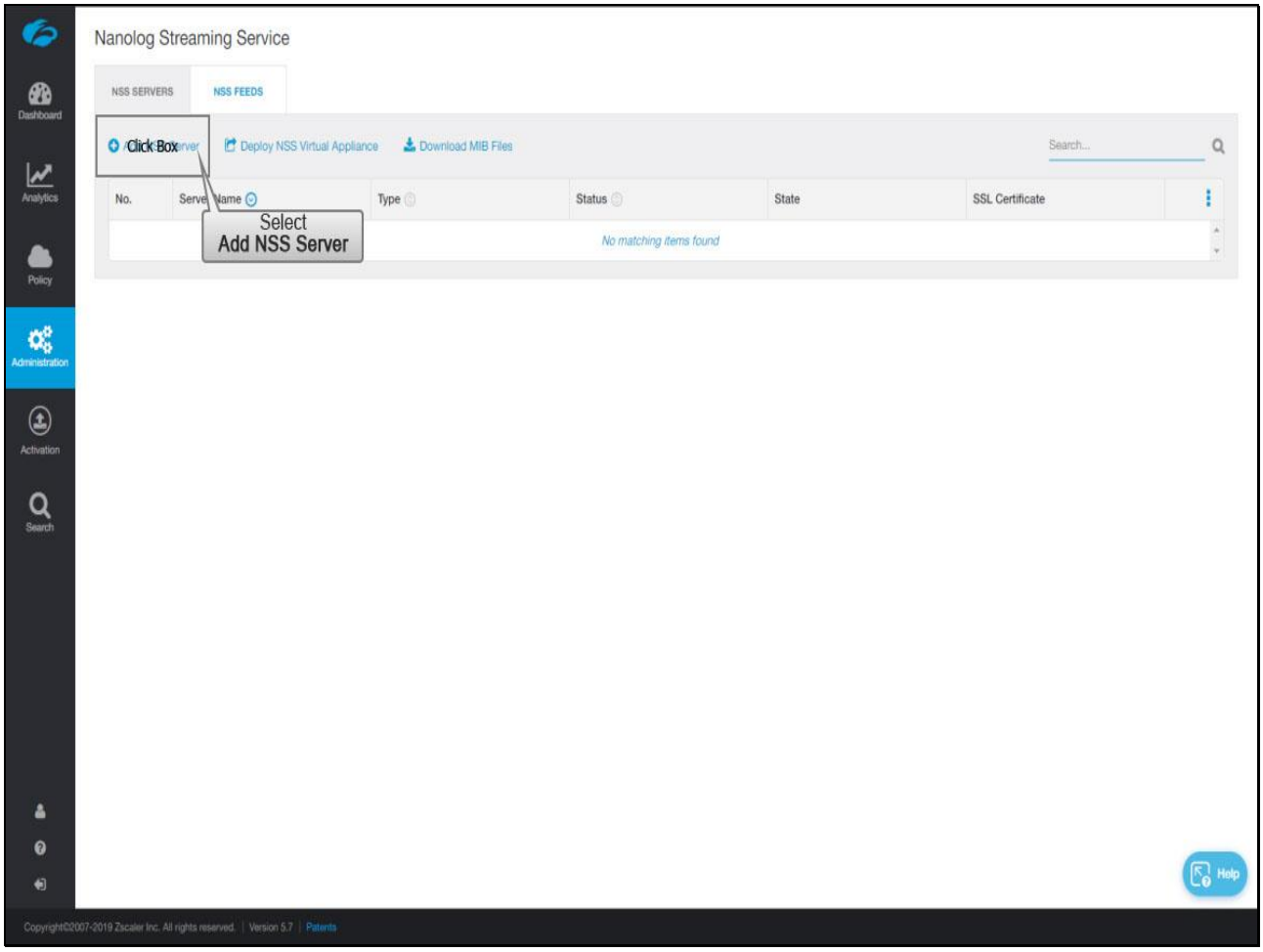
Slide notes

Log into the Zscaler Admin UI and click on the “Administration” tab.



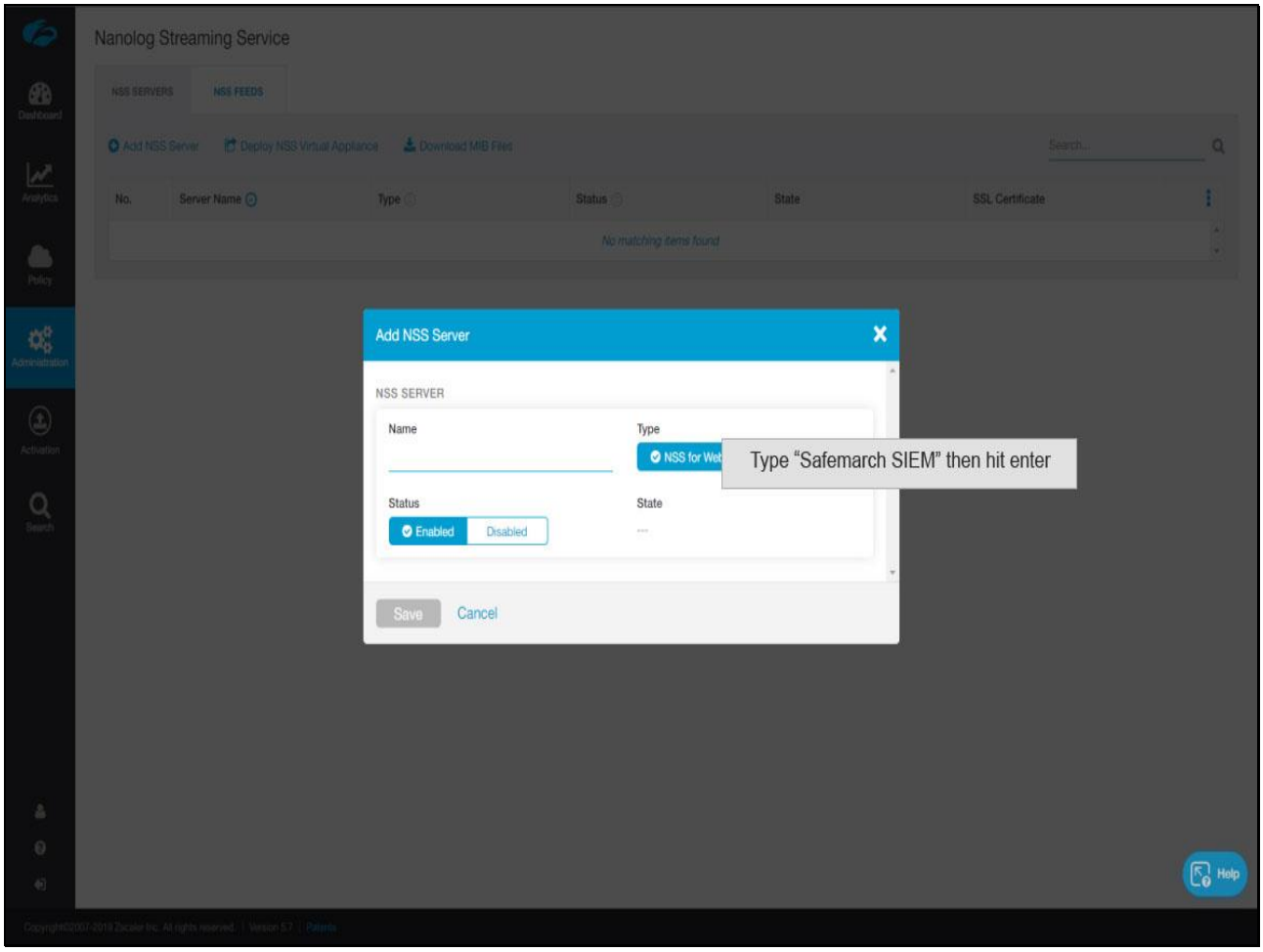
Slide notes

Click on Nanolog Streaming Service.



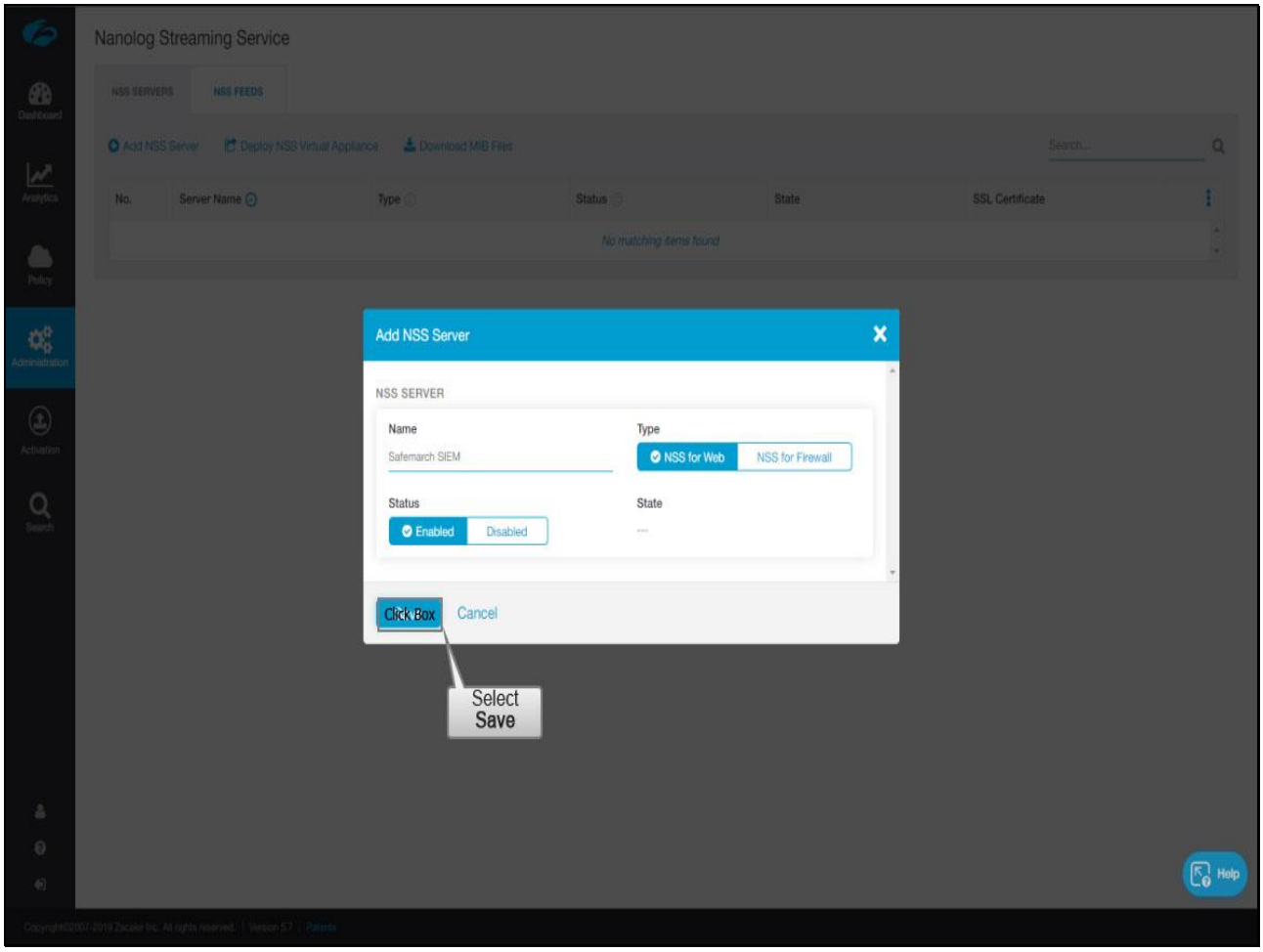
Slide notes

Click **Add NSS Server**



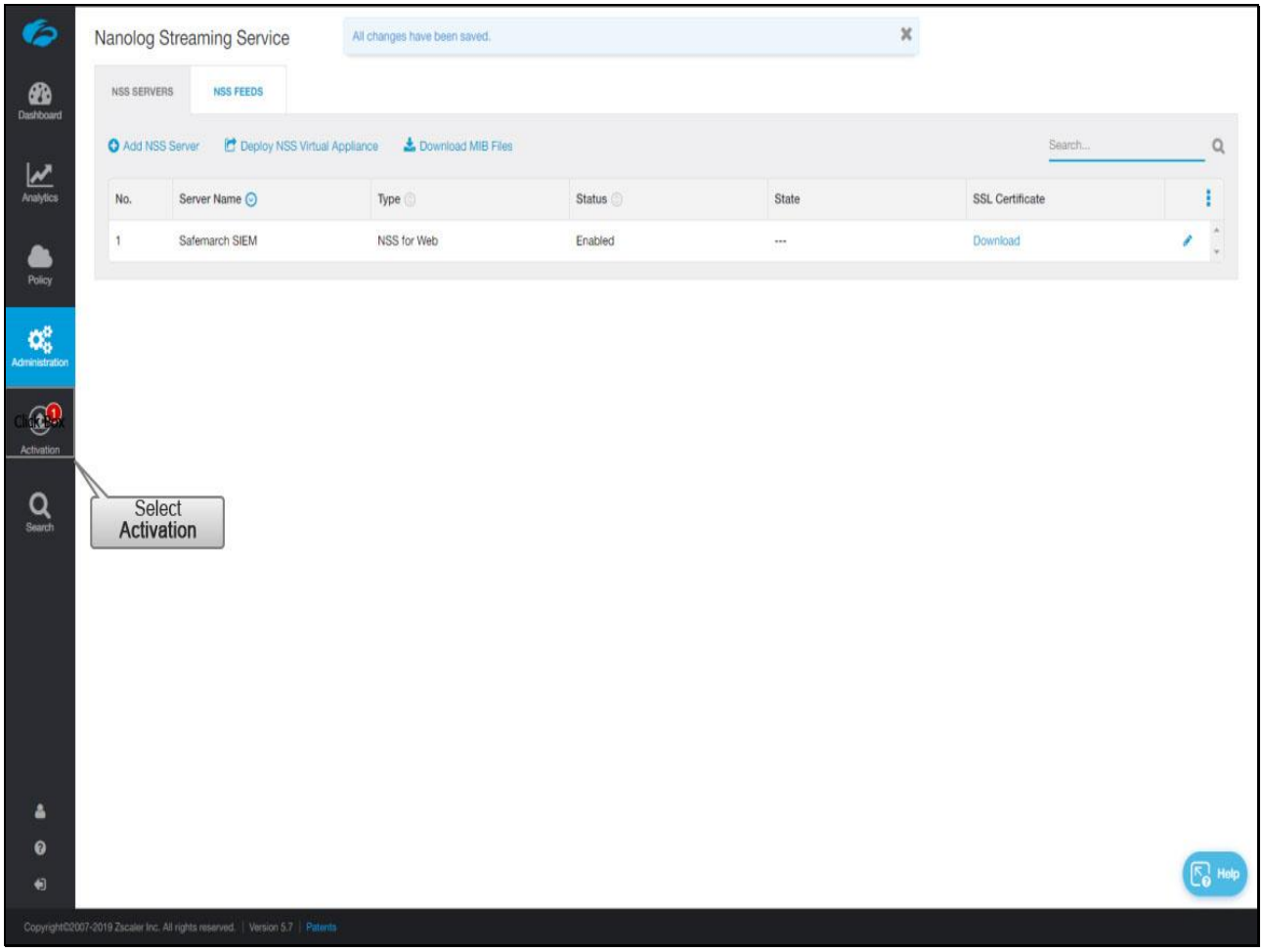
Slide notes

Name this NSS instance



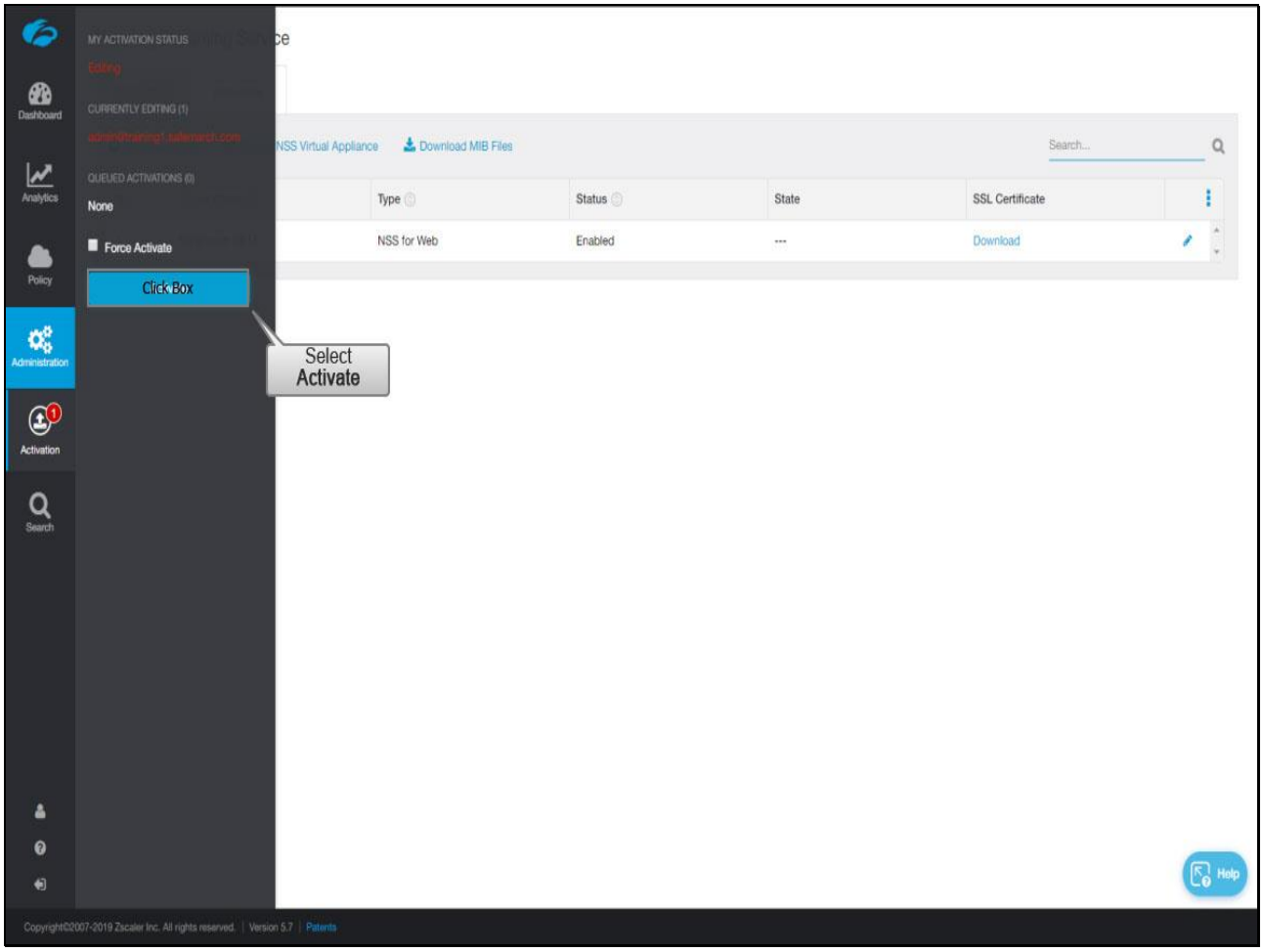
Slide notes

and click “Save”.



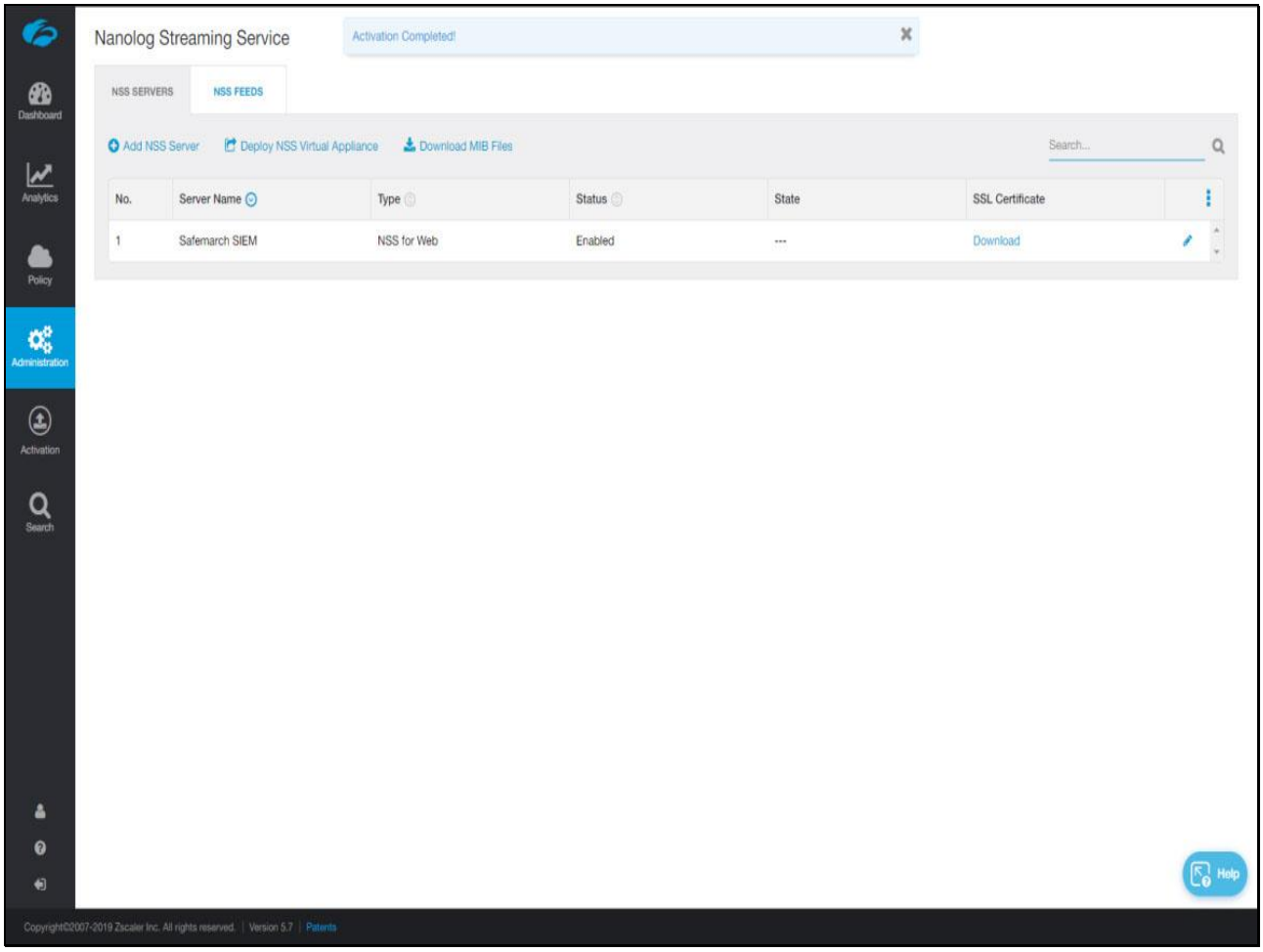
Slide notes

Then **Activate** your changes.


MY ACTIVATION STATUS
Editing
CURRENTLY EDITING (1)
QUEUED ACTIVATIONS (0)
None
Force Activate
Click Box
Select Activate
Dashboard
Analytics
Policy
Administration
Activation
Search
NSS Virtual Appliance
Download MIB Files
Search...
Type
Status
State
SSL Certificate
NSS for Web
Enabled

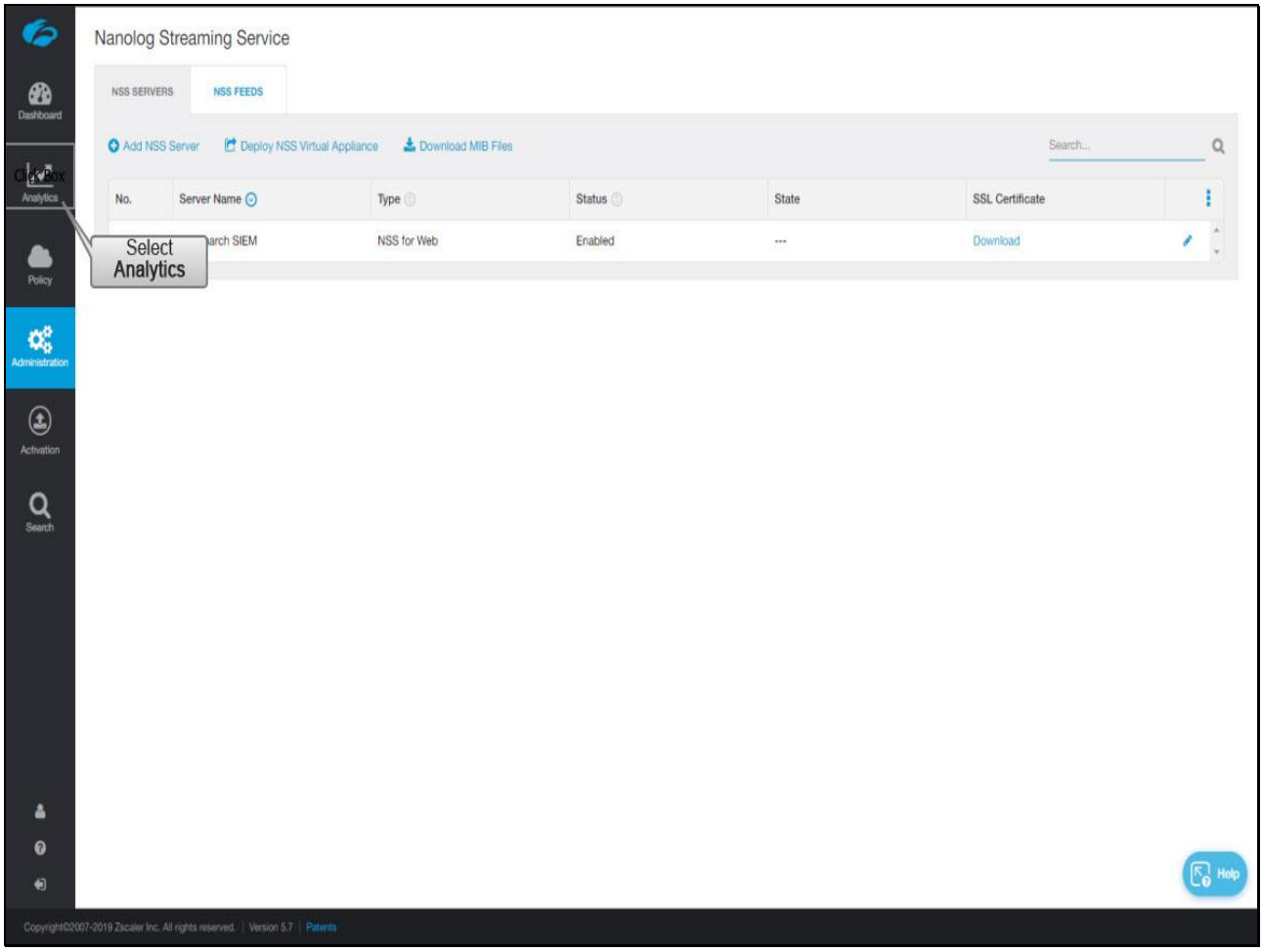
Download
Help
Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents

Slide notes


Nanolog Streaming Service
Activation Completed!
NSS SERVERS
NSS FEEDS
Add NSS Server
Deploy NSS Virtual Appliance
Download MIB Files
Search...
No.
Server Name
Type
Status
State
SSL Certificate
1
Safemarch SIEM
NSS for Web
Enabled

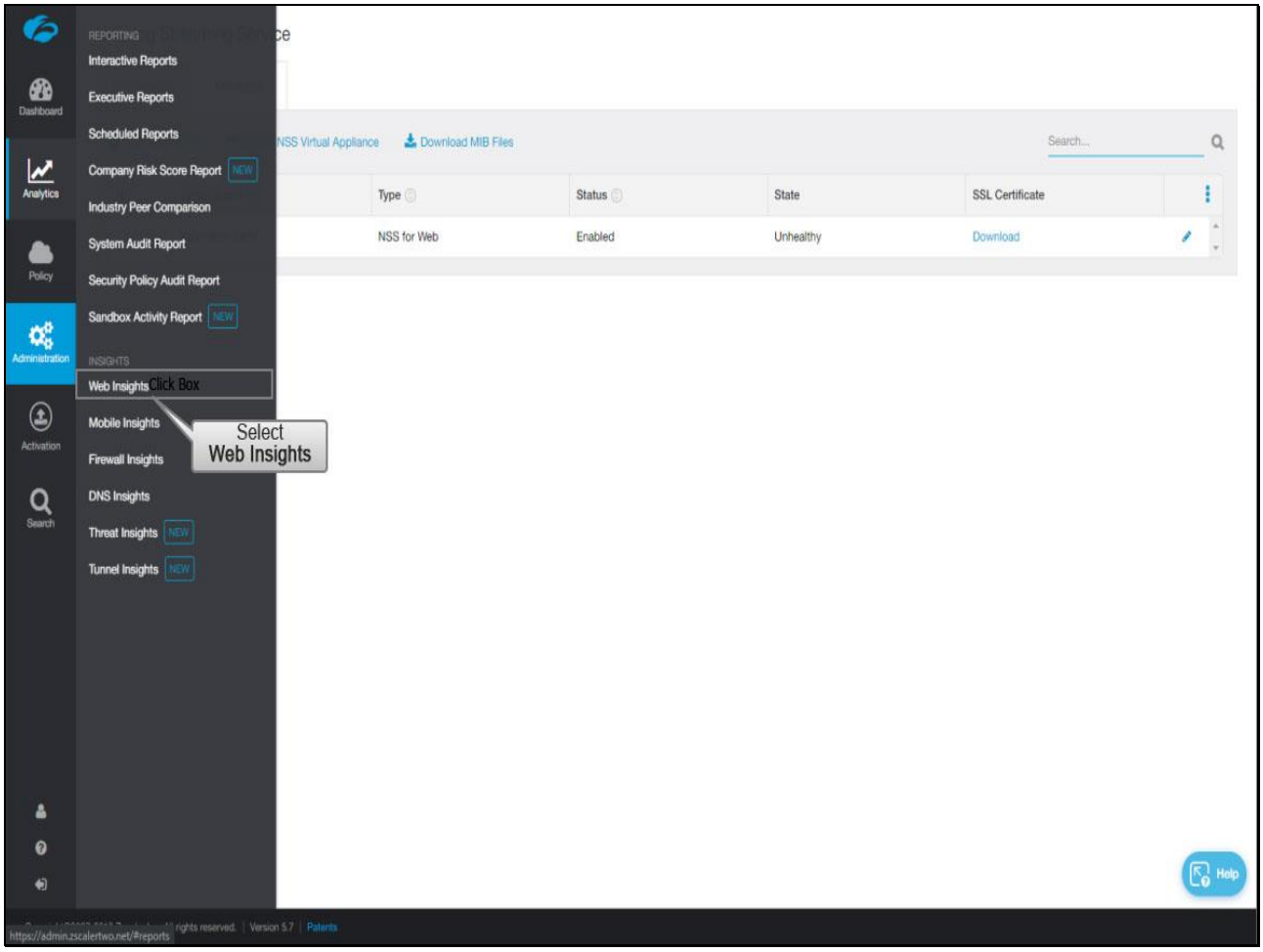
Download
Dashboard
Analytics
Policy
Administration
Activation
Search
Help
Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents

Slide notes



Slide notes

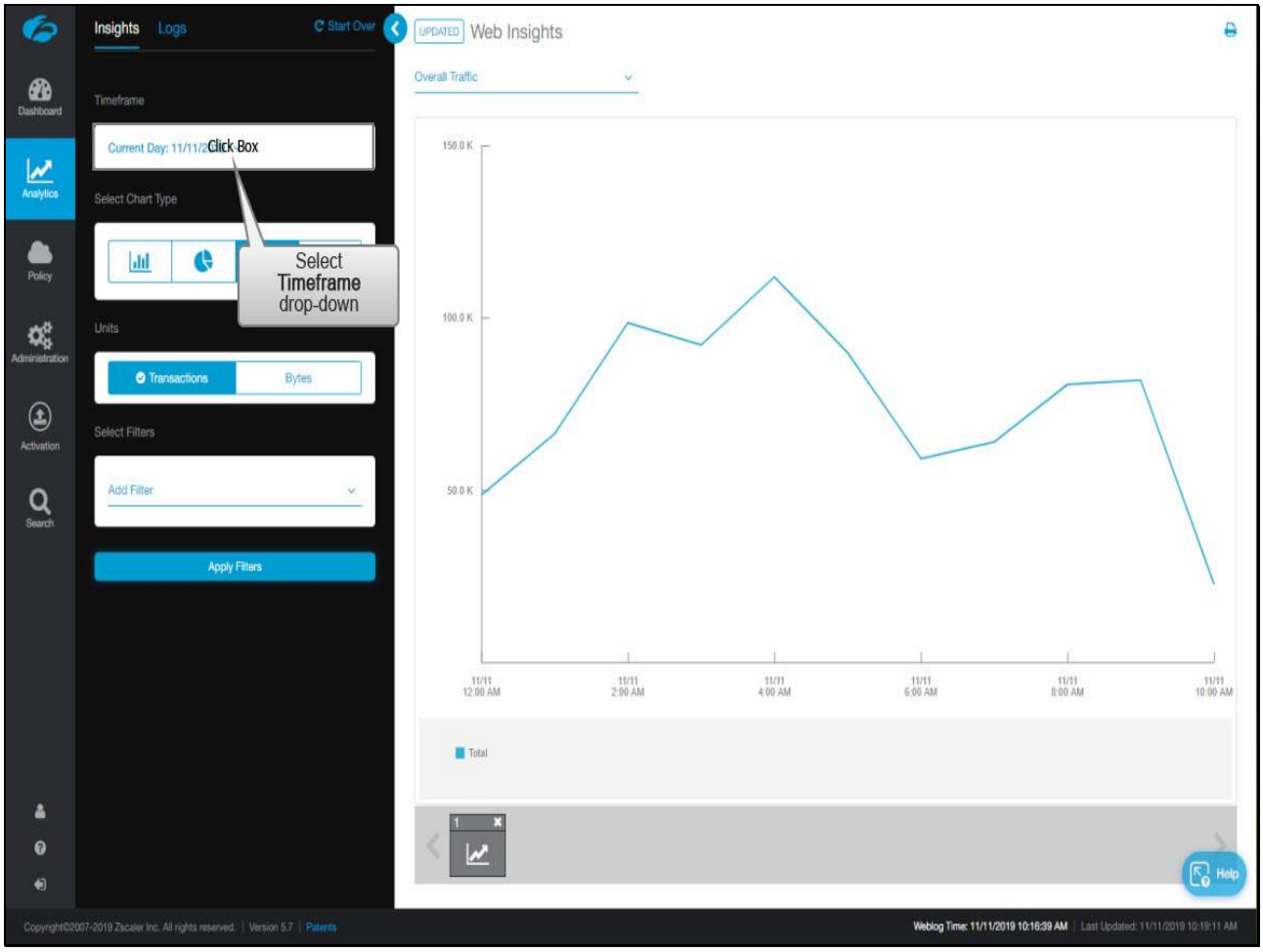
Our next step is to download the VM image. But before we do that, we need to have two data points to correctly size the VM. You will need your number of users and your peak transactions per hour. The first one is pretty straightforward. For the second you can use the Zscaler Admin UI itself to give you the number. Click the Analytics Tab



Slide notes

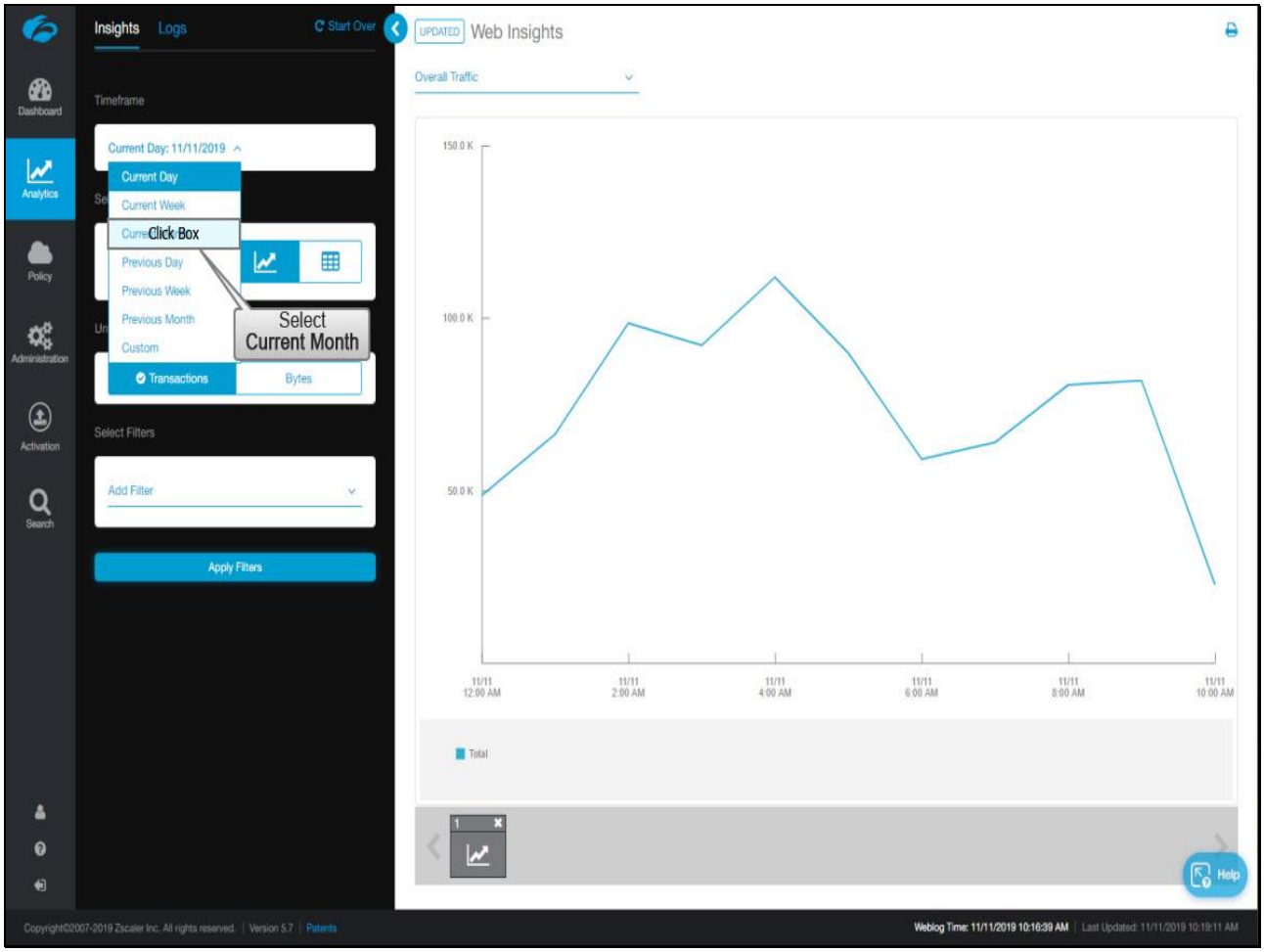
and then click “Web Insights”.

Slide 32 - Slide 32



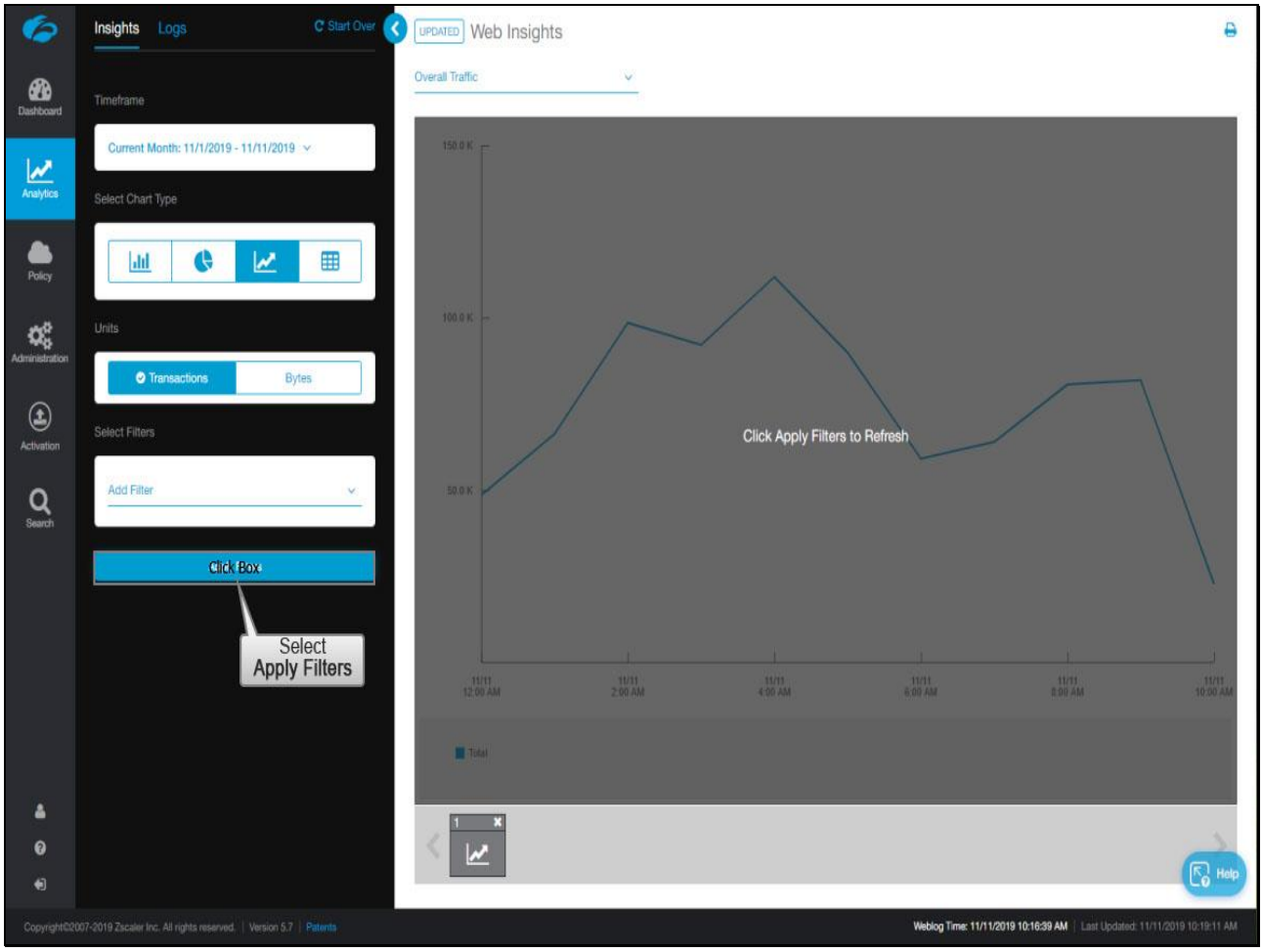
Slide notes

Try a variety of timeframes and note the peaks. You don't need to be super exact – you're basically looking for orders of magnitude; are you going 500,000 or 5,000,000 transactions per hour?



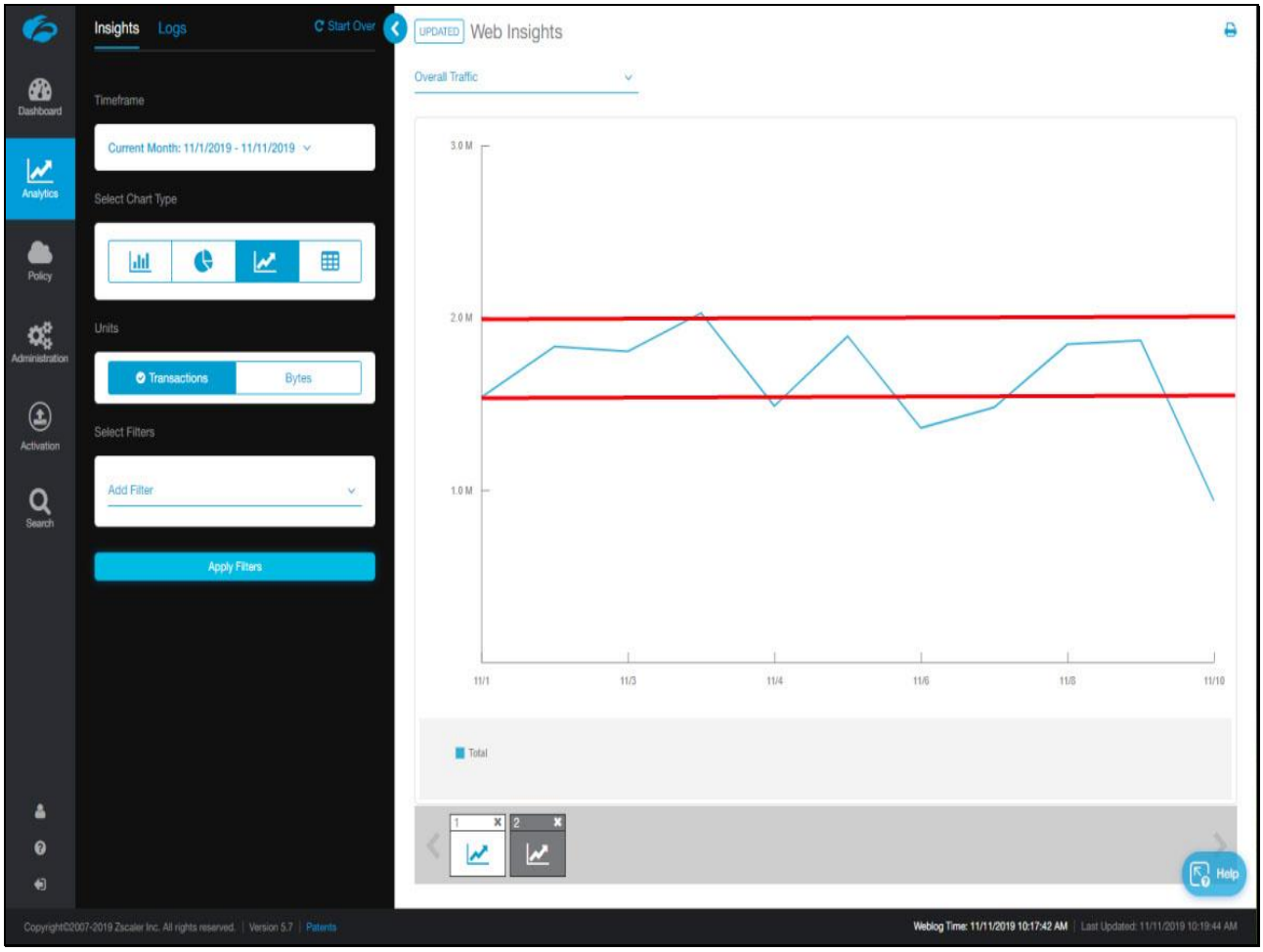
Slide notes

Click on “Current Month”.



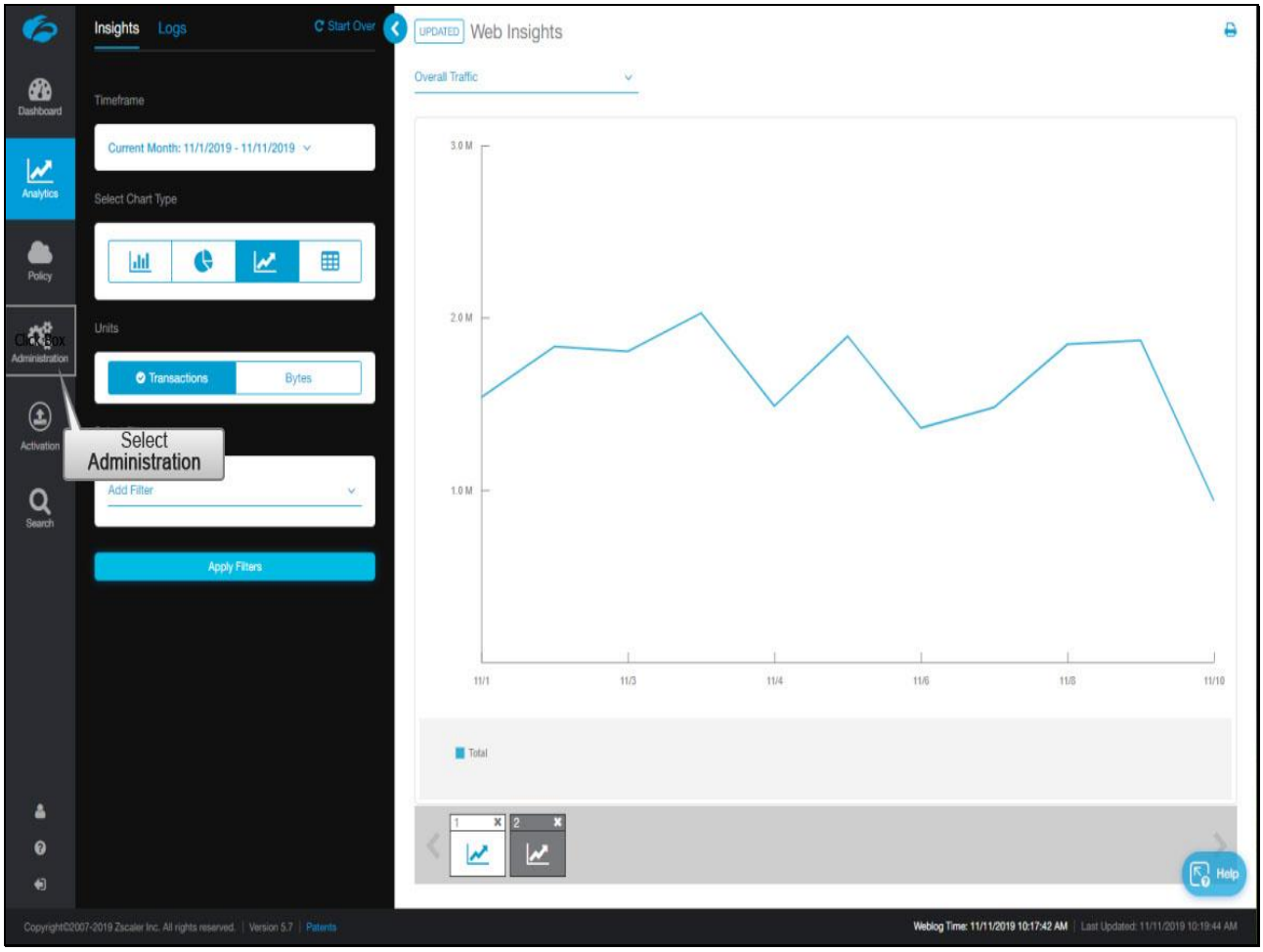
Slide notes

Then click “Apply Filters”.



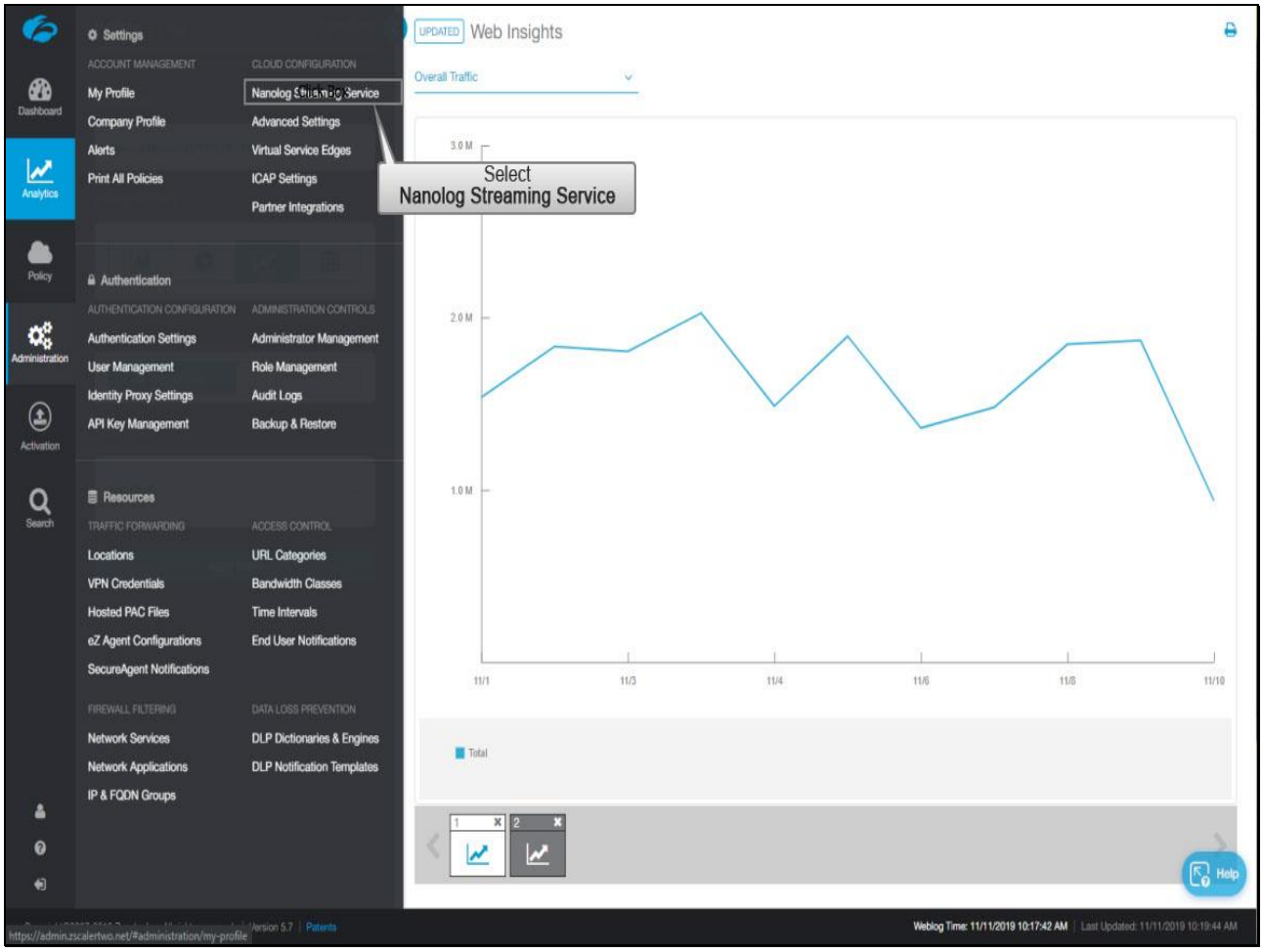
Slide notes

Note that your average number of transactions over the past month was around one and a half million with a peak of around 2 million. Note down 2 million for this example.

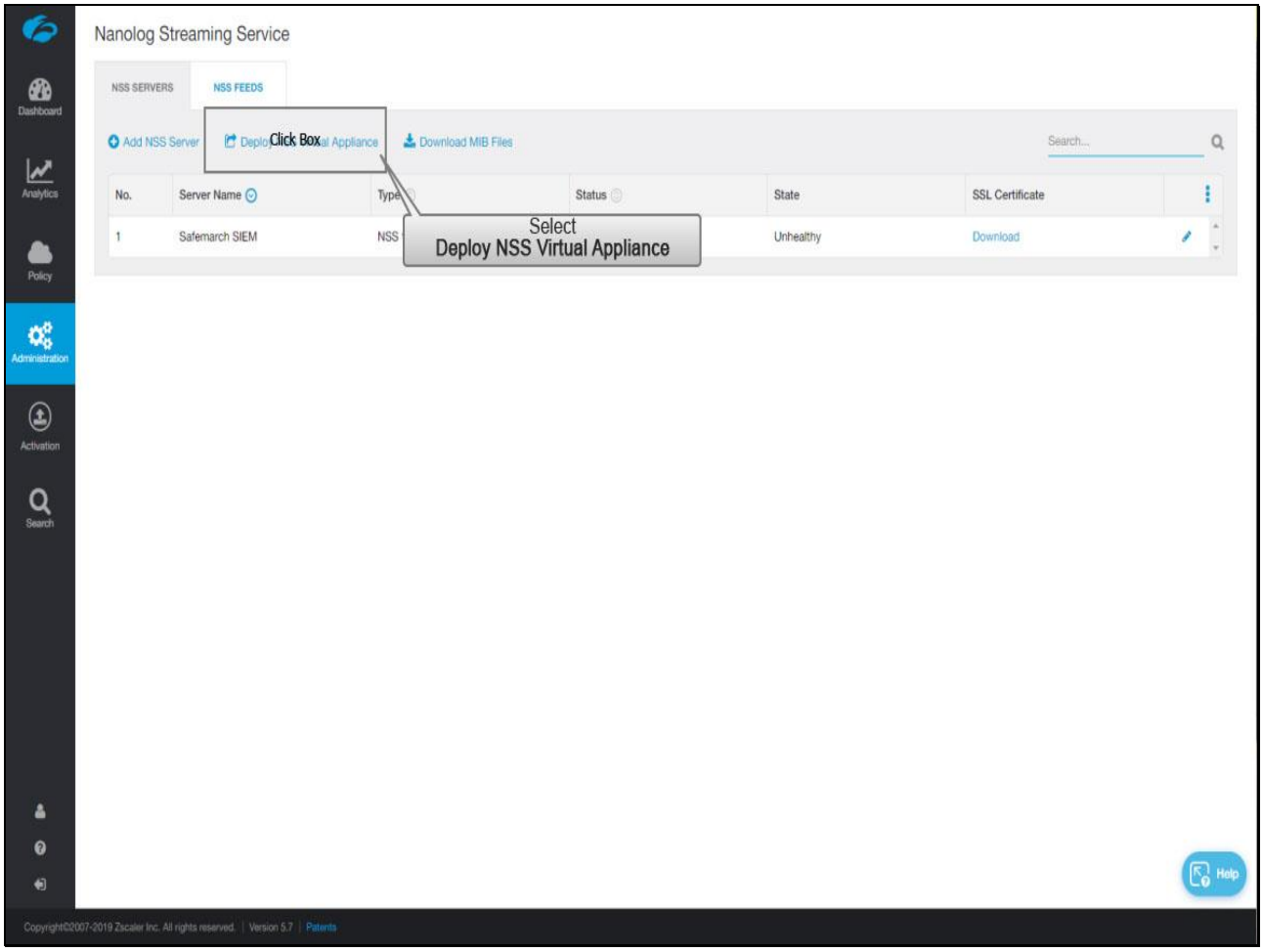


Slide notes

Let’s head back over to the NSS page.

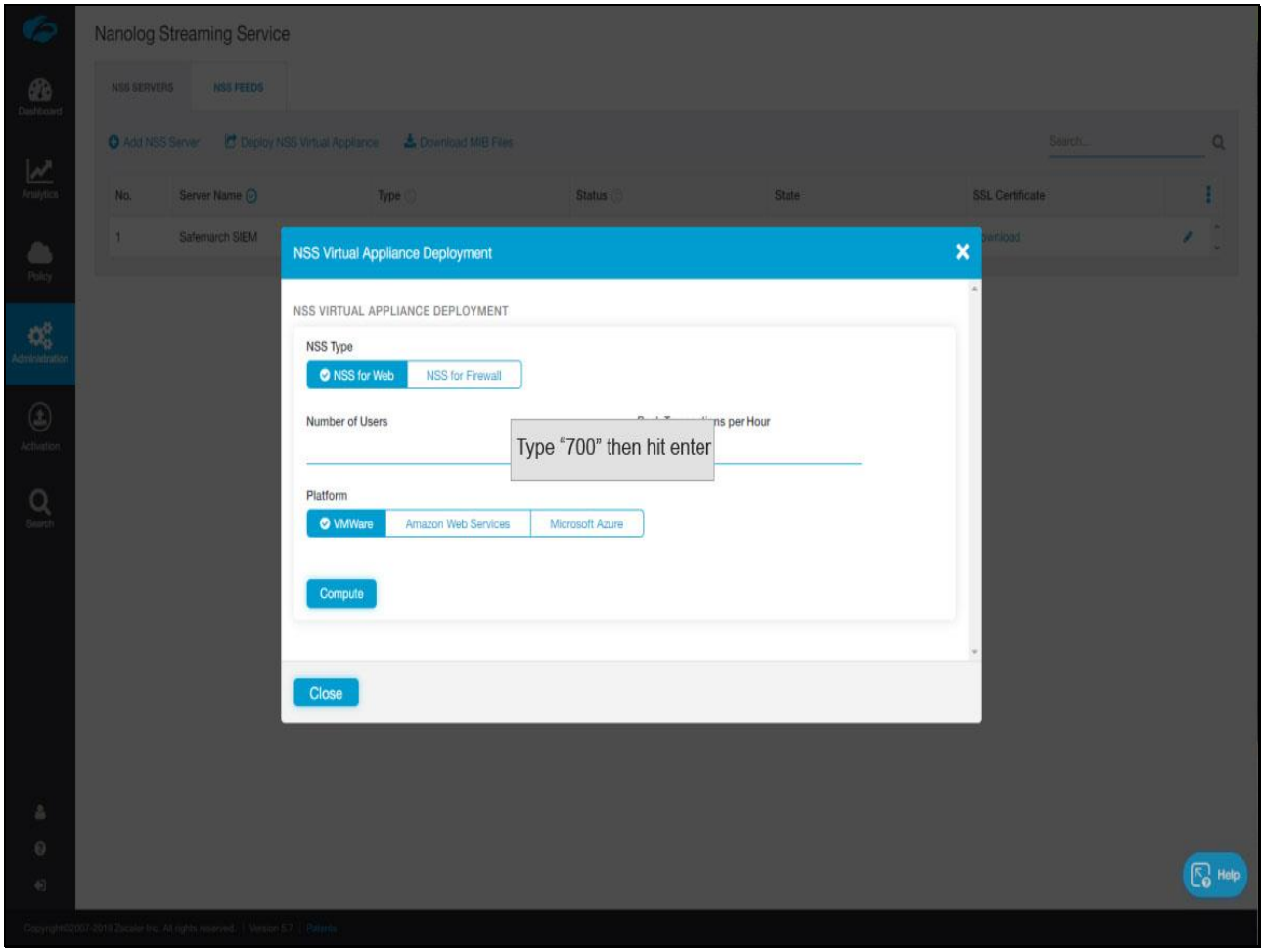

Settings
ACCOUNT MANAGEMENT
My Profile
Company Profile
Alerts
Print All Policies
CLOUD CONFIGURATION
Nanolog Streaming Service
Advanced Settings
Virtual Service Edges
ICAP Settings
Partner Integrations
Authentication
AUTHENTICATION CONFIGURATION
Authentication Settings
User Management
Identity Proxy Settings
API Key Management
ADMINISTRATION CONTROLS
Administrator Management
Role Management
Audit Logs
Backup & Restore
Resources
TRAFFIC FORWARDING
Locations
VPN Credentials
Hosted PAC Files
eZ Agent Configurations
SecureAgent Notifications
ACCESS CONTROL
URL Categories
Bandwidth Classes
Time Intervals
End User Notifications
FIREWALL FILTERING
Network Services
Network Applications
IP & FQDN Groups
DATA LOSS PREVENTION
DLP Dictionaries & Engines
DLP Notification Templates
Dashboard
Analytics
Policy
Administration
Activation
Search
UPDATED
Web Insights
Overall Traffic
Select
Nanolog Streaming Service
3.0 M
2.0 M
1.0 M
11/1
11/3
11/4
11/6
11/8
11/10
Total
Help
Weblog Time: 11/11/2019 10:17:42 AM
Last Updated: 11/11/2019 10:19:44 AM
https://admin.zscalertwo.net/#administration/my-profile

Slide notes



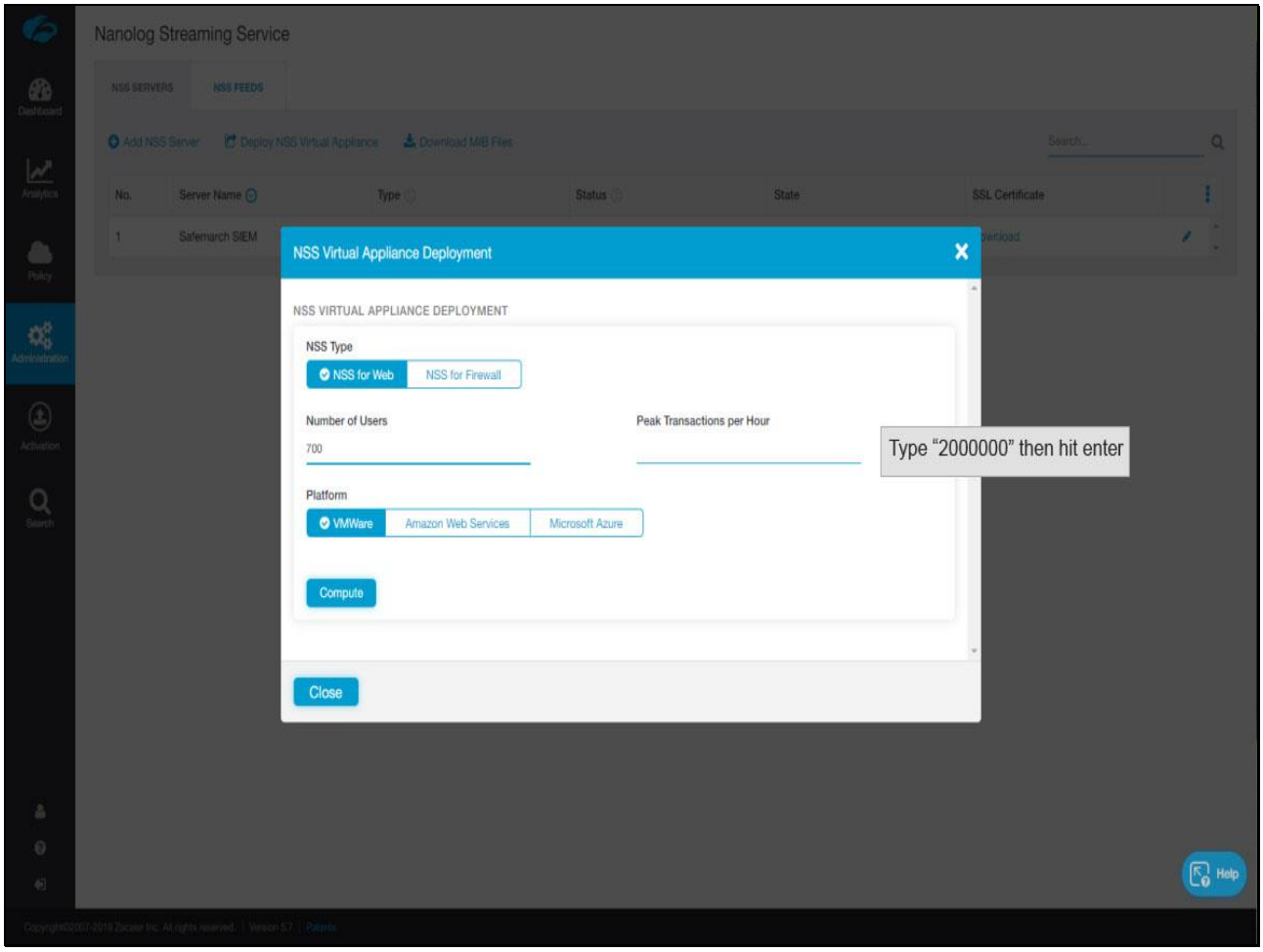
Slide notes

Click Deploy NSS Virtual Appliance.



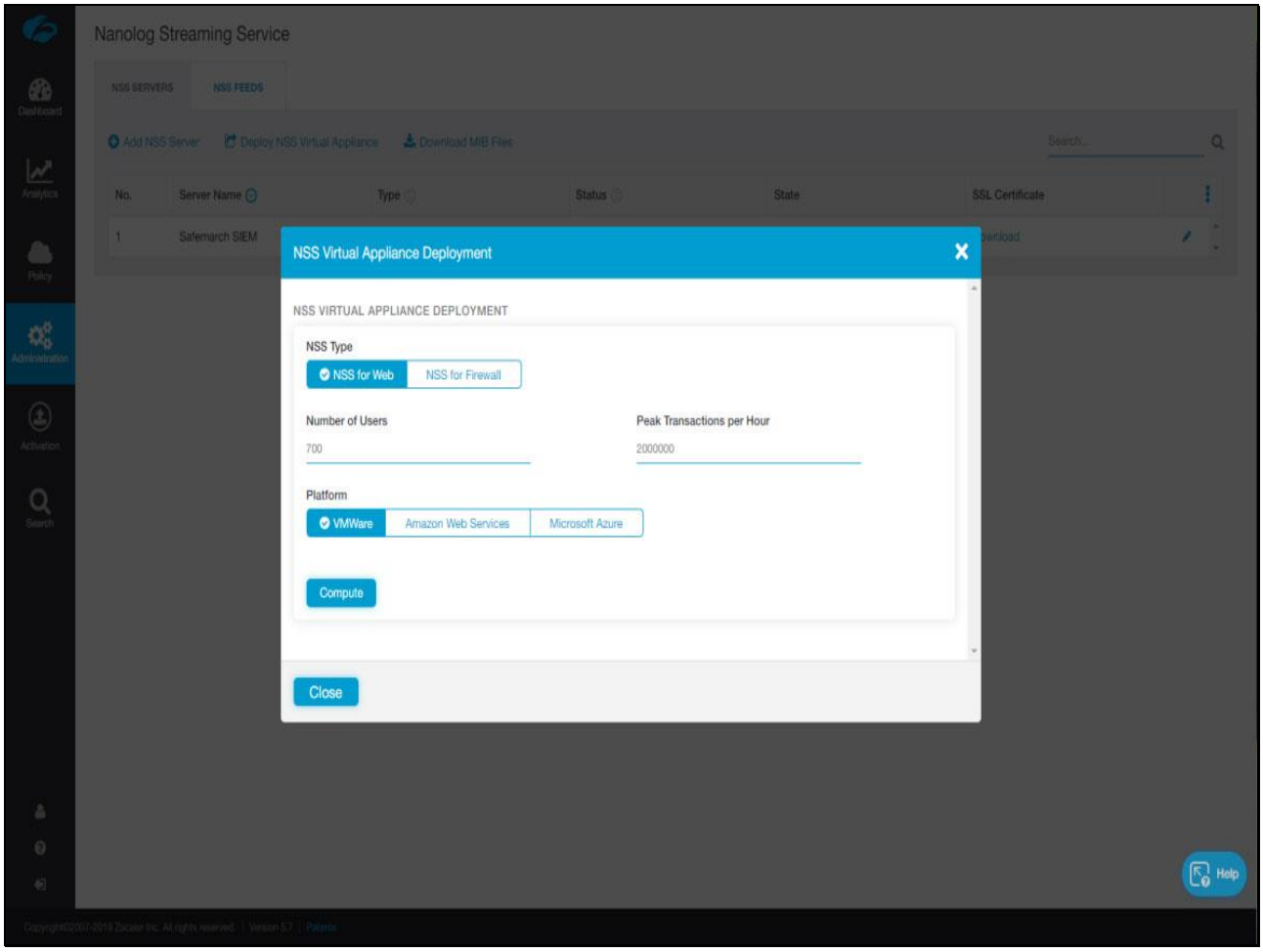
Slide notes

Let's assume that we are protecting 700 users in this organization. Enter 700 in the "Number of Users" field.



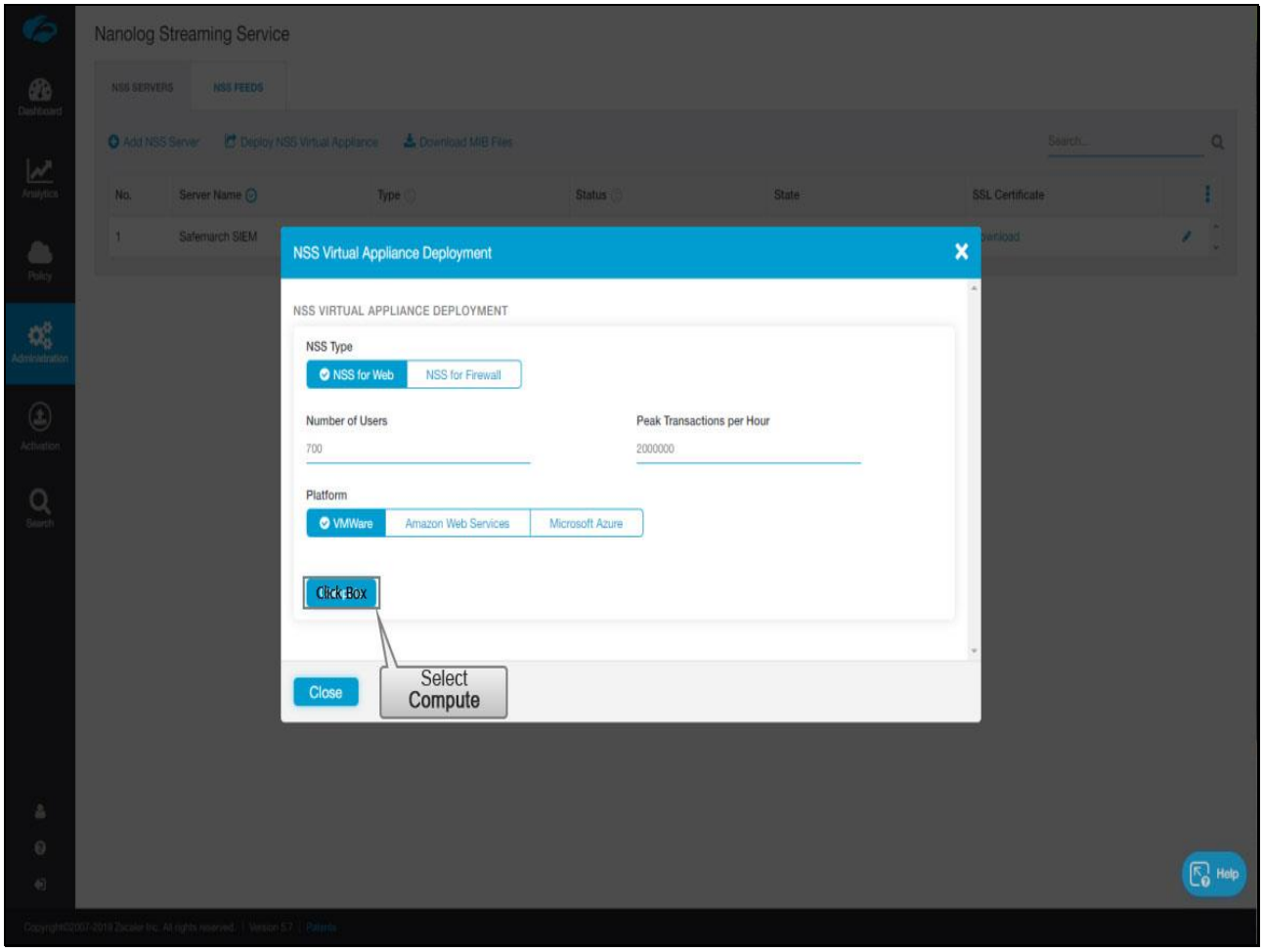
Slide notes

and 2,000,000 transactions.



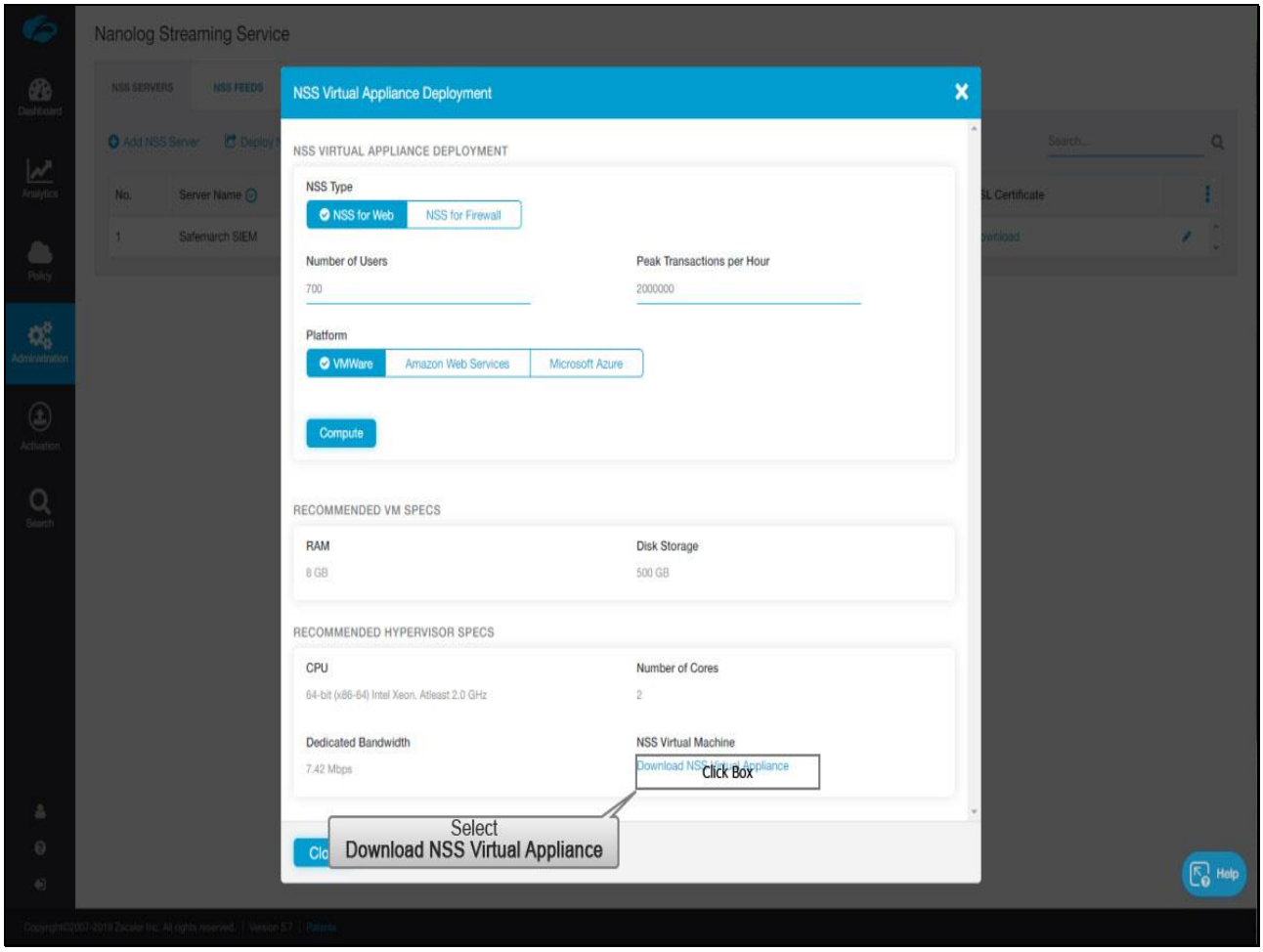
Slide notes

You can select between deploying an on-premise VM instance, in AWS, or in Microsoft Azure. For this demo, we will use VMWare.



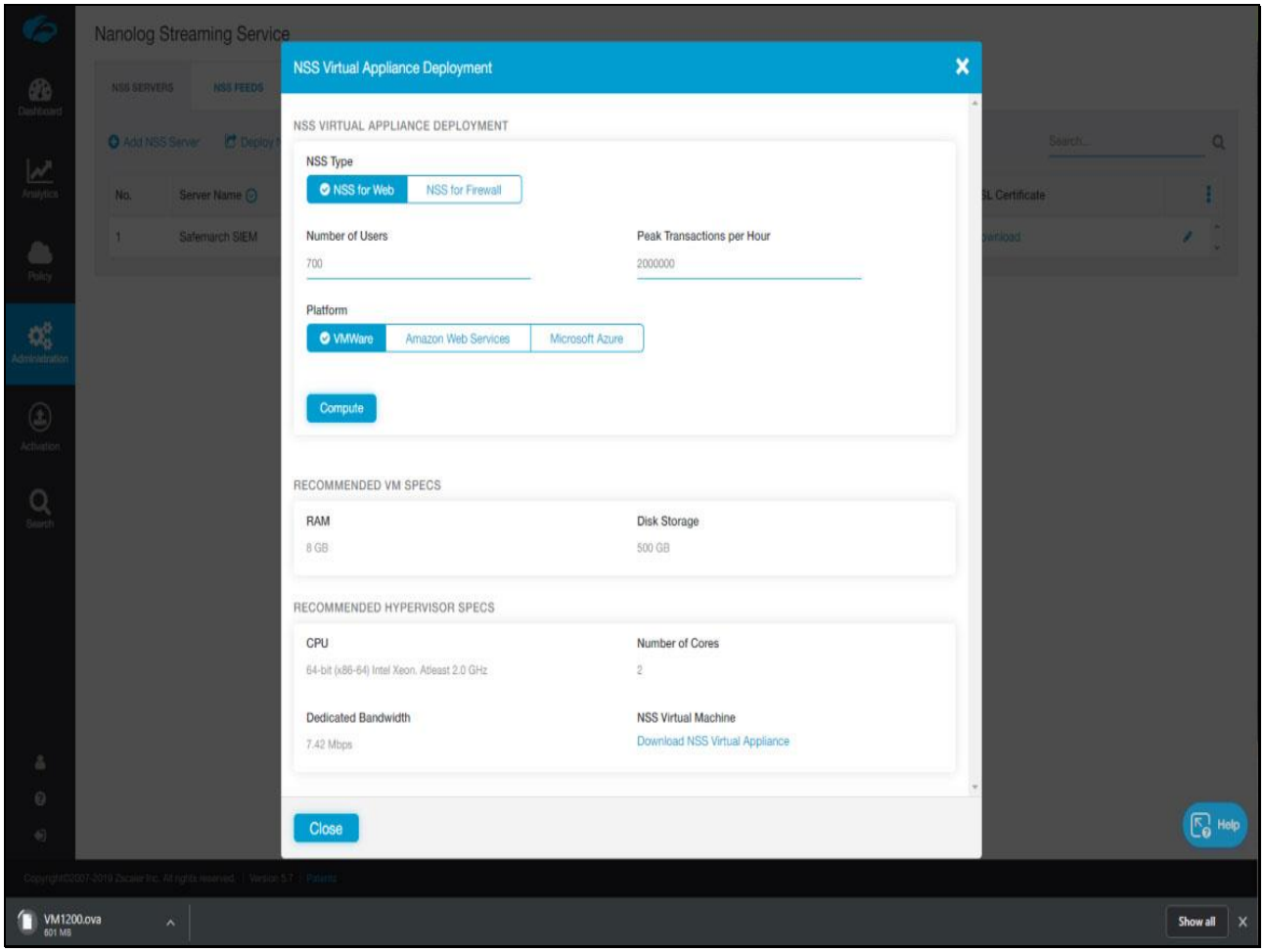
Slide notes

and click “Compute”.

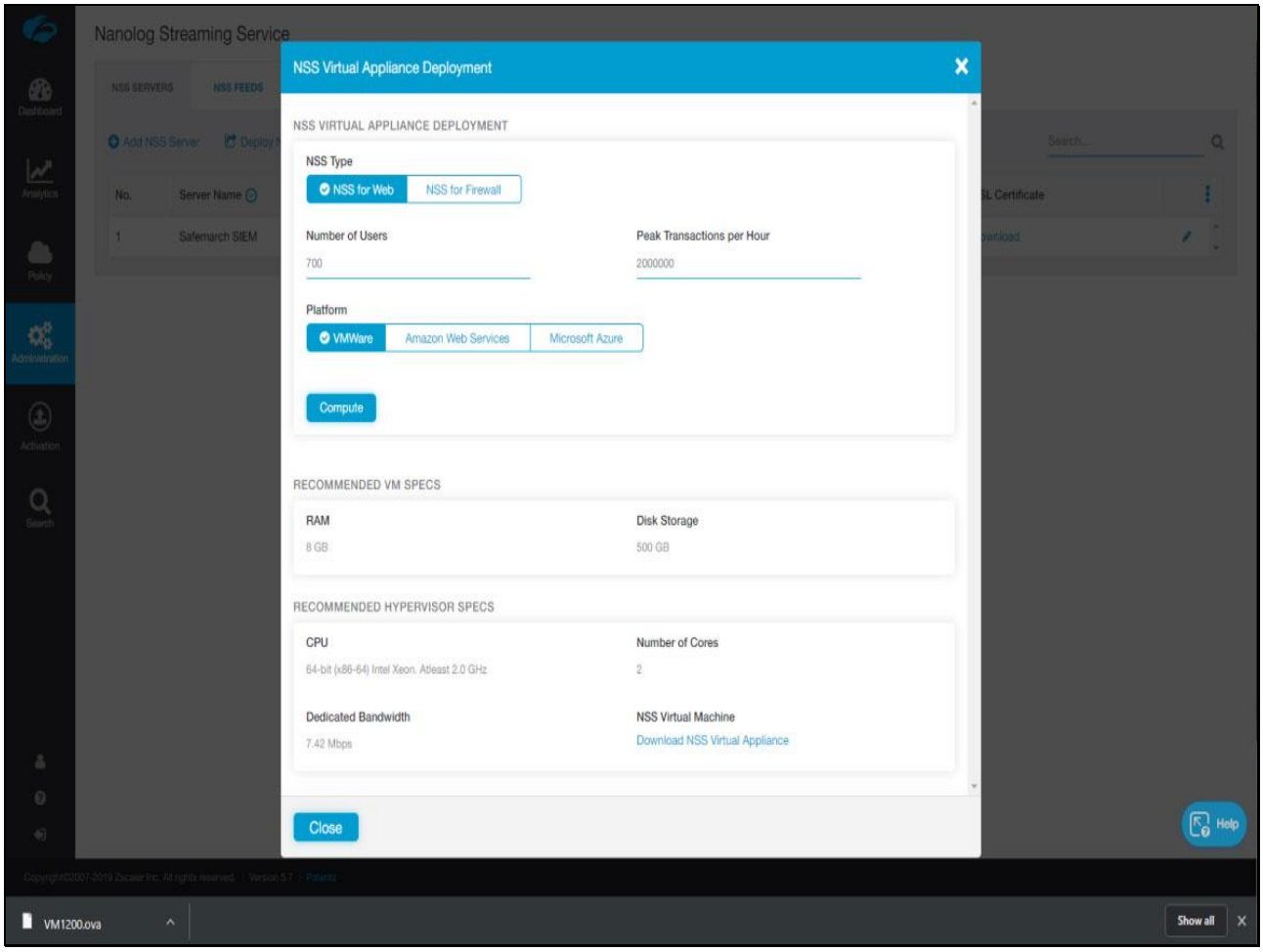


Slide notes

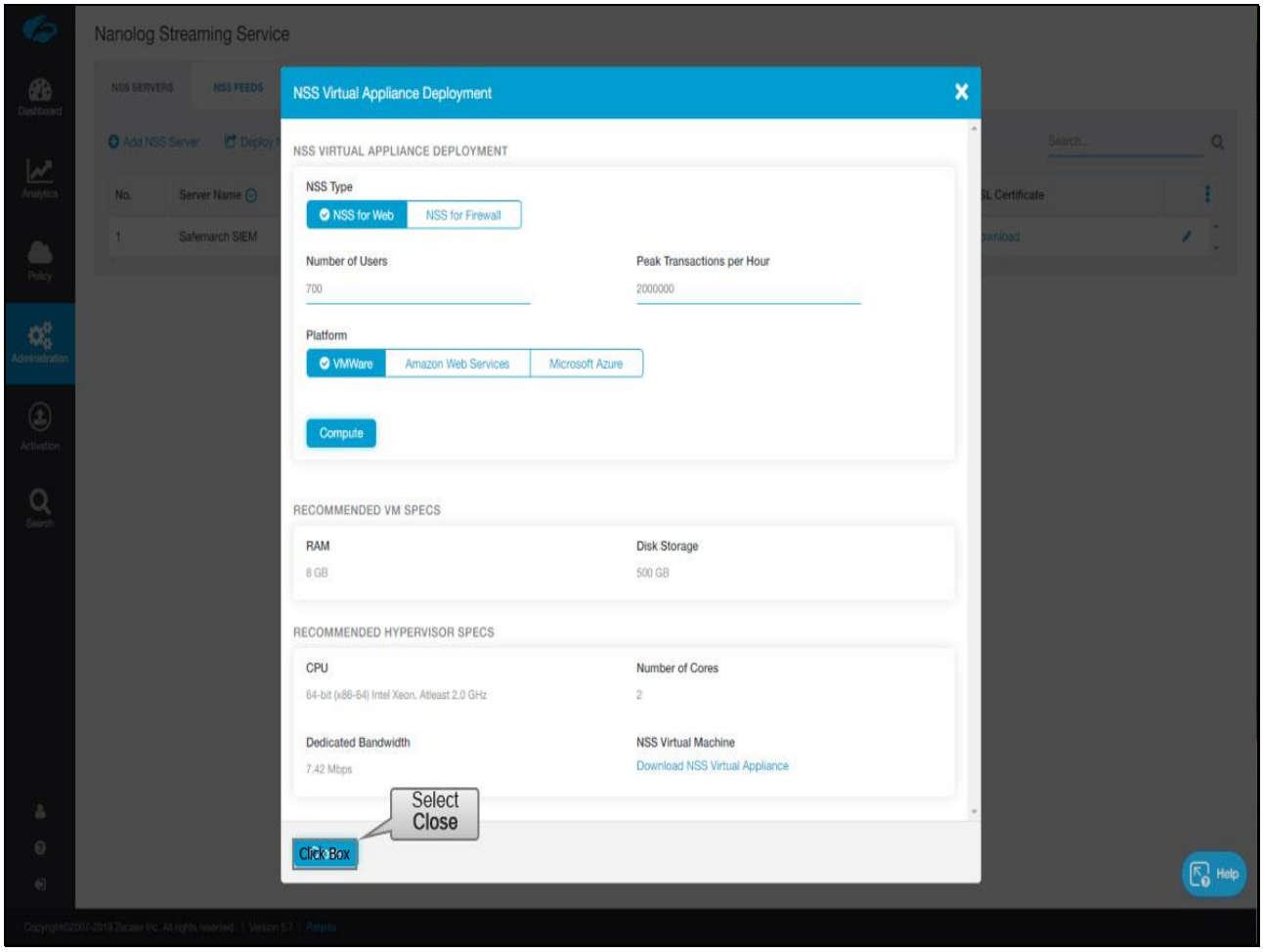
The VM specs will be listed there. Once you've made a note of the specs click "Download NSS Virtual Appliance".


Nanolog Streaming Service
NSS SERVERS
NSS FEEDS
Add NSS Server
No.
Server Name
1
Safemarch SIEM
NSS Virtual Appliance Deployment
NSS VIRTUAL APPLIANCE DEPLOYMENT
NSS Type
NSS for Web
NSS for Firewall
Number of Users
700
Peak Transactions per Hour
2000000
Platform
VMWare
Amazon Web Services
Microsoft Azure
Compute
RECOMMENDED VM SPECS
RAM
8 GB
Disk Storage
500 GB
RECOMMENDED HYPERVISOR SPECS
CPU
64-bit (x86-64) Intel Xeon. Atleast 2.0 GHz
Number of Cores
2
Dedicated Bandwidth
7.42 Mbps
NSS Virtual Machine
Download NSS Virtual Appliance
Close
Help
VM1200.ova
601 MB
Show all

Slide notes

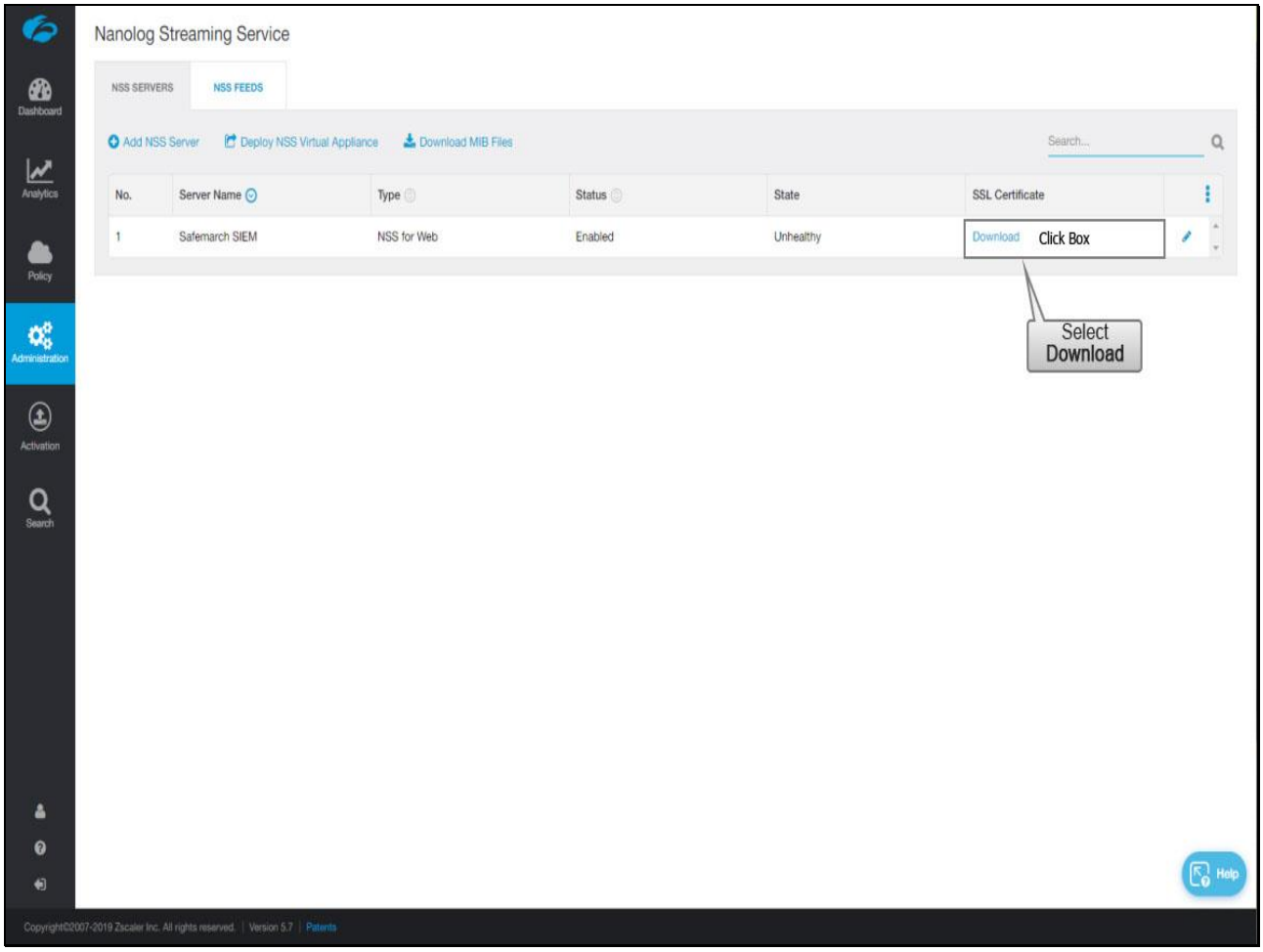

Nanolog Streaming Service
NSS SERVERS
NSS FEEDS
Add NSS Server
No.
Server Name
1
Safemarch SIEM
NSS Virtual Appliance Deployment
NSS VIRTUAL APPLIANCE DEPLOYMENT
NSS Type
NSS for Web
NSS for Firewall
Number of Users
700
Peak Transactions per Hour
2000000
Platform
VMWare
Amazon Web Services
Microsoft Azure
Compute
RECOMMENDED VM SPECS
RAM
8 GB
Disk Storage
500 GB
RECOMMENDED HYPERVISOR SPECS
CPU
64-bit (x86-64) Intel Xeon. Atleast 2.0 GHz
Number of Cores
2
Dedicated Bandwidth
7.42 Mbps
NSS Virtual Machine
Download NSS Virtual Appliance
Close
Help
VM1200.ova
Show all

Slide notes



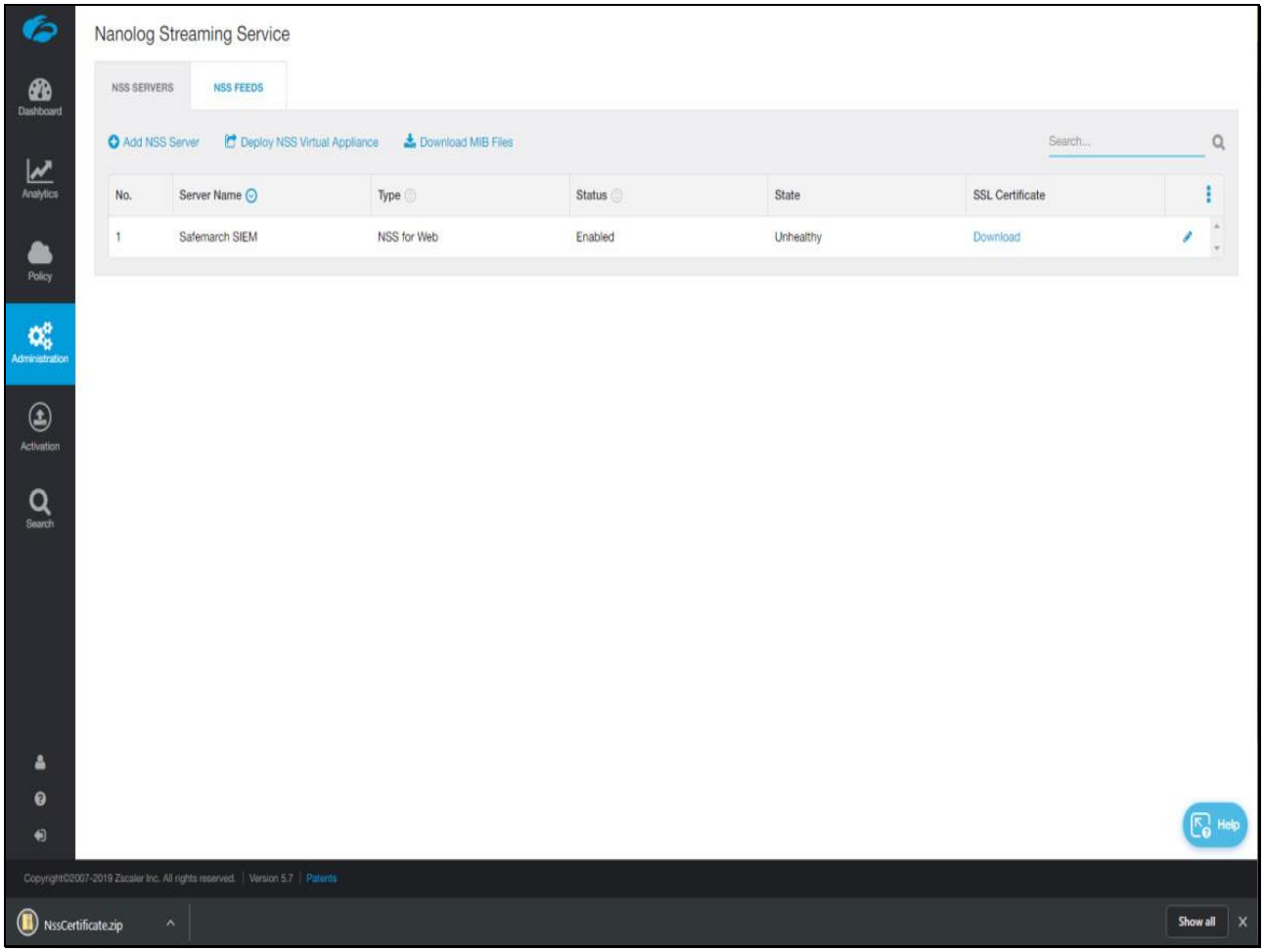
Slide notes

Click “Close”.

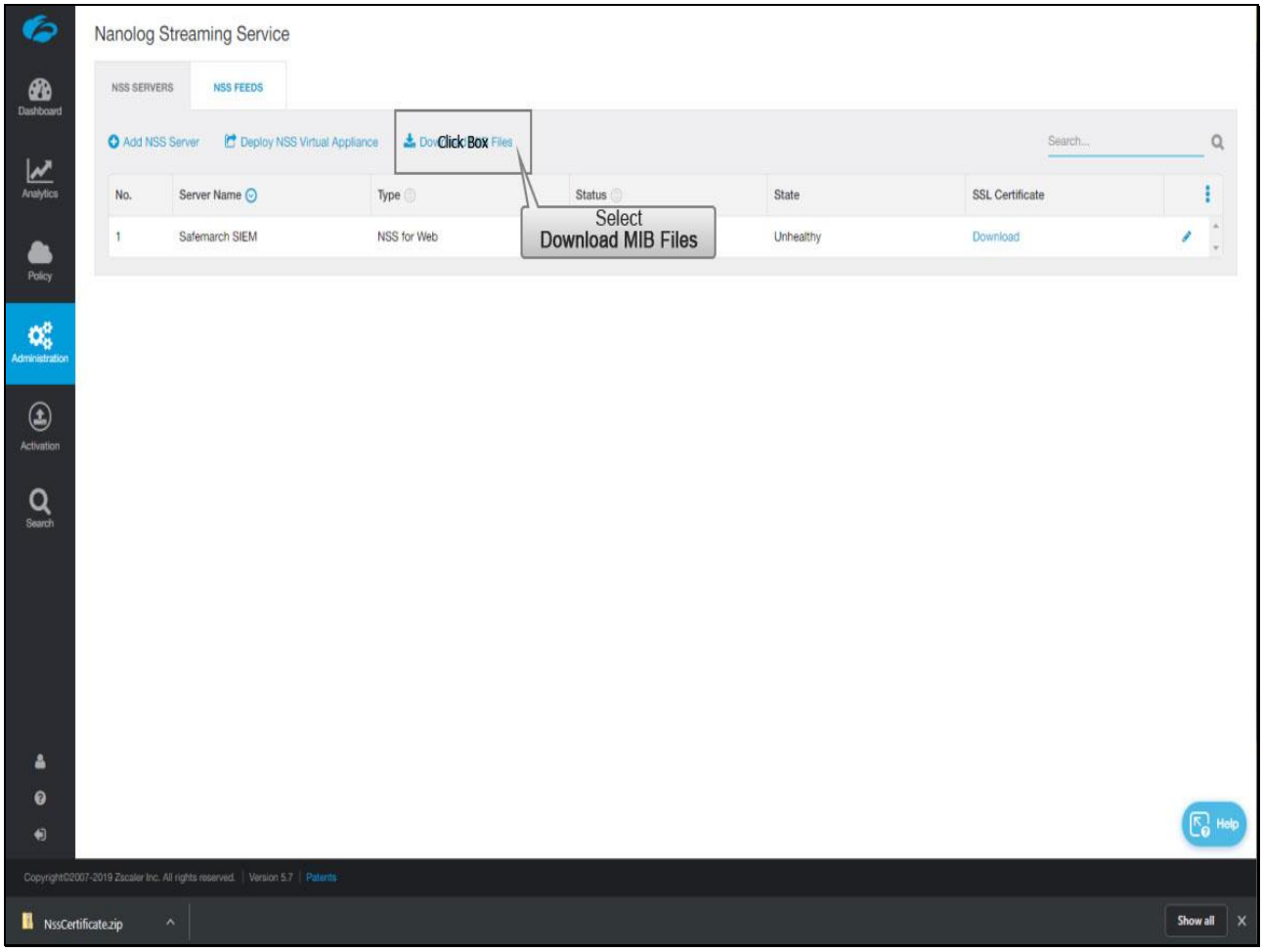


Slide notes

Next, Download the SSL client certificate.

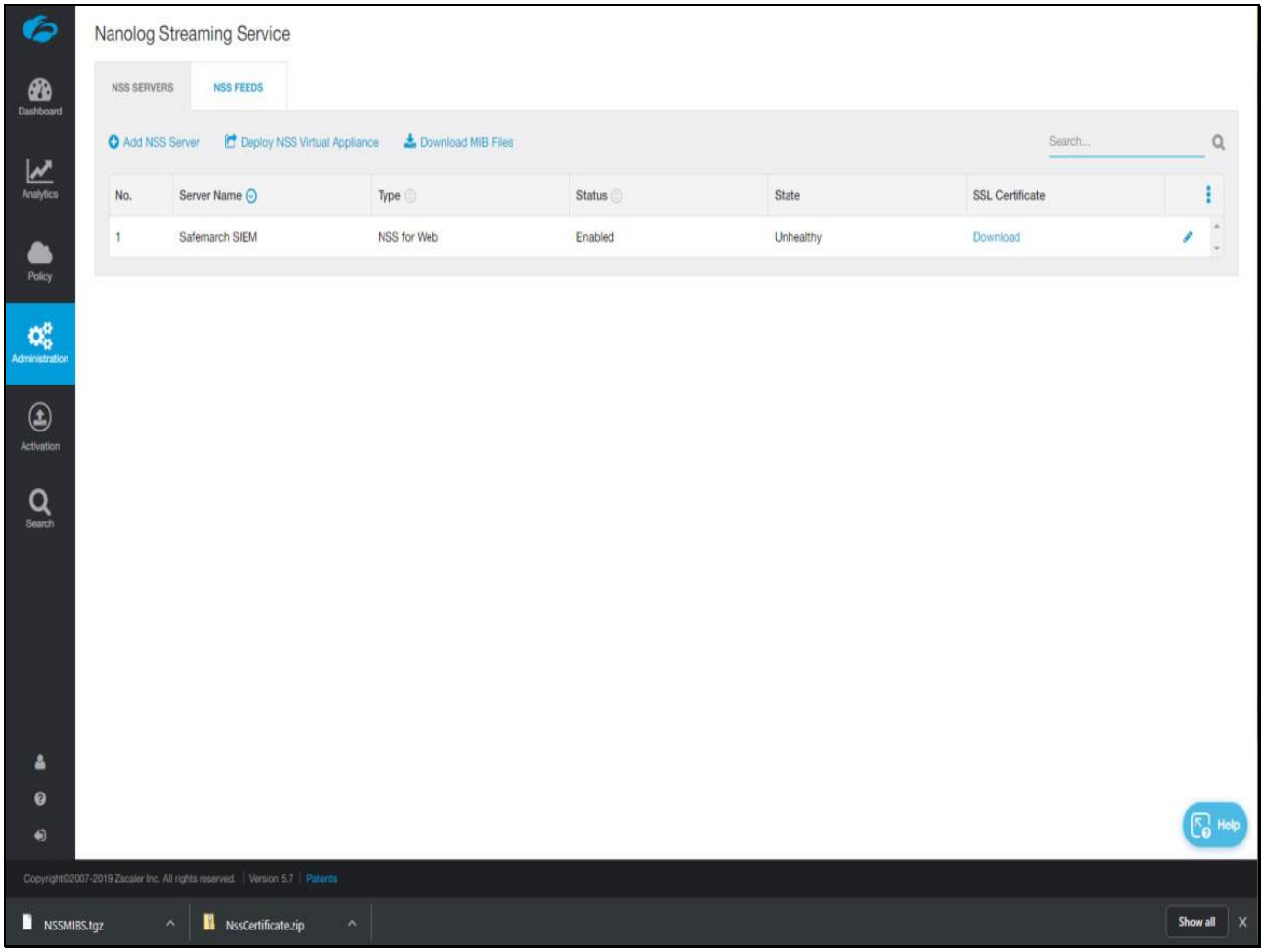

Nanolog Streaming Service
NSS SERVERS
NSS FEEDS
Add NSS Server
Deploy NSS Virtual Appliance
Download MIB Files
Search...
No.
Server Name
Type
Status
State
SSL Certificate
1
Safemarch SIEM
NSS for Web
Enabled
Unhealthy
Download
Dashboard
Analytics
Policy
Administration
Activation
Search
Help
Copyright©2007-2019 Zscaler Inc. All rights reserved.
Version 5.7
Patents
NssCertificate.zip
Show all

Slide notes

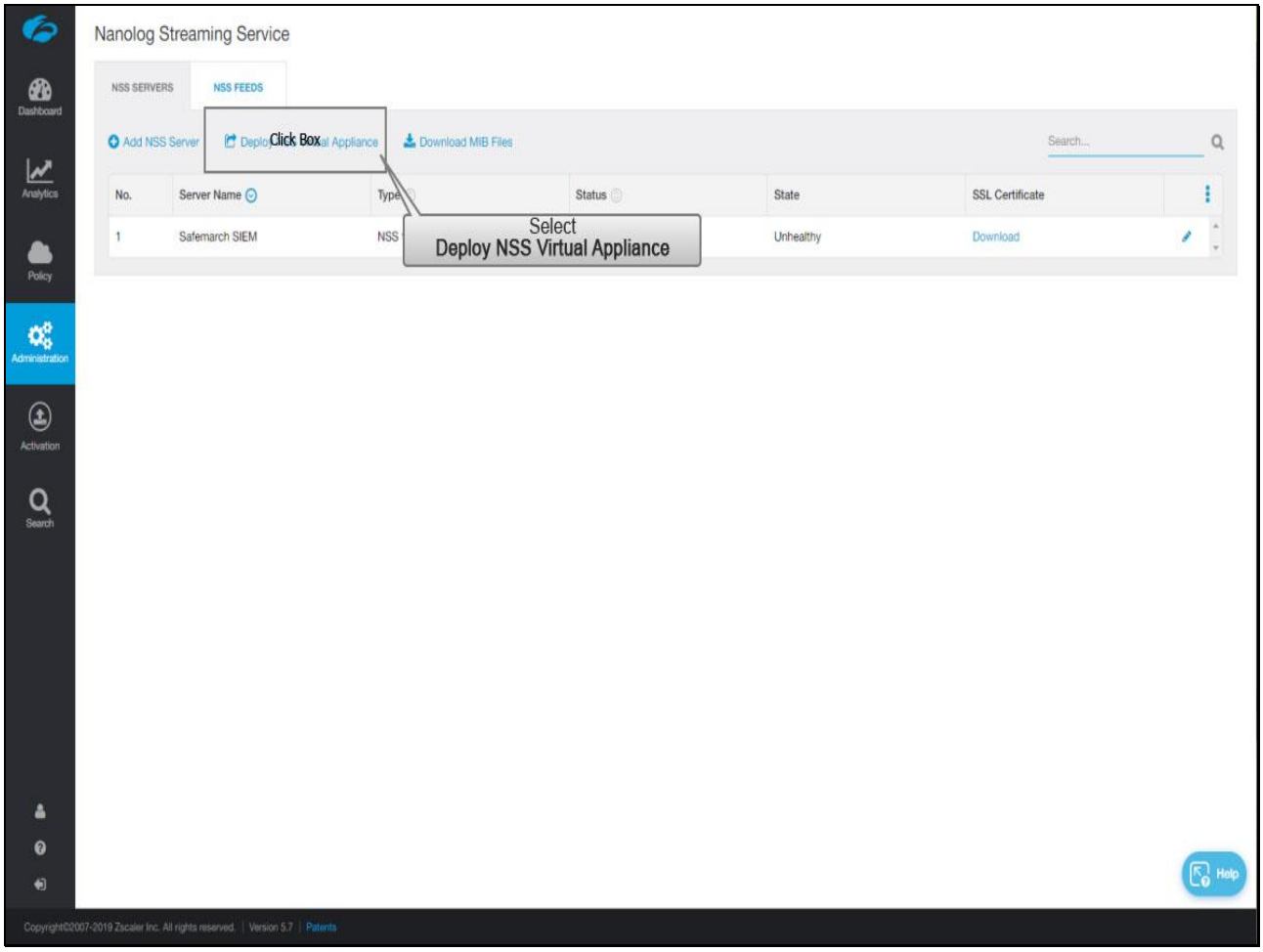


Slide notes

If you would like to monitor your NSS via SNMP, download a copy of the Zscaler NSS MIB for import into your SNMP manager. Click Download MIB Files.

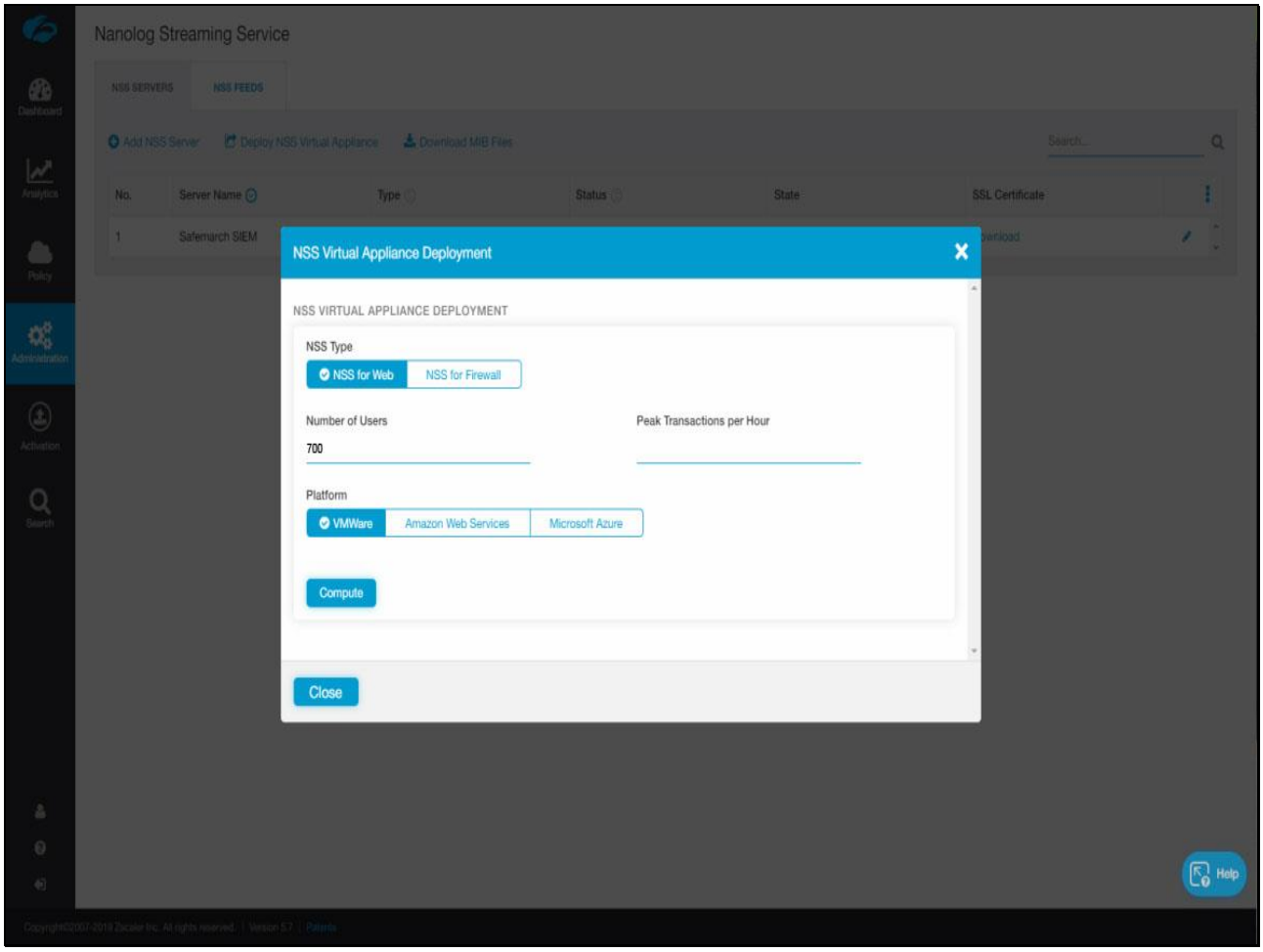

Nanolog Streaming Service
NSS SERVERS
NSS FEEDS
Add NSS Server
Deploy NSS Virtual Appliance
Download MIB Files
Search...
No.
Server Name
Type
Status
State
SSL Certificate
1
Safemarch SIEM
NSS for Web
Enabled
Unhealthy
Download
Dashboard
Analytics
Policy
Administration
Activation
Search
Help
Copyright©2007-2019 Zscaler Inc. All rights reserved.
Version 5.7
Patents
NSSMIBS.tgz
NssCertificate.zip
Show all

Slide notes



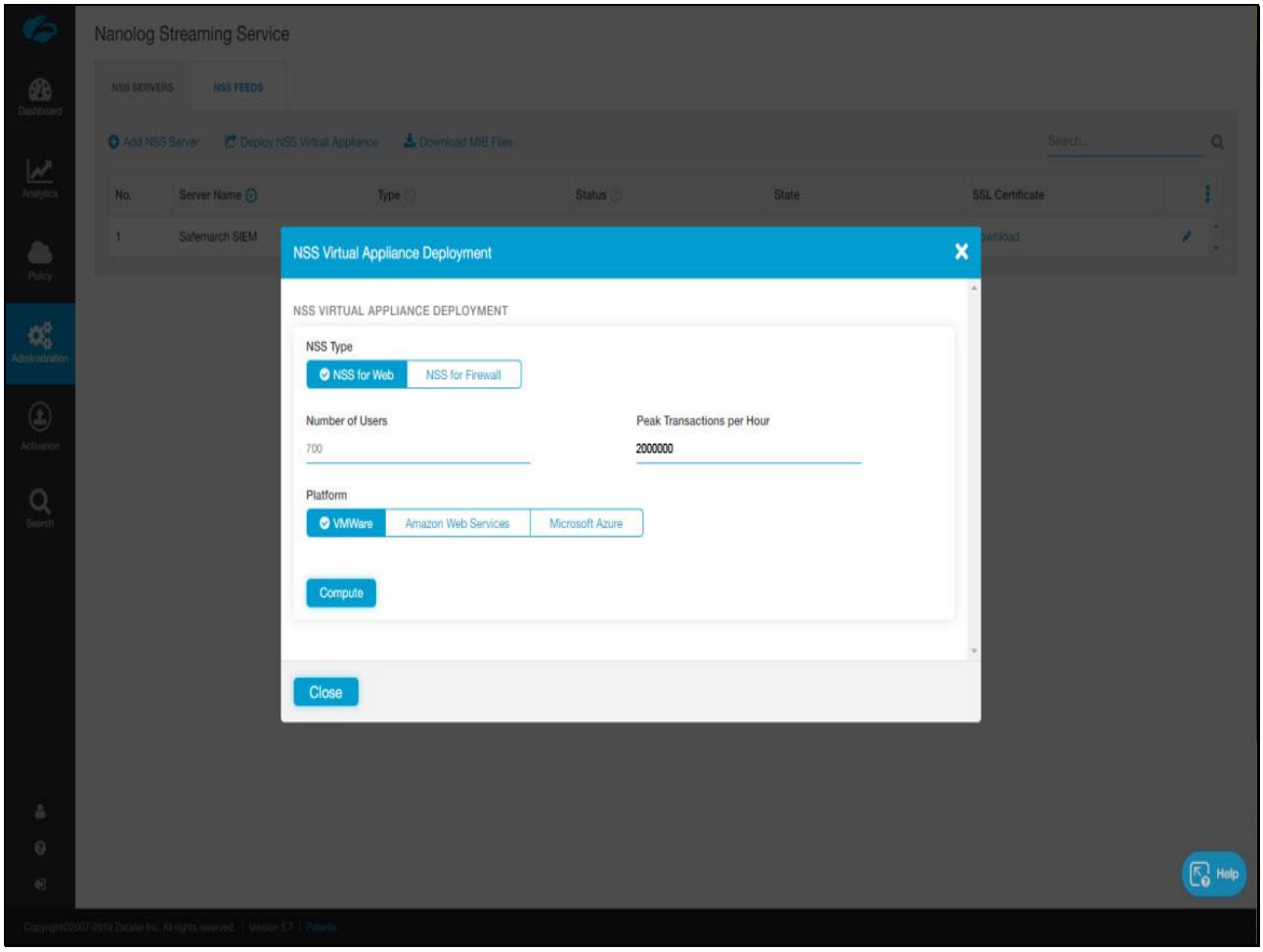
Slide notes

Let’s take a look at the process of deploying an NSS instance in AWS. Click Deploy NSS Virtual Appliance.



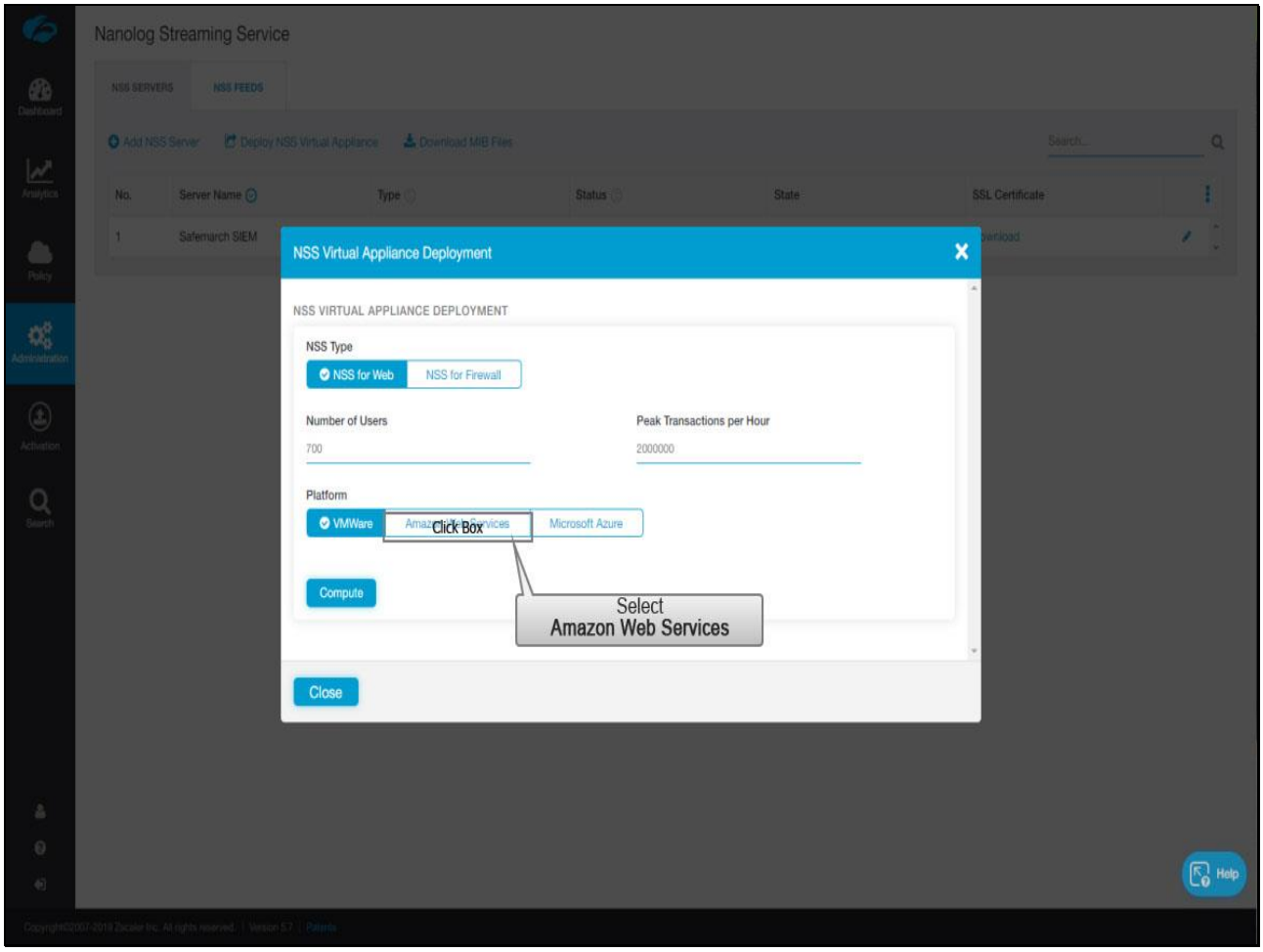
Slide notes

Enter 700 users



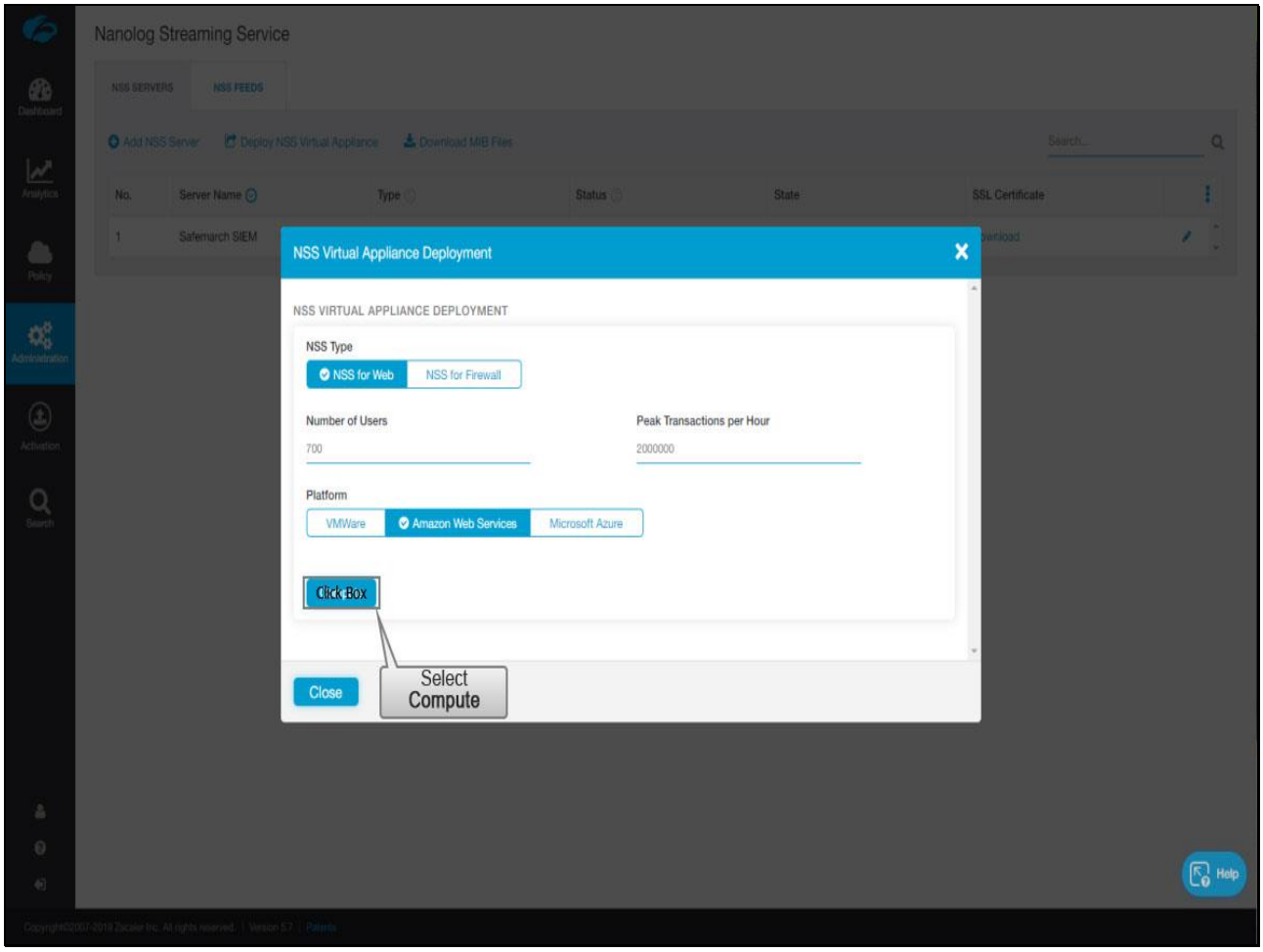
Slide notes

and 2,000,000 transactions.



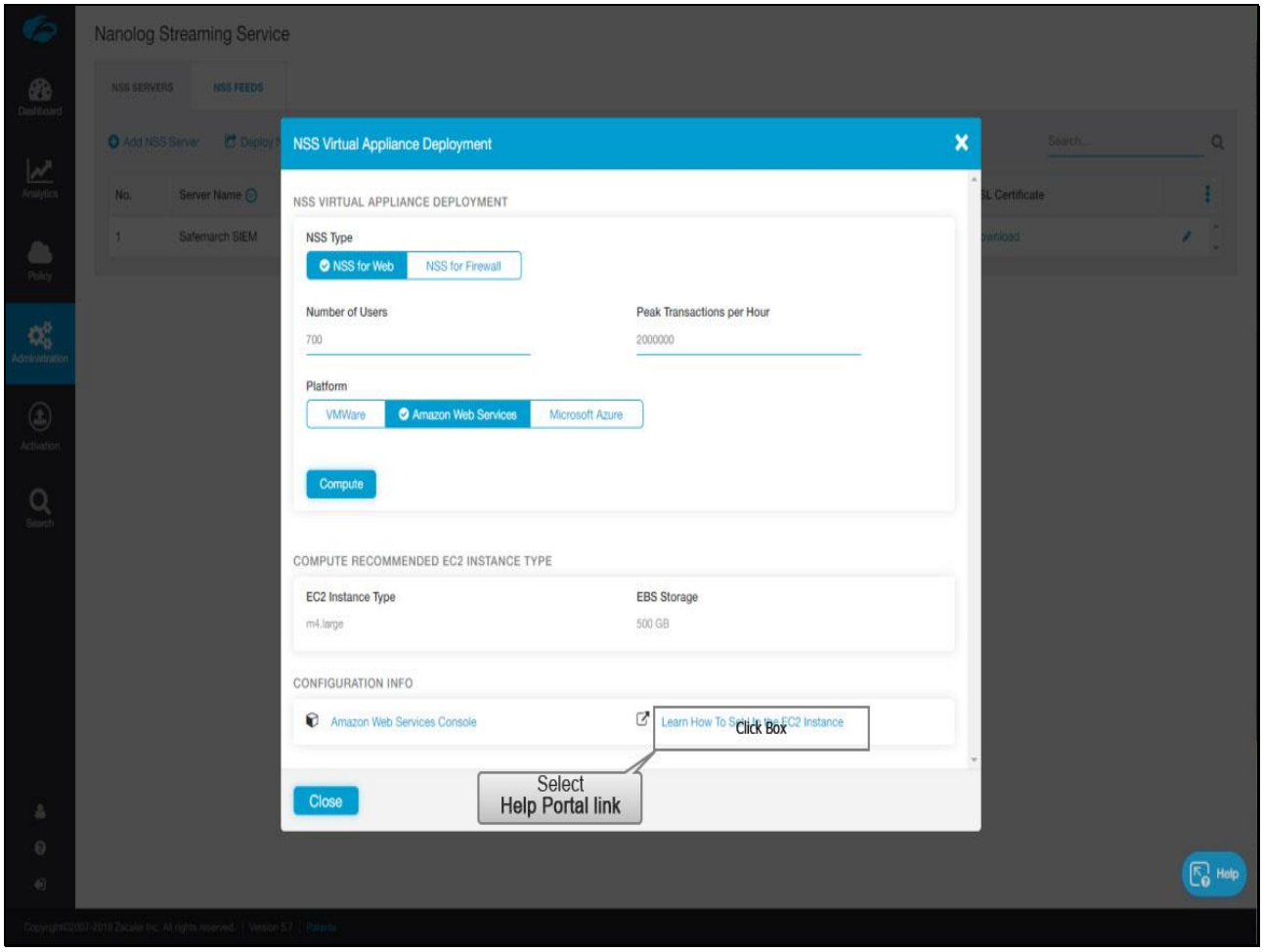
Slide notes

In the previous example you downloaded the .ova file to deploy the NSS instance on-premise. In this example, click on Amazon Web Services to deploy the NSS in AWS.



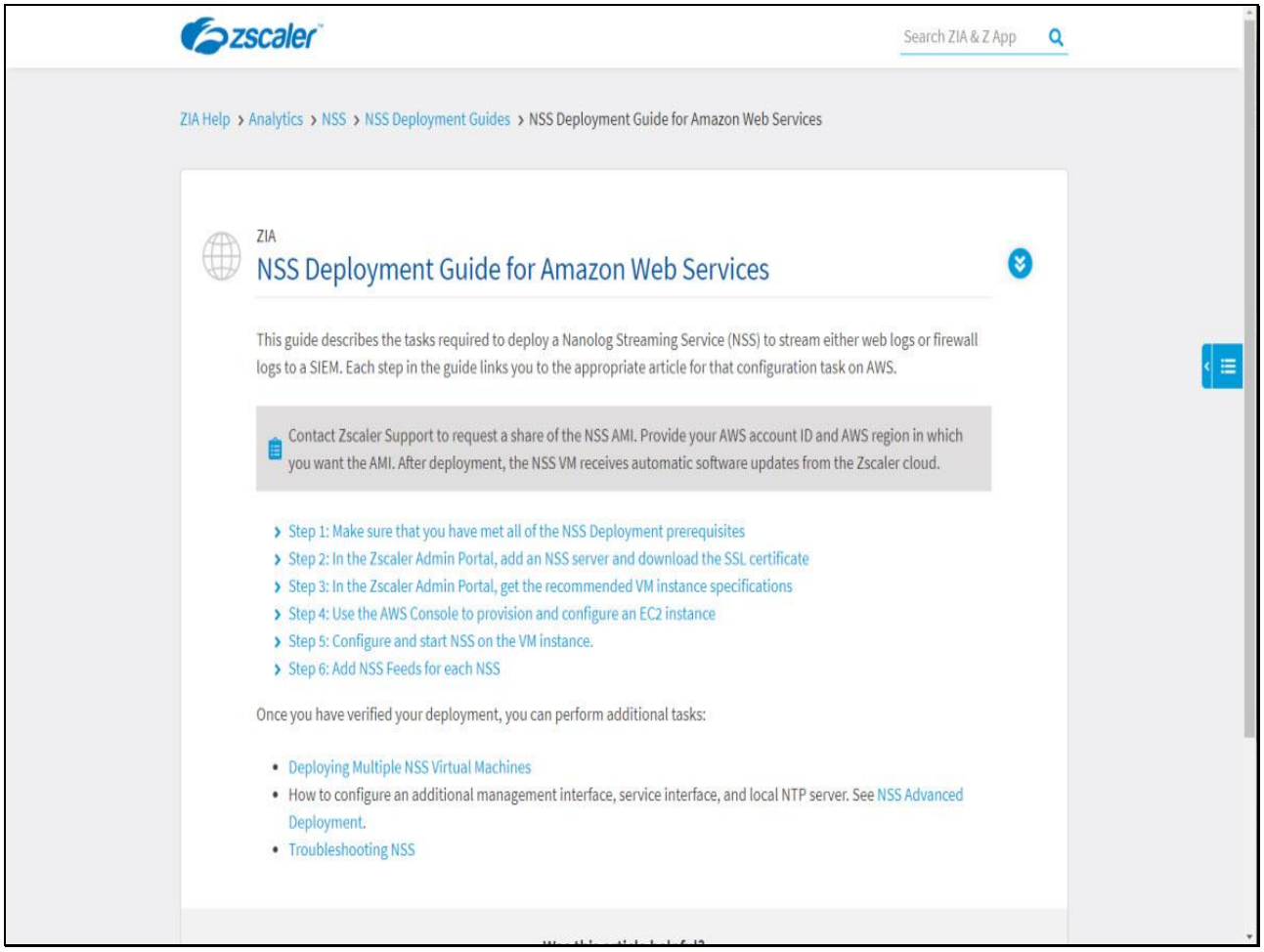
Slide notes

and click “Compute”.



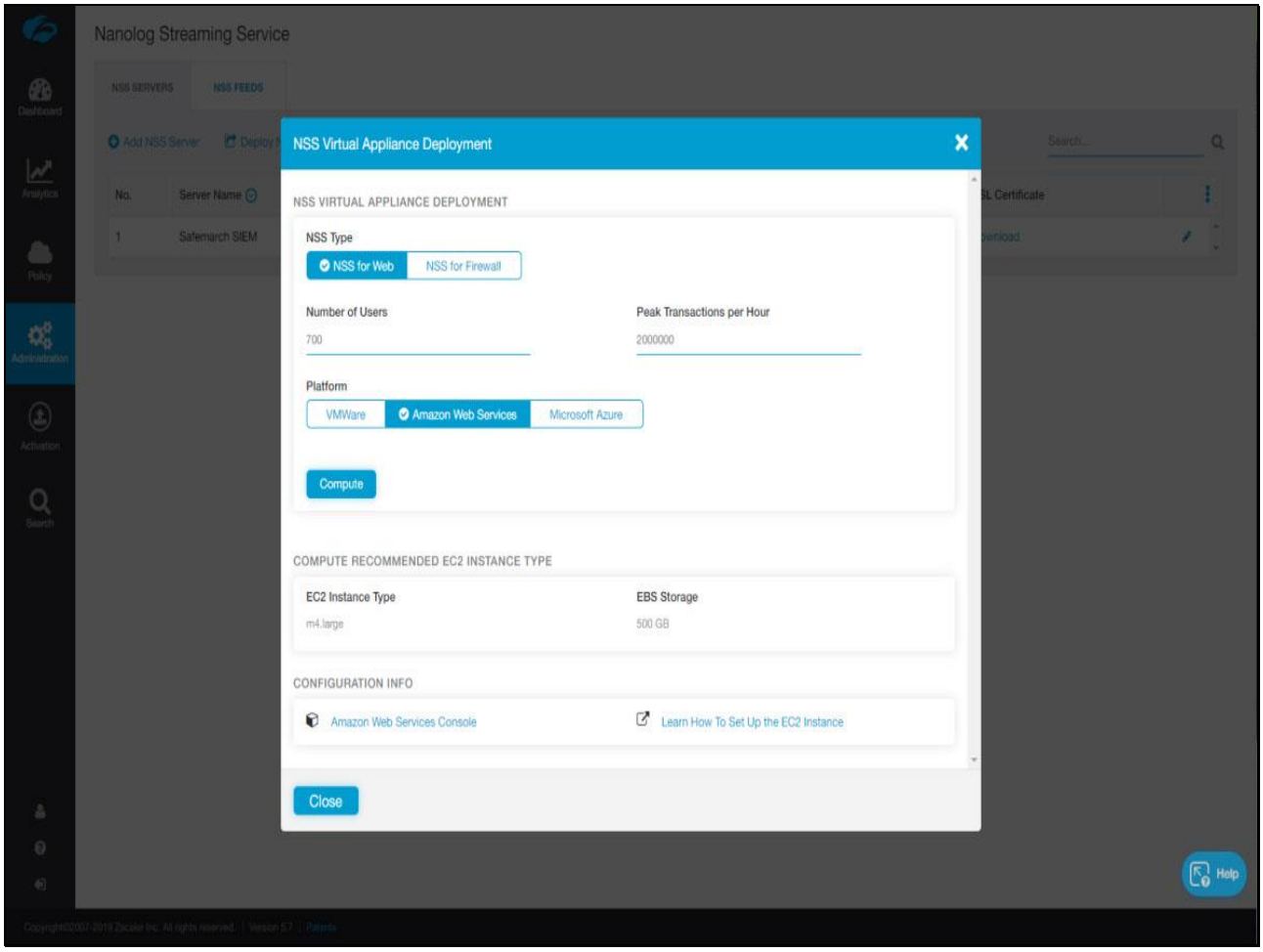
Slide notes

To see the details on how to deploy your NSS instance in AWS click the Help Portal article link. Be sure to record your recommendations for your EC2 instance before closing this page



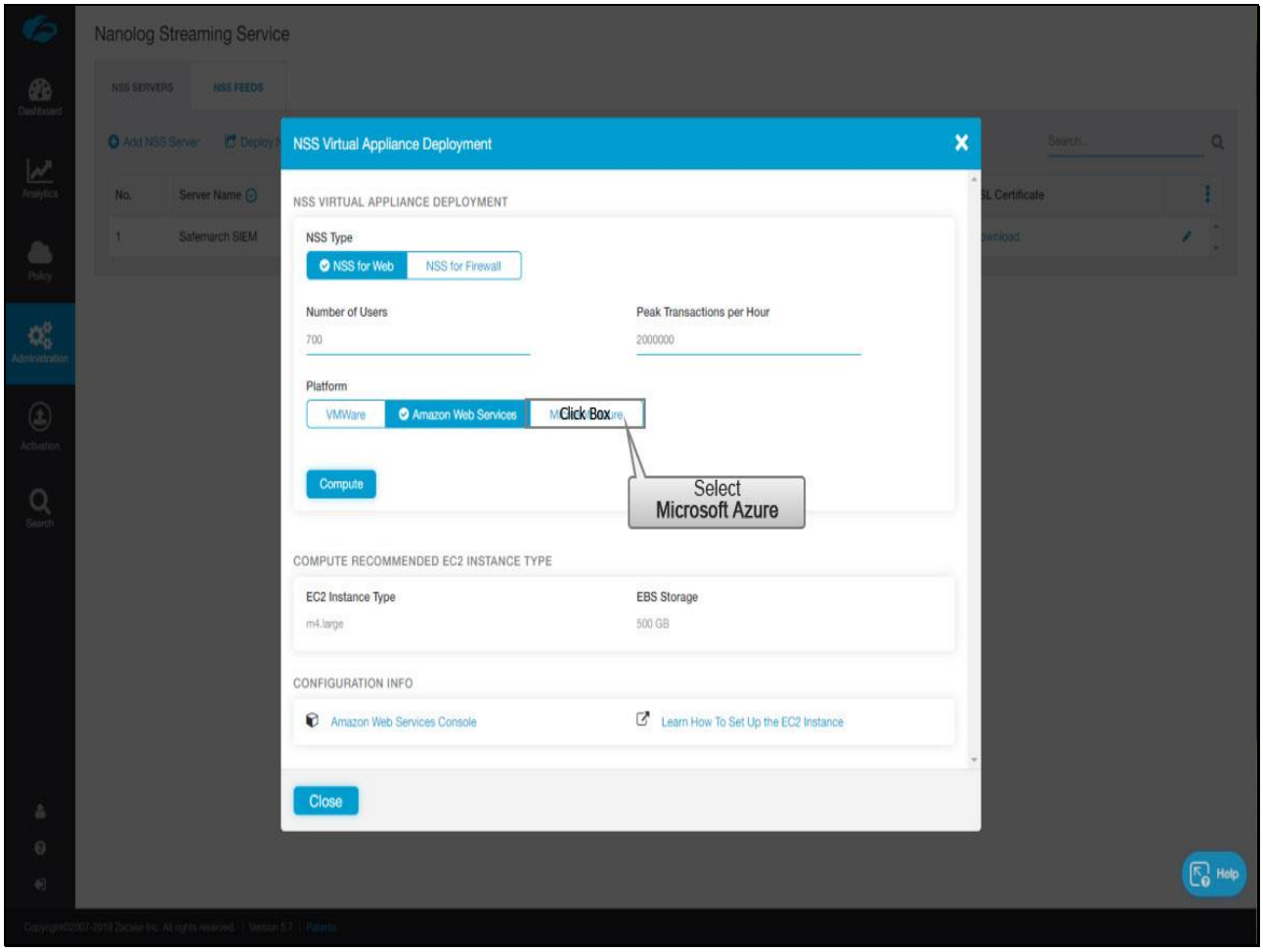
Slide notes

Full details for deploying NSS in AWS are available on this page. Expand the steps in the article to see all the steps involved.



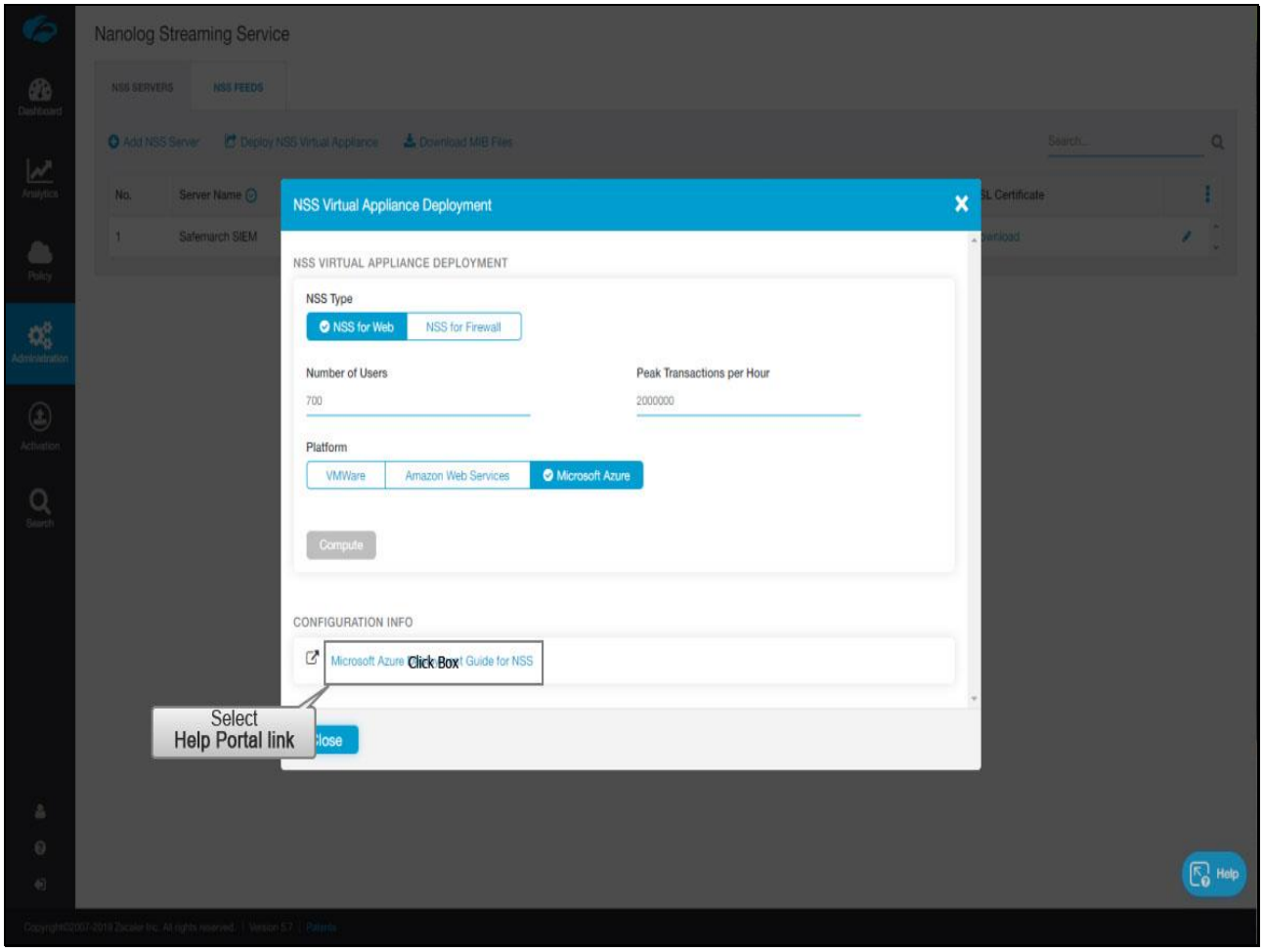
Slide notes

Similarly, to see the steps involved in deploying NSS in Microsoft Azure, click Microsoft Azure.



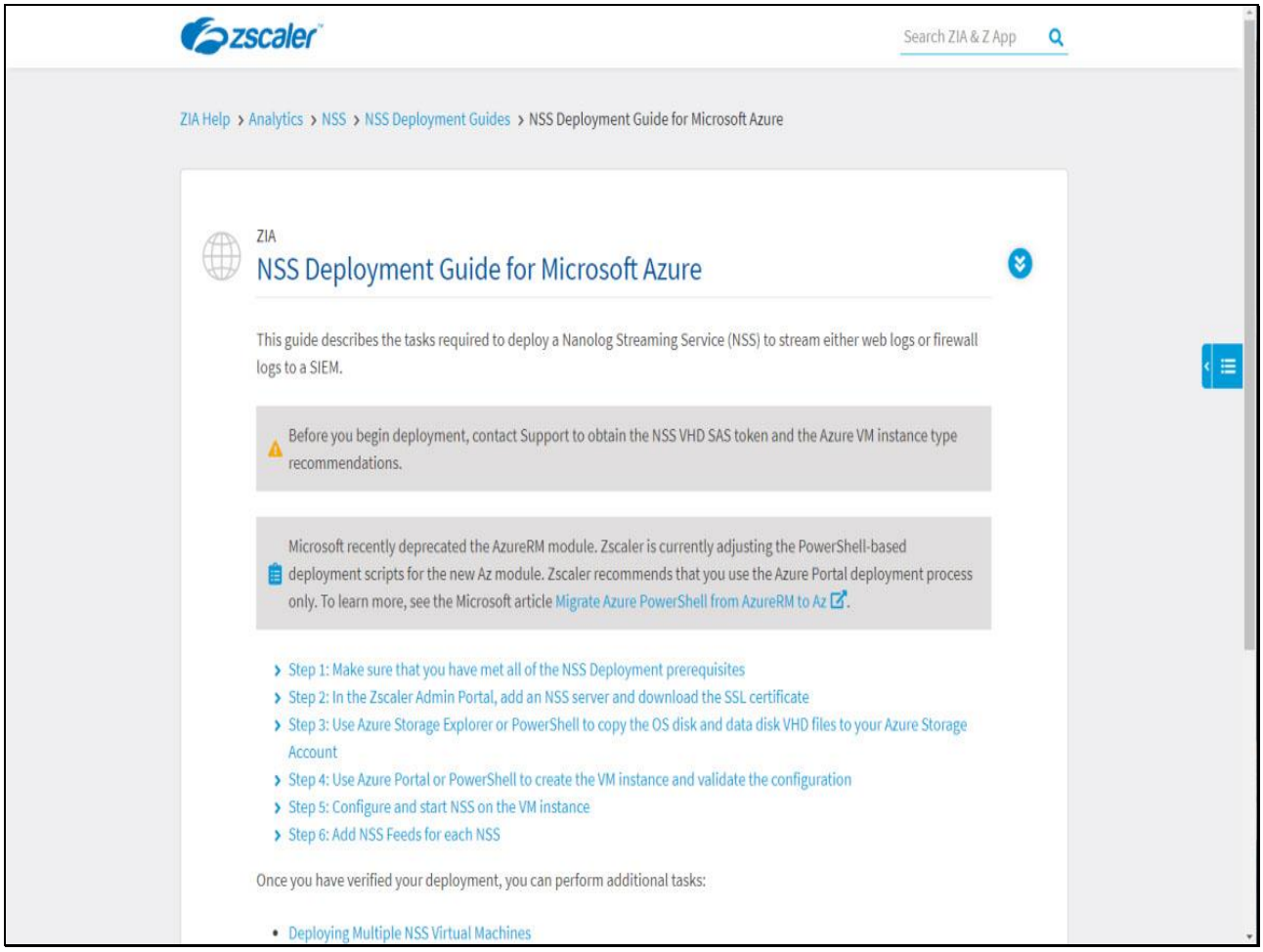
Slide notes

Similarly, to see the steps involved in deploying NSS in Microsoft Azure, click Microsoft Azure.

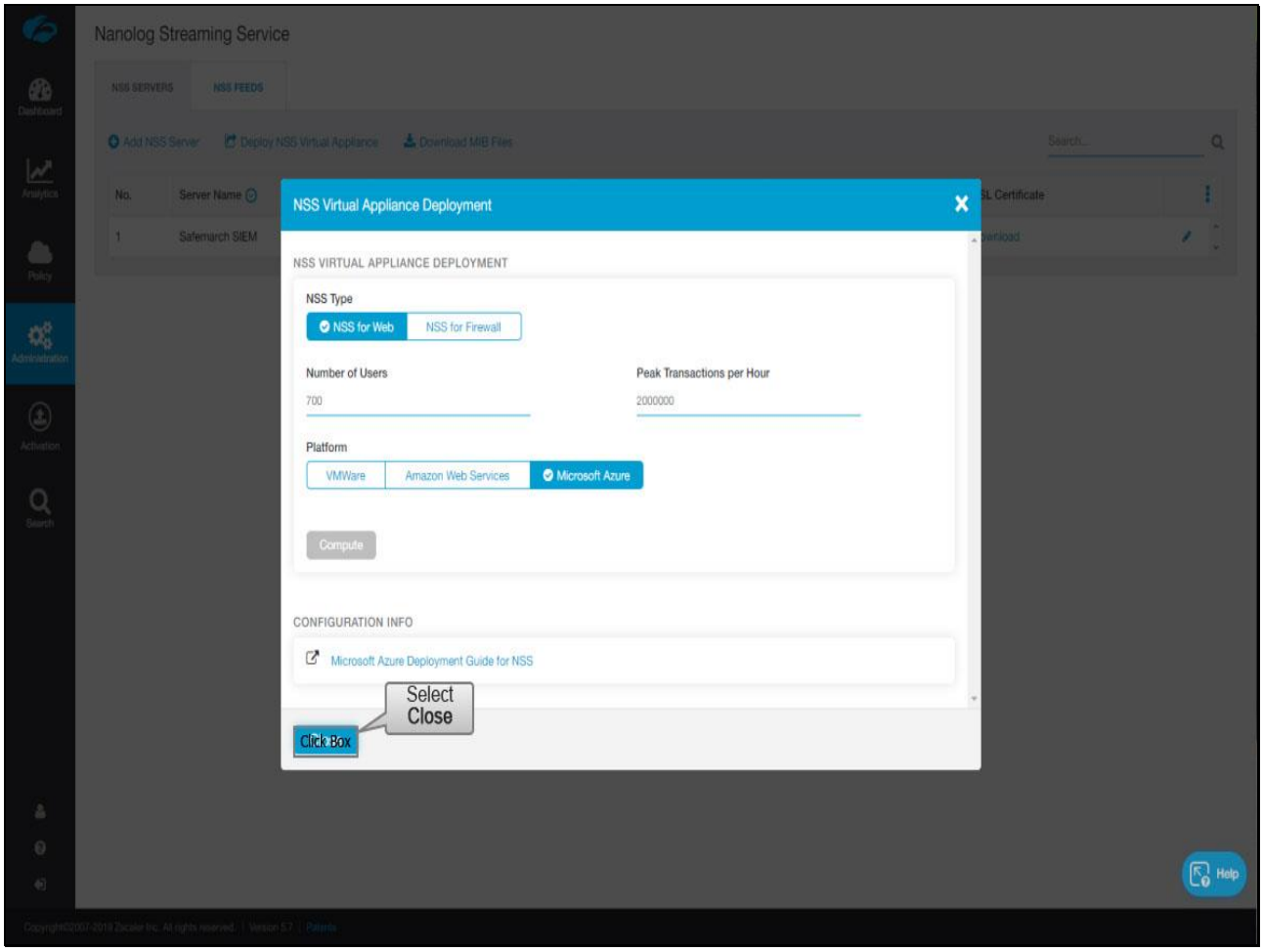


Slide notes

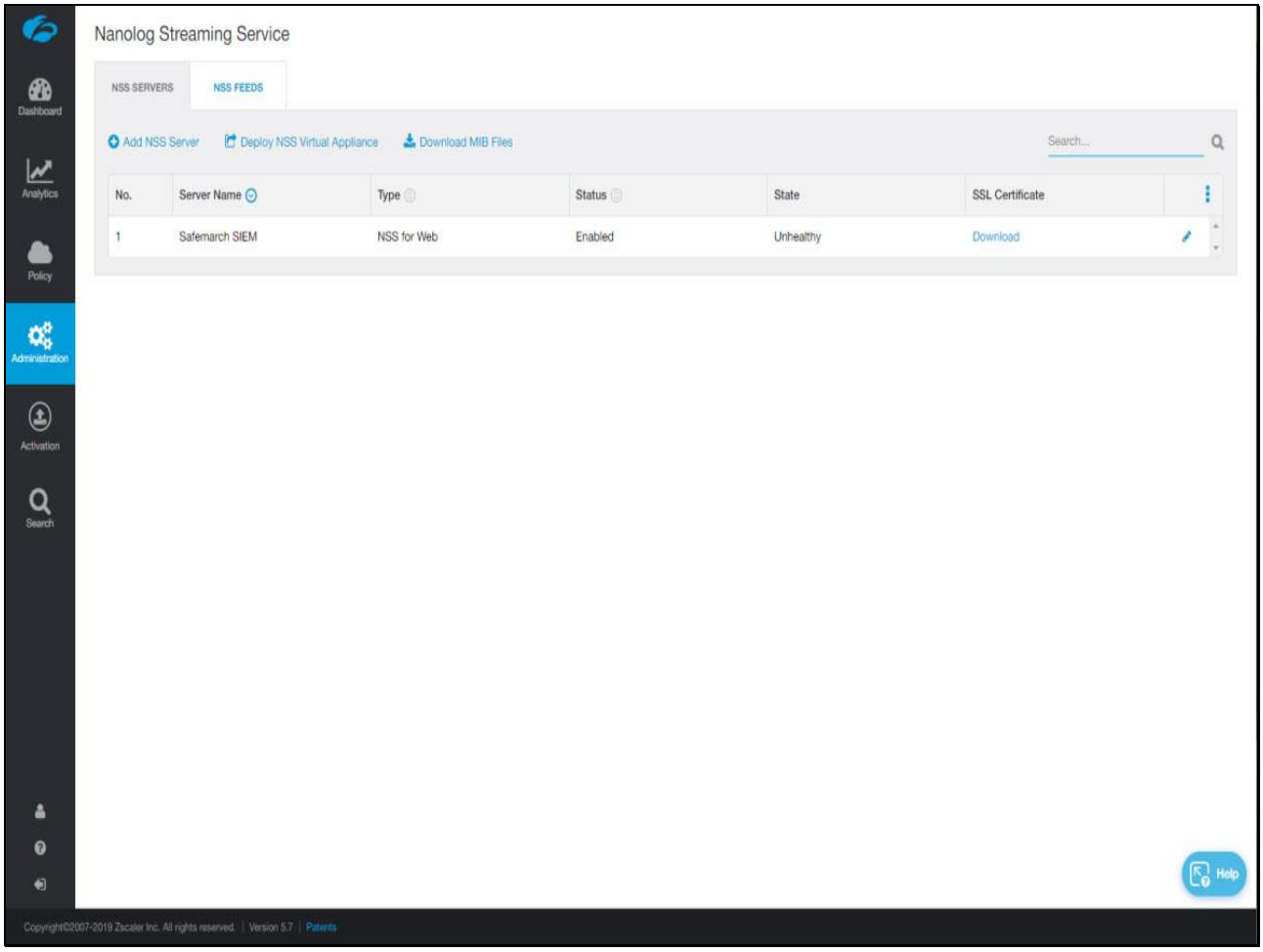
Then click the Help Portal link.


zscaler
Search ZIA & Z App
ZIA Help › Analytics › NSS › NSS Deployment Guides › NSS Deployment Guide for Microsoft Azure
ZIA
NSS Deployment Guide for Microsoft Azure
This guide describes the tasks required to deploy a Nanolog Streaming Service (NSS) to stream either web logs or firewall logs to a SIEM.
Before you begin deployment, contact Support to obtain the NSS VHD SAS token and the Azure VM instance type recommendations.
Microsoft recently deprecated the AzureRM module. Zscaler is currently adjusting the PowerShell-based deployment scripts for the new Az module. Zscaler recommends that you use the Azure Portal deployment process only. To learn more, see the Microsoft article Migrate Azure PowerShell from AzureRM to Az.
Step 1: Make sure that you have met all of the NSS Deployment prerequisites
Step 2: In the Zscaler Admin Portal, add an NSS server and download the SSL certificate
Step 3: Use Azure Storage Explorer or PowerShell to copy the OS disk and data disk VHD files to your Azure Storage Account
Step 4: Use Azure Portal or PowerShell to create the VM instance and validate the configuration
Step 5: Configure and start NSS on the VM instance
Step 6: Add NSS Feeds for each NSS
Once you have verified your deployment, you can perform additional tasks:
Deploying Multiple NSS Virtual Machines

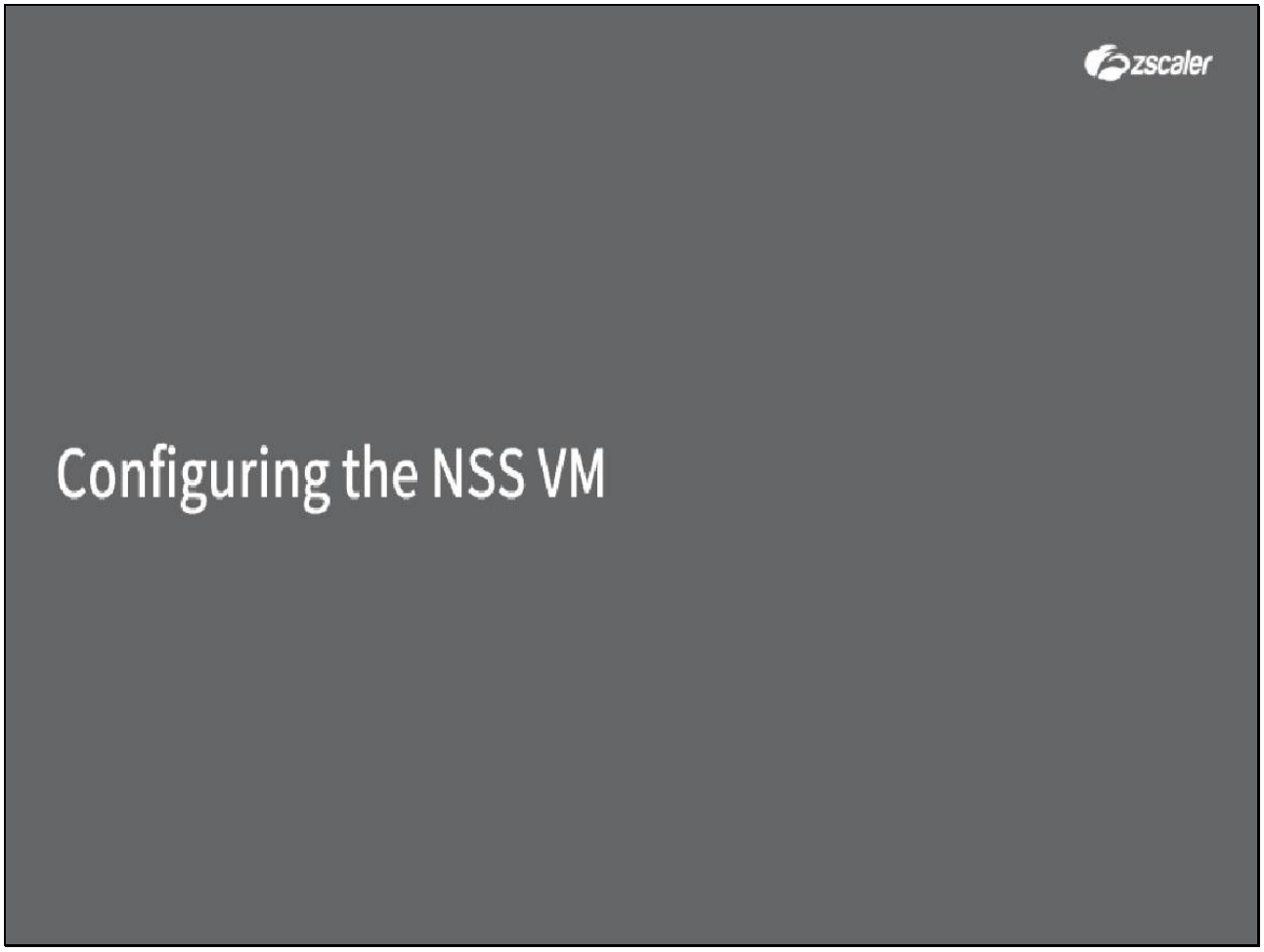
Slide notes


Nanolog Streaming Service
NSS SERVERS
NSS FEEDS
Add NSS Server
Deploy NSS Virtual Appliance
Download MIB Files
Search...
No.
Server Name
SL Certificate
1
Safemarch SIEM
NSS Virtual Appliance Deployment
NSS VIRTUAL APPLIANCE DEPLOYMENT
NSS Type
NSS for Web
NSS for Firewall
Number of Users
700
Peak Transactions per Hour
2000000
Platform
VMWare
Amazon Web Services
Microsoft Azure
Compute
CONFIGURATION INFO
Microsoft Azure Deployment Guide for NSS
Select Close
Click Box
Help

Slide notes

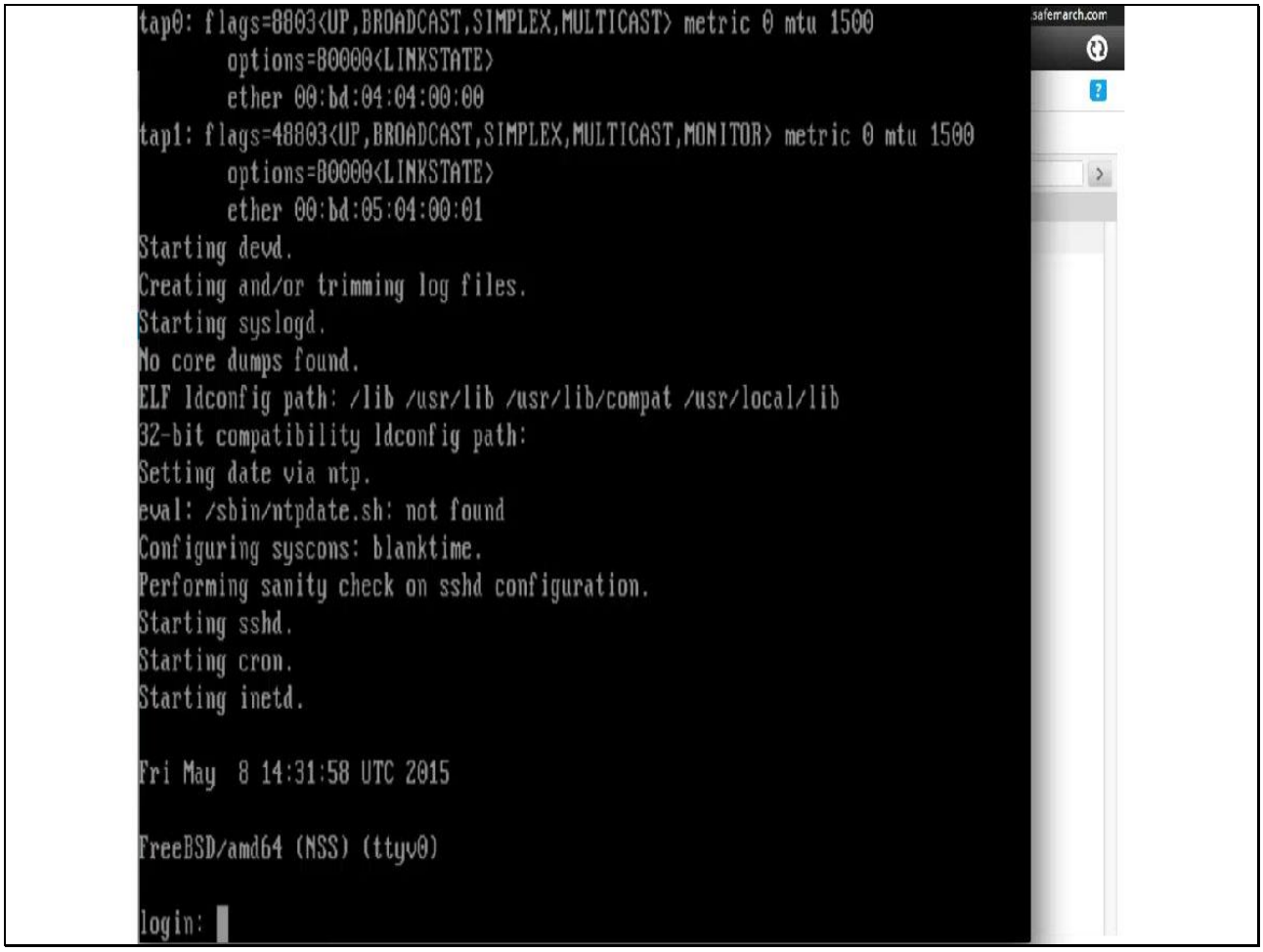

Nanolog Streaming Service
NSS SERVERS
NSS FEEDS
Add NSS Server
Deploy NSS Virtual Appliance
Download MIB Files
Search...
No.
Server Name
Type
Status
State
SSL Certificate
1
Safemarch SIEM
NSS for Web
Enabled
Unhealthy
Download
Dashboard
Analytics
Policy
Administration
Activation
Search
Help
Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents

Slide notes



Slide notes

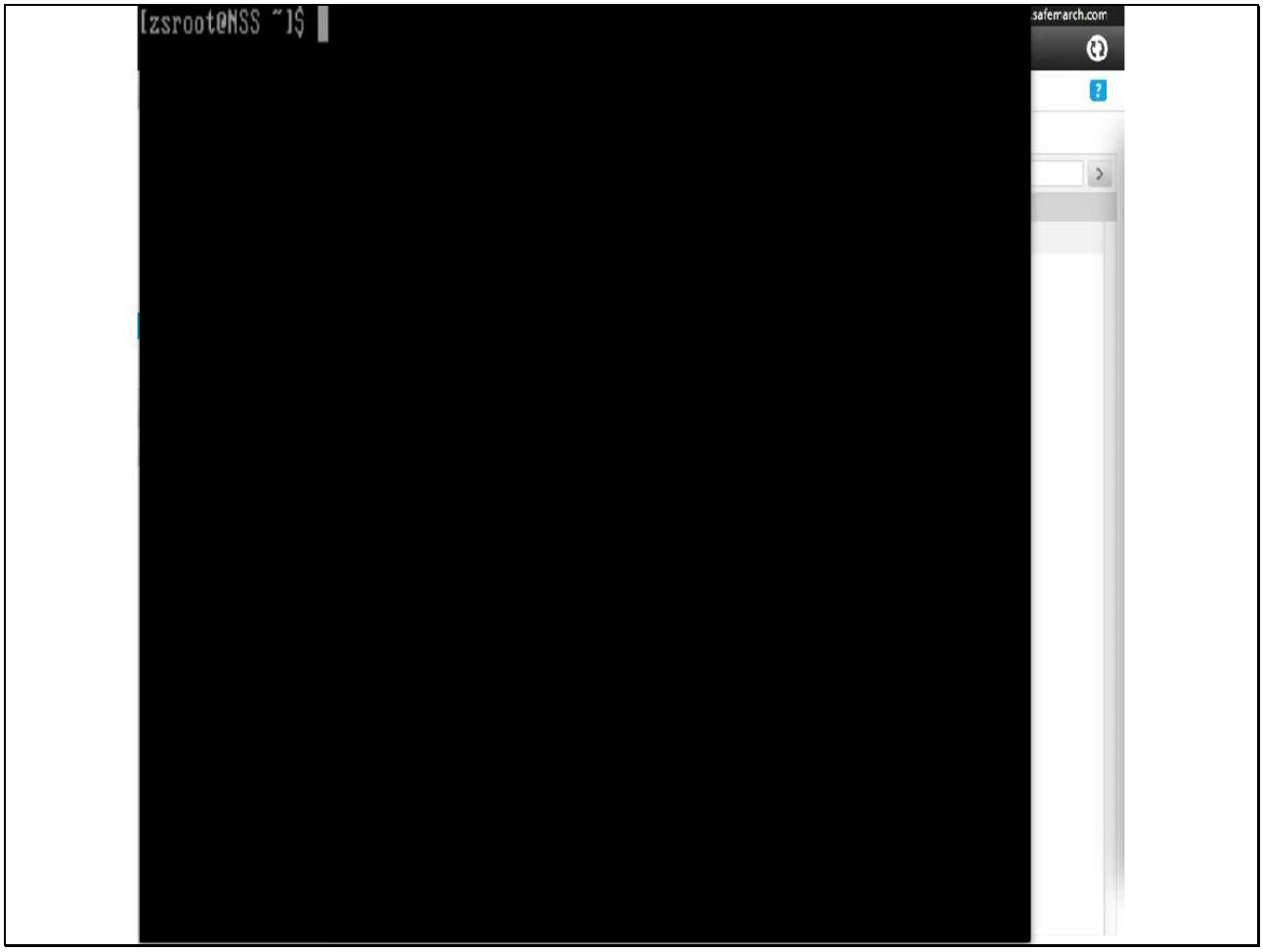
We will now turn our attention away from the Admin UI and look at the configuration process for the NSS instance via the NSS console.



Slide notes

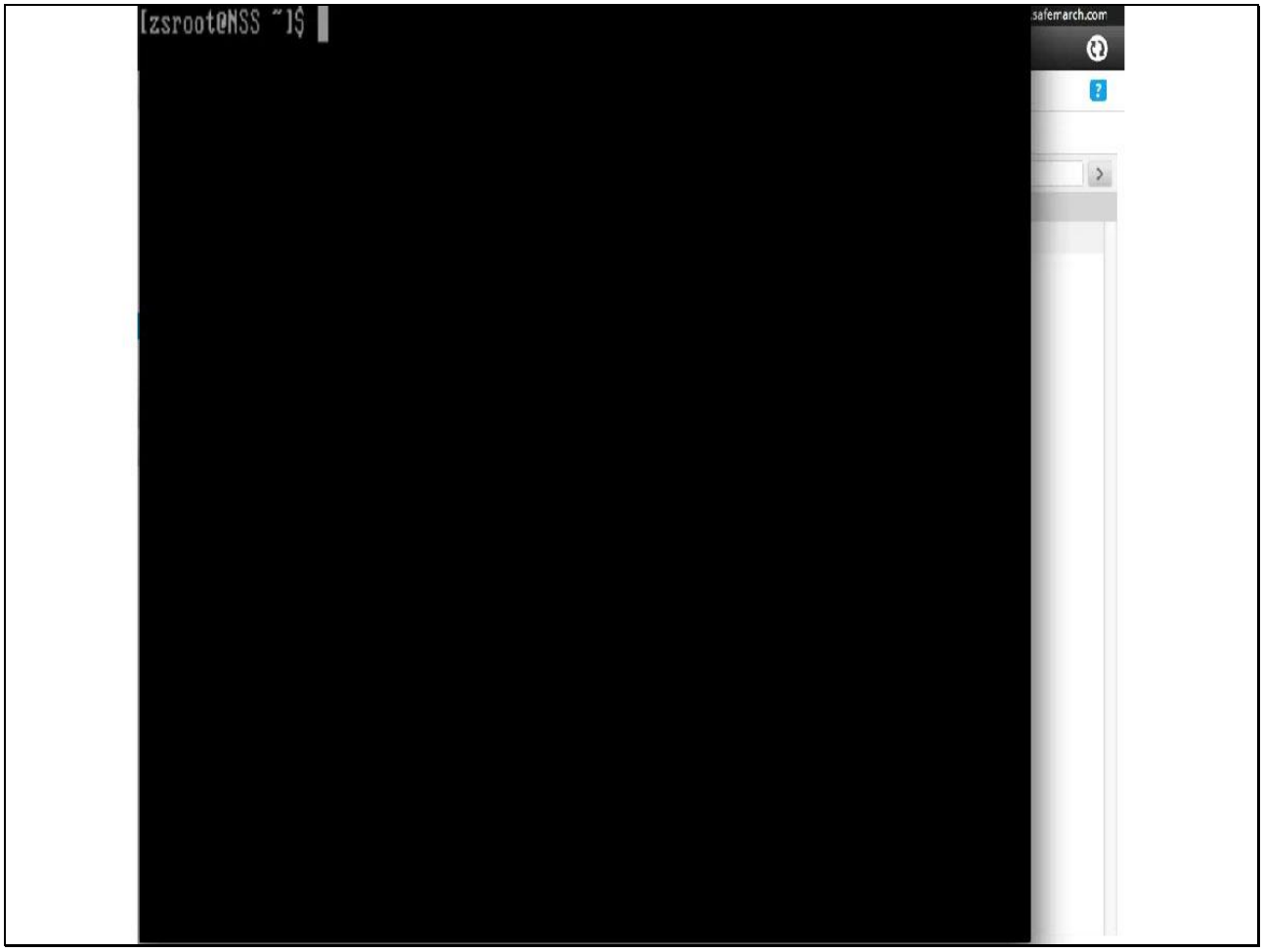
Once the VM is running, connect to the console. Log in as user zsroot and password zsroot. Your first task is to run the passwd command to change the default password. Now we will configure the network interfaces. Run the command, sudo nss configure. Enter the DNS server IP, management interface IP and gateway, and service IP address IP and gateway.

Note that the management and service IPs can be on different subnets as long as the DNS server is reachable from both interfaces. Now we need to upload the client certificate. You can use FTP, SCP, or SFTP to upload the certificate file.



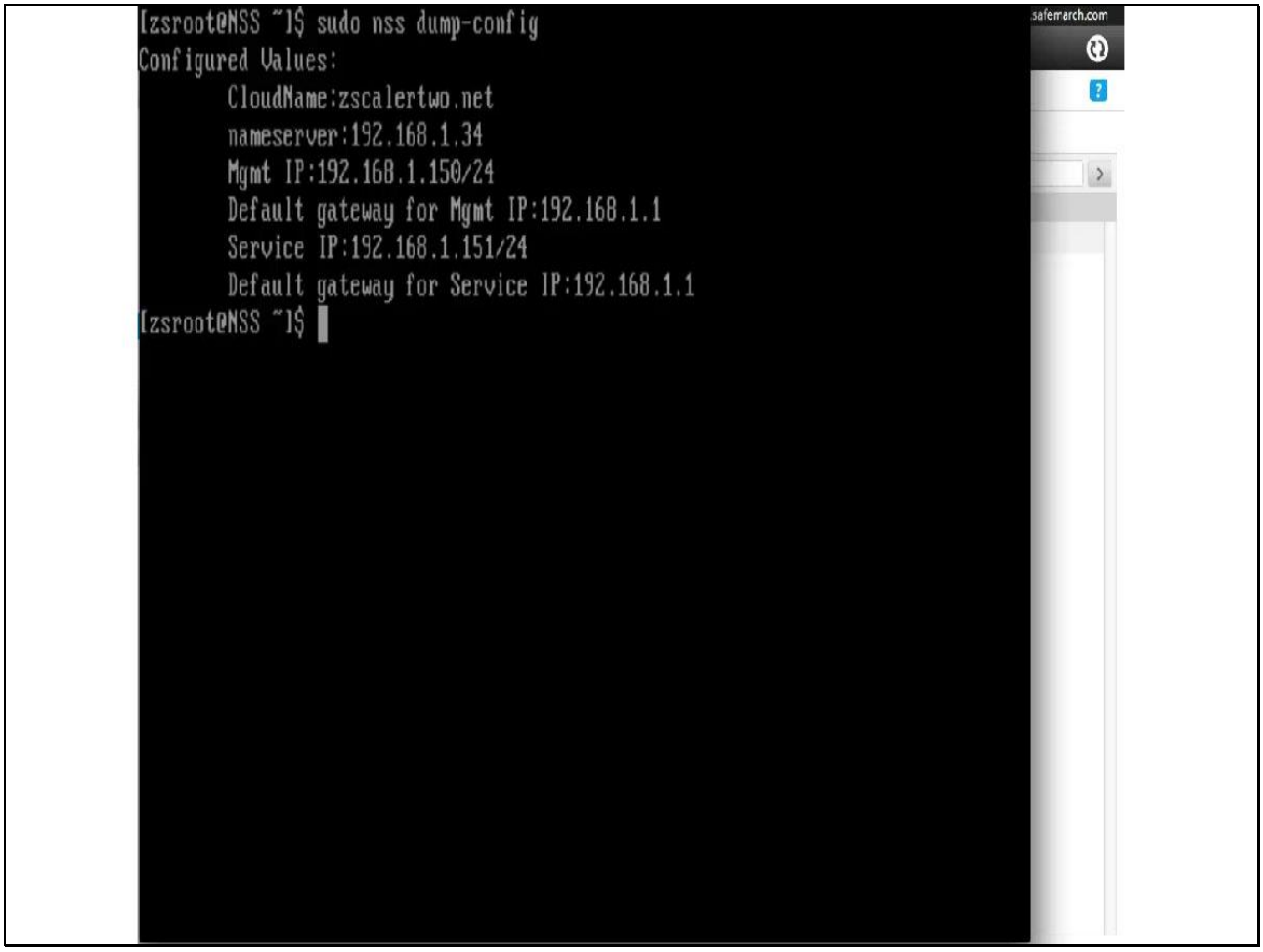
Slide notes

We'll use SCP in this demonstration. To install the certificate run the command sudo nss install-cert.



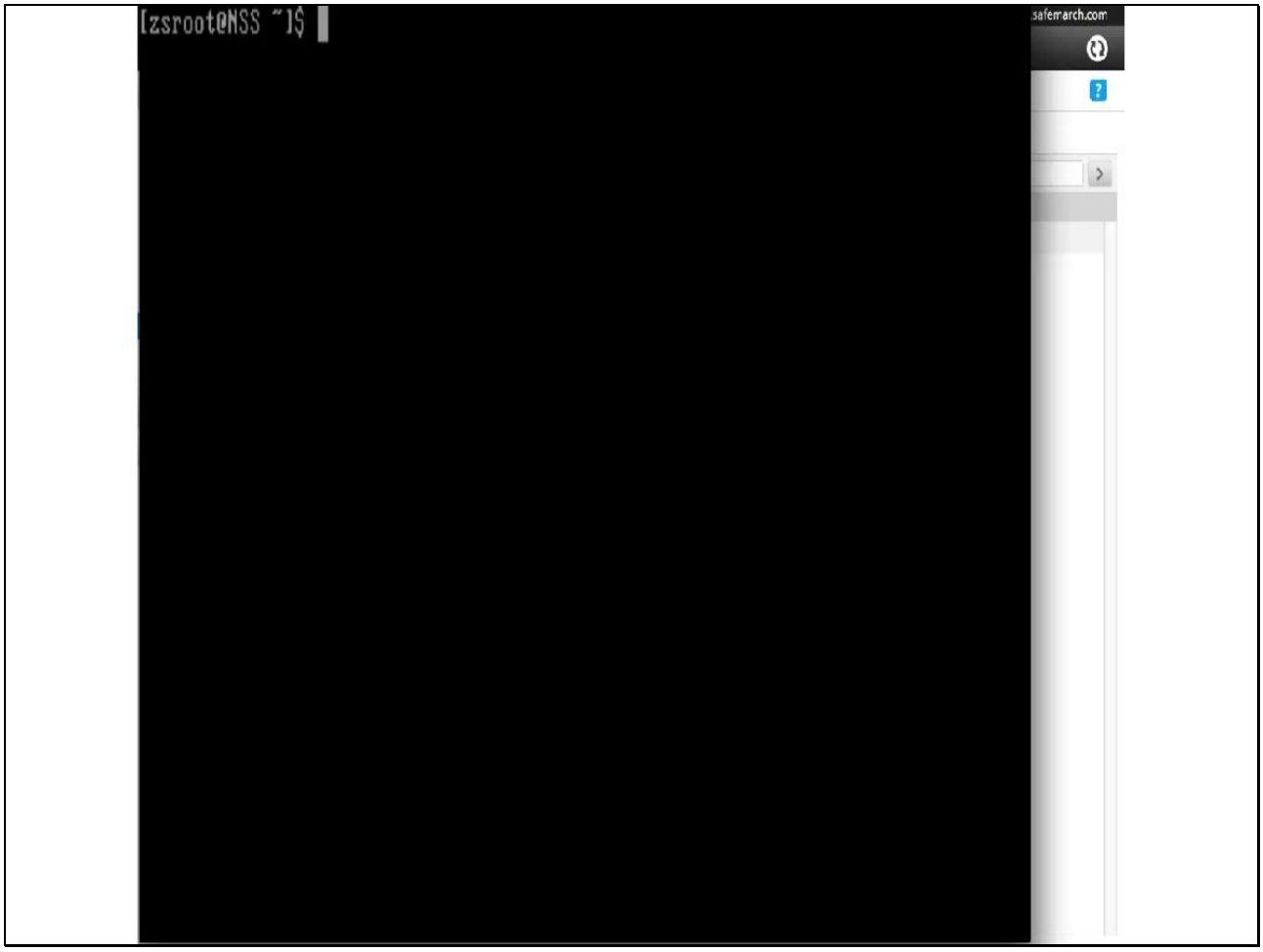
Slide notes

You can verify the cert was loaded by running the command sudo nss dump config.



Slide notes

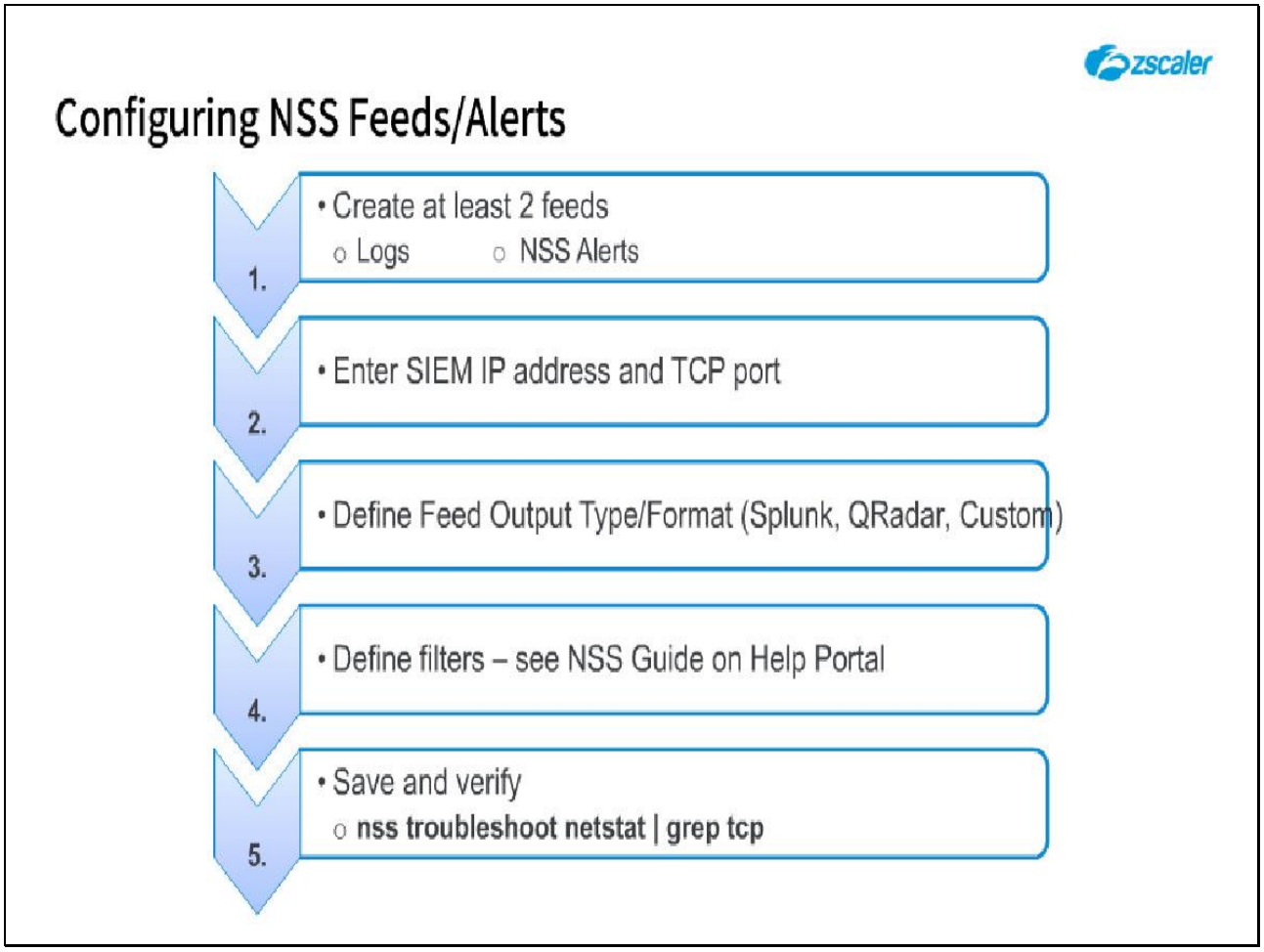
Next we will download the latest NSS binaries. Once NSS is running the system will automatically update whenever new versions are available. Run the command sudo nss update-now. Next, start NSS by running the command sudo nss start and make sure nss starts automatically by running the command sudo nss enable-autostart.



Slide notes

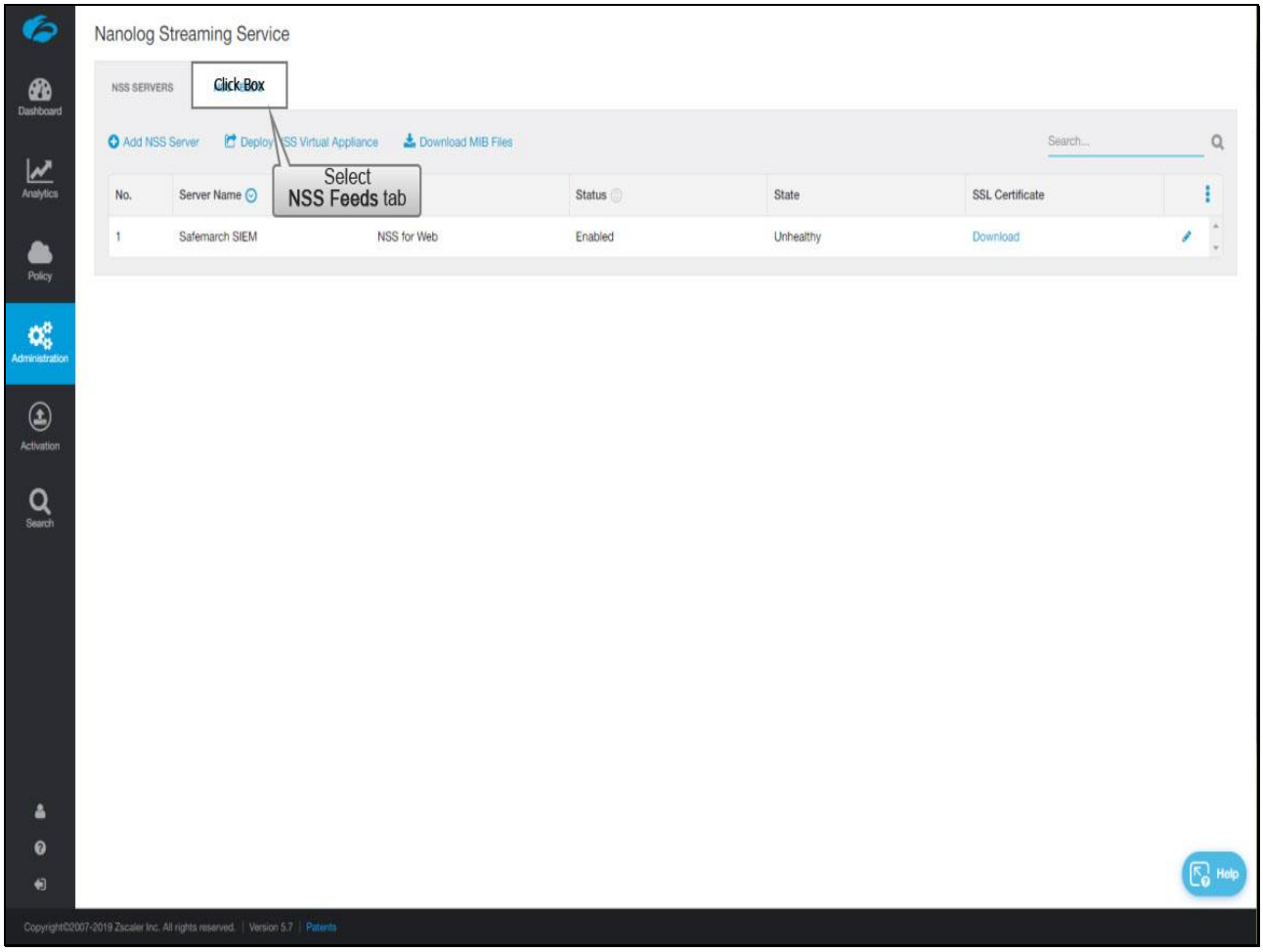
You can verify that nss is running by entering sudo nss troubleshoot netstat | grep tcp and look for a connection to Zscaler on port 9422

Slide notes



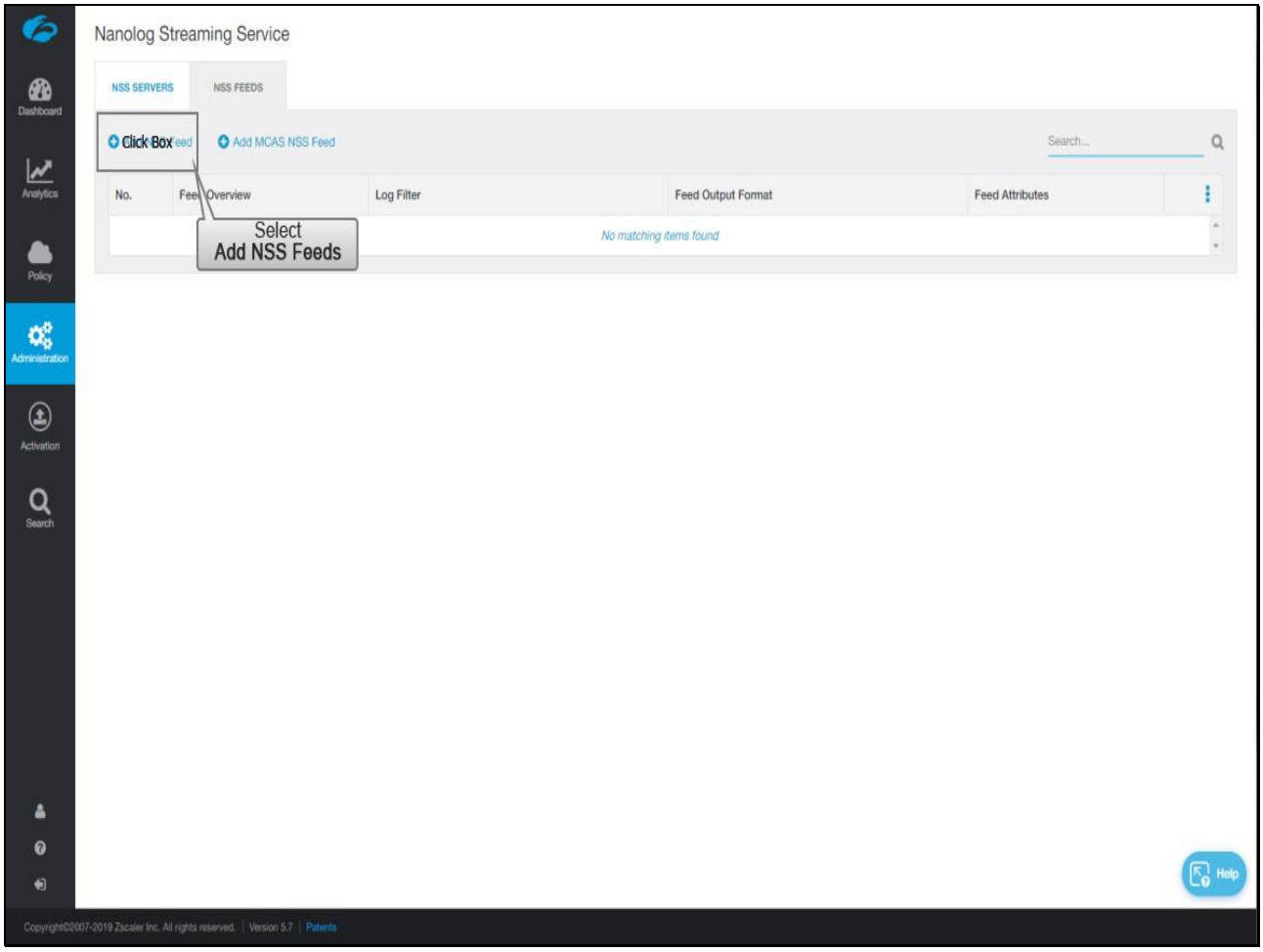
Slide notes

Now that the NSS virtual machine is running, we need to specify where and how to send the logs. Zscaler recommends creating 2 feeds. One for user logs and one for alerts about the status of NSS itself. After that we'll enter our SIEM address and TCP port, define the Feed Output Type, Define Filter, and then Save and Verify.



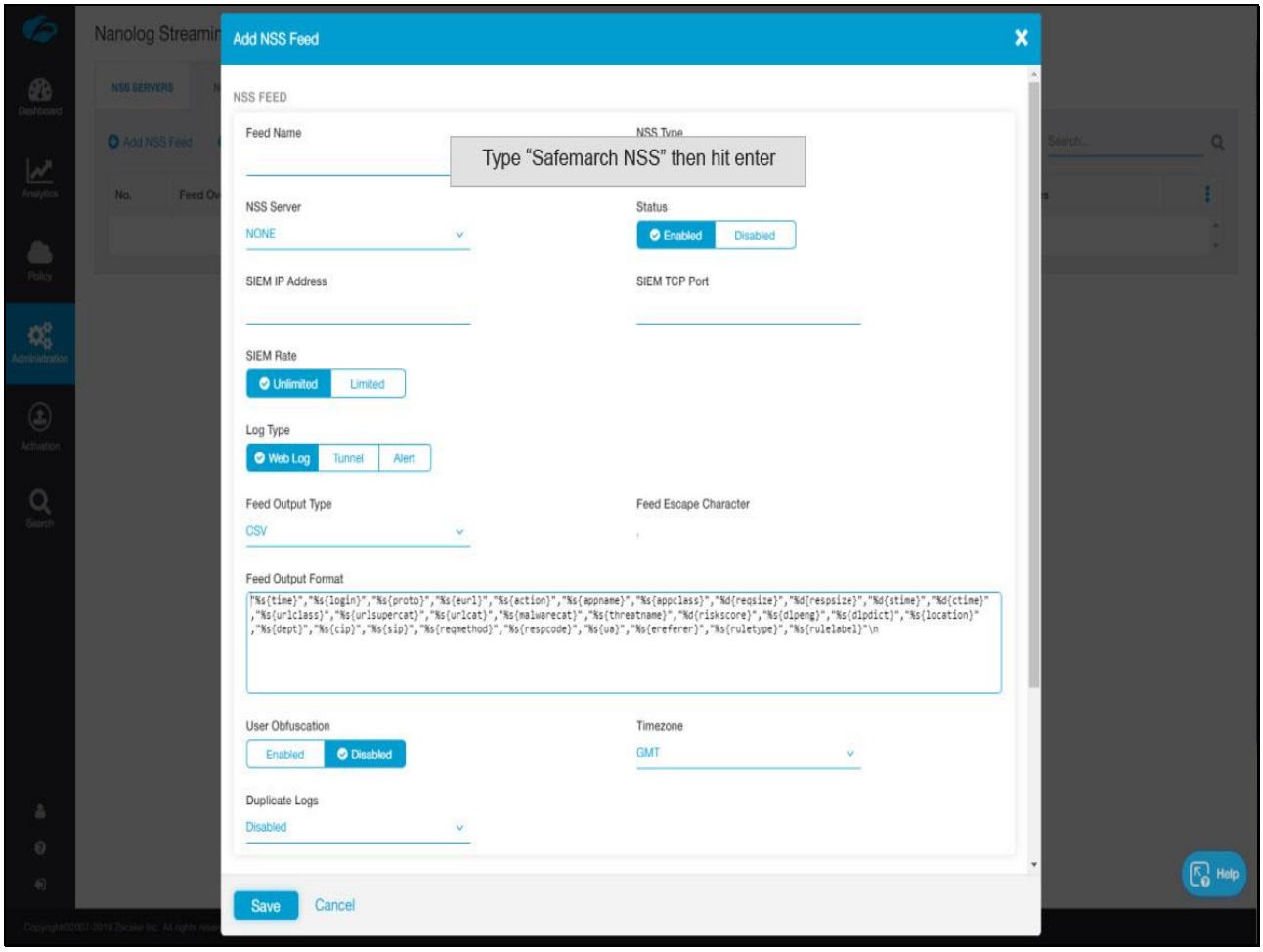
Slide notes

We'll start with the Alerts feed. Click the "NSS Feeds" tab.



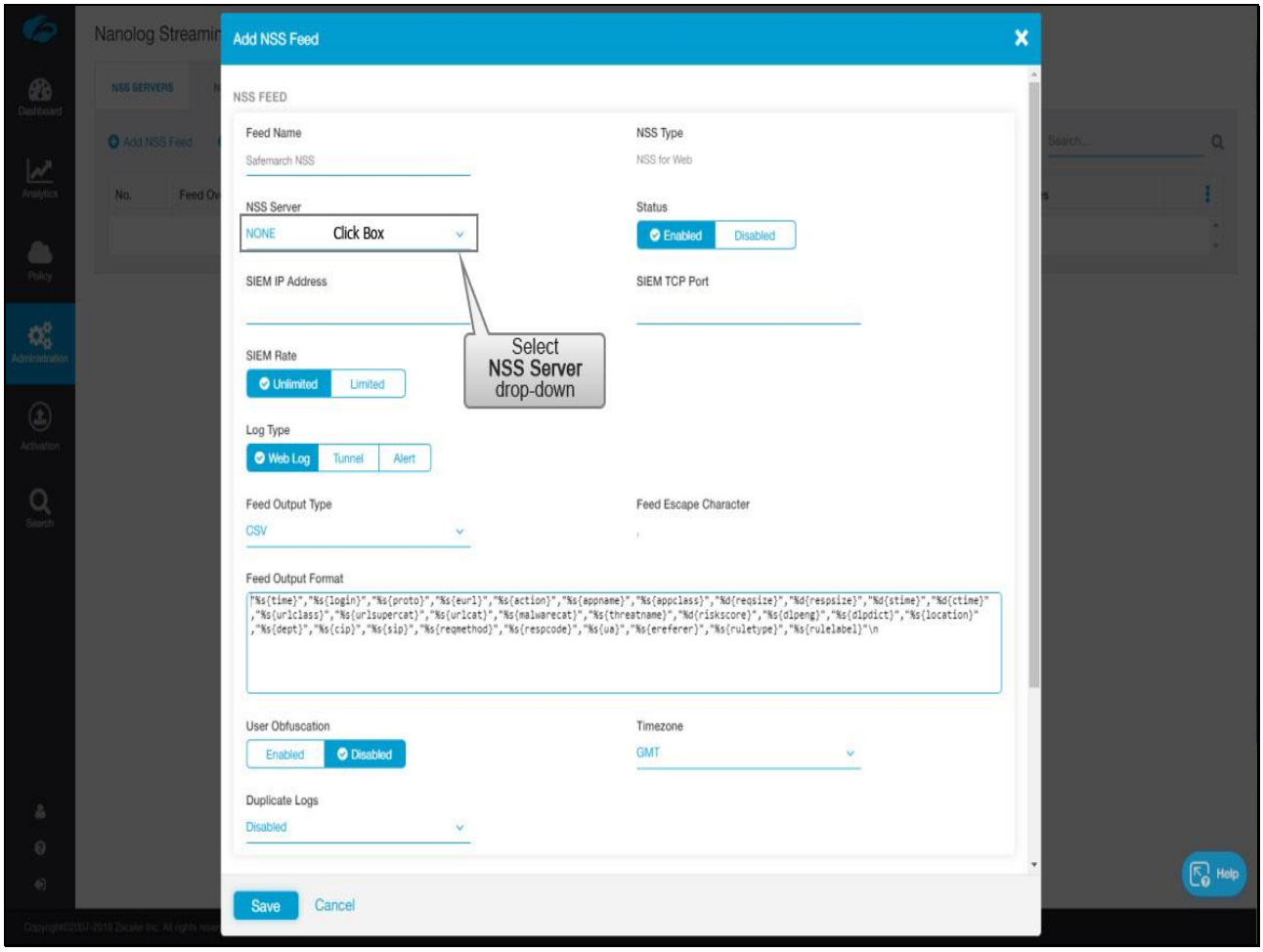
Slide notes

Click “Add NSS Feeds”.



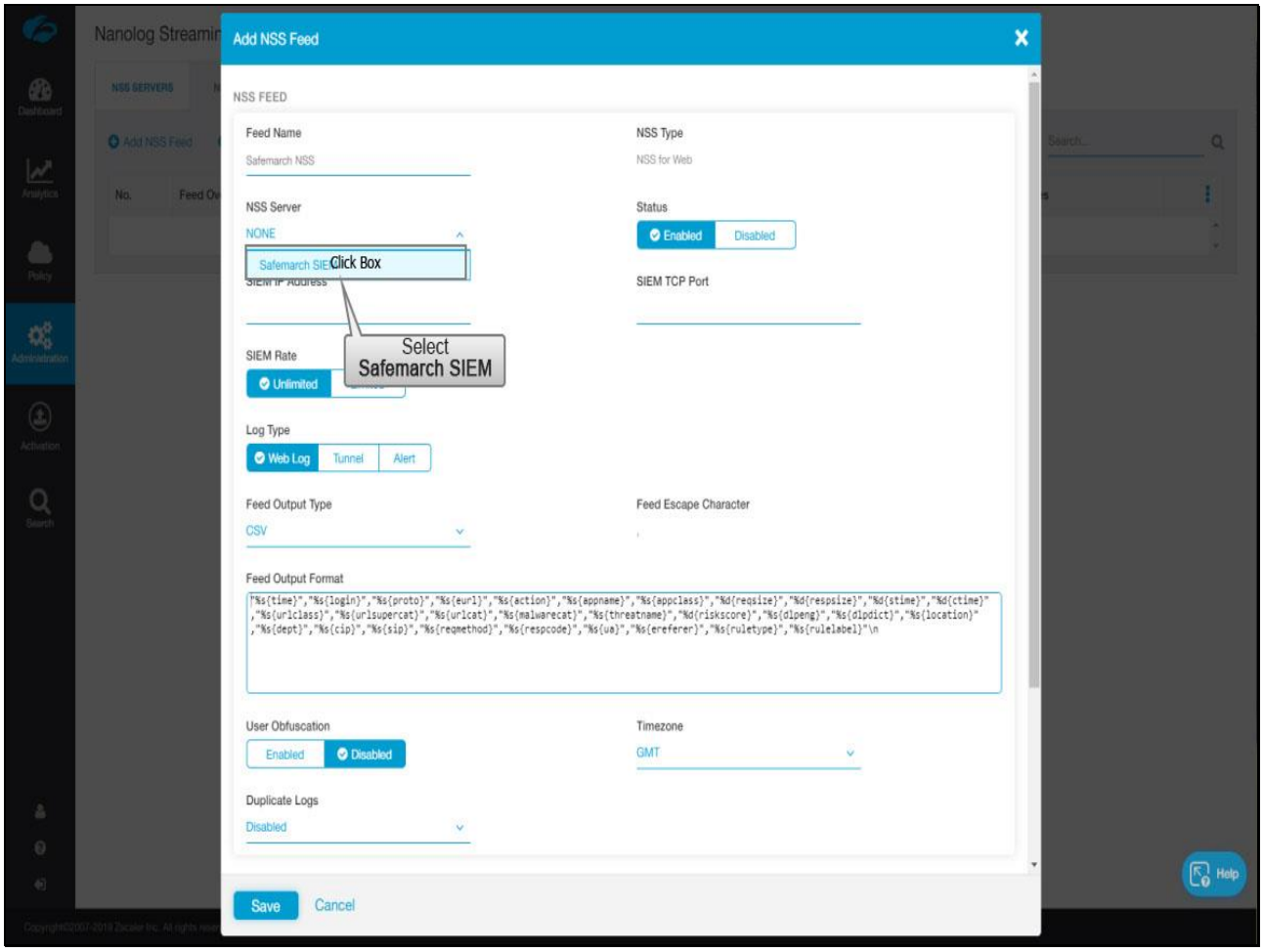
Slide notes

Enter a name for the Feed.

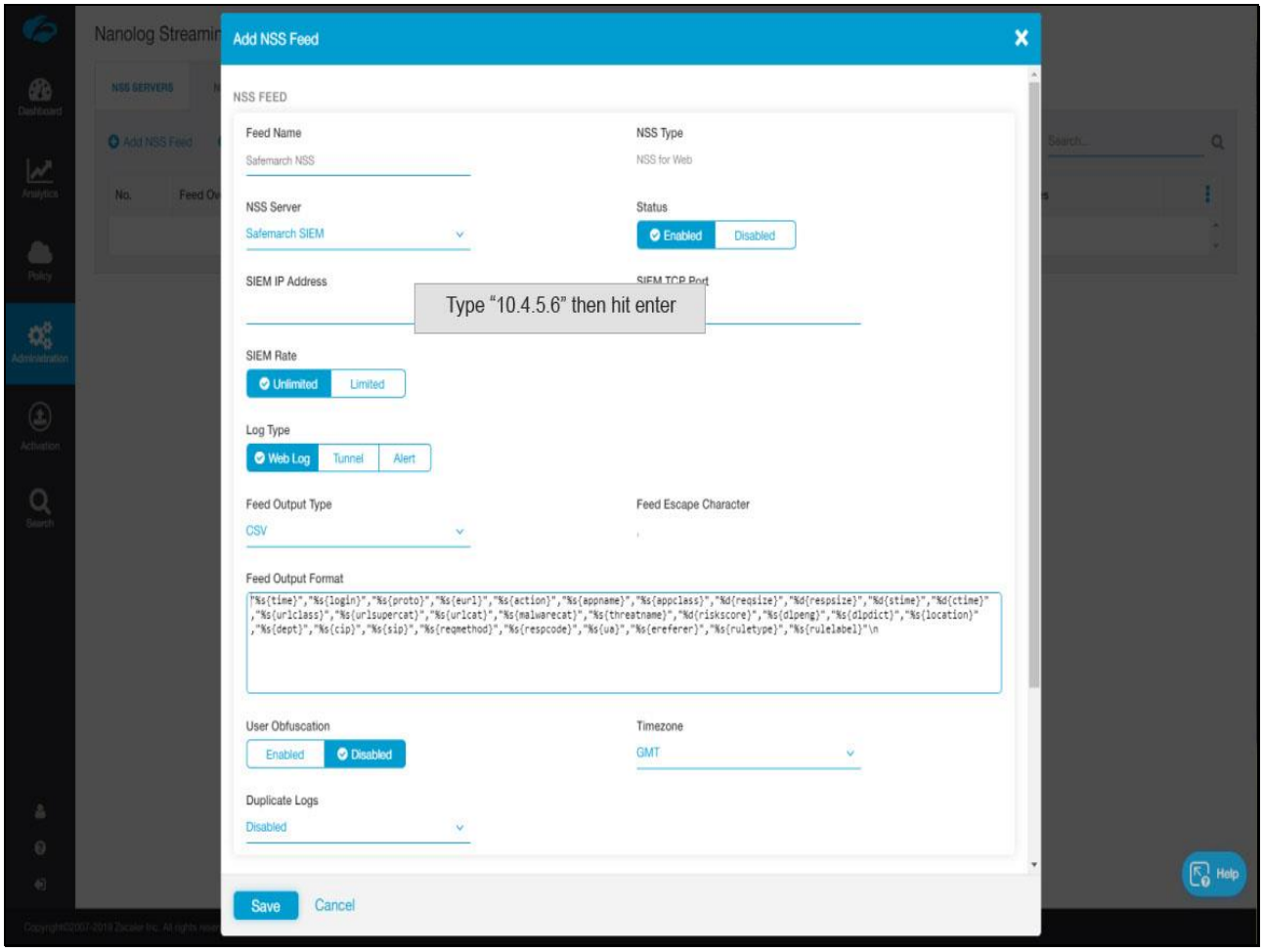


Slide notes

Then select the NSS server.

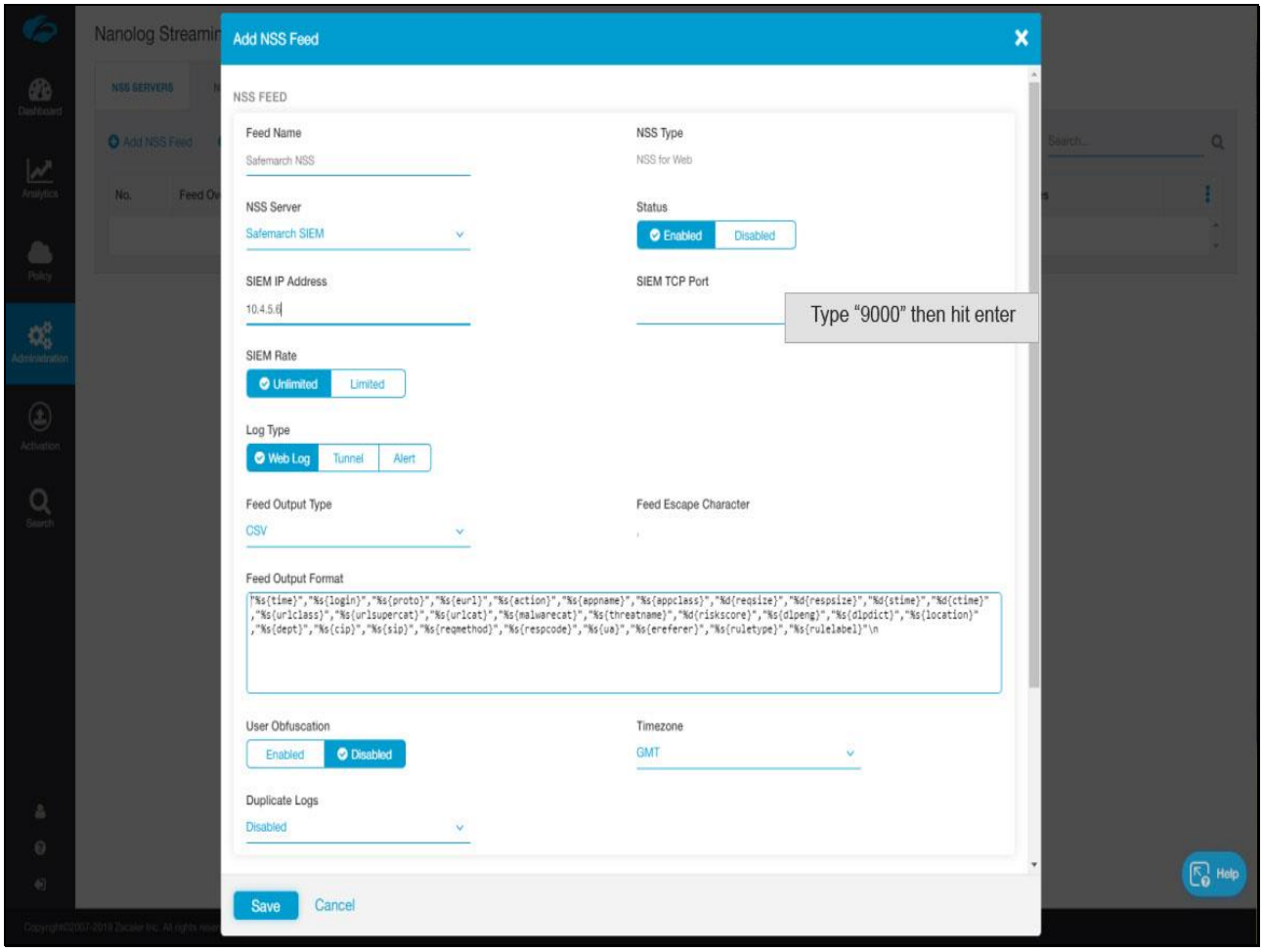

Add NSS Feed
NSS FEED
Feed Name
Safemarch NSS
NSS Type
NSS for Web
NSS Server
NONE
Safemarch SIEM
Click Box
Status
Enabled
Disabled
SIEM IP Address
SIEM TCP Port
Select
Safemarch SIEM
SIEM Rate
Unlimited
Log Type
Web Log
Tunnel
Alert
Feed Output Type
CSV
Feed Escape Character
Feed Output Format
User Obfuscation
Enabled
Disabled
Timezone
GMT
Duplicate Logs
Disabled
Save
Cancel
Help

Slide notes

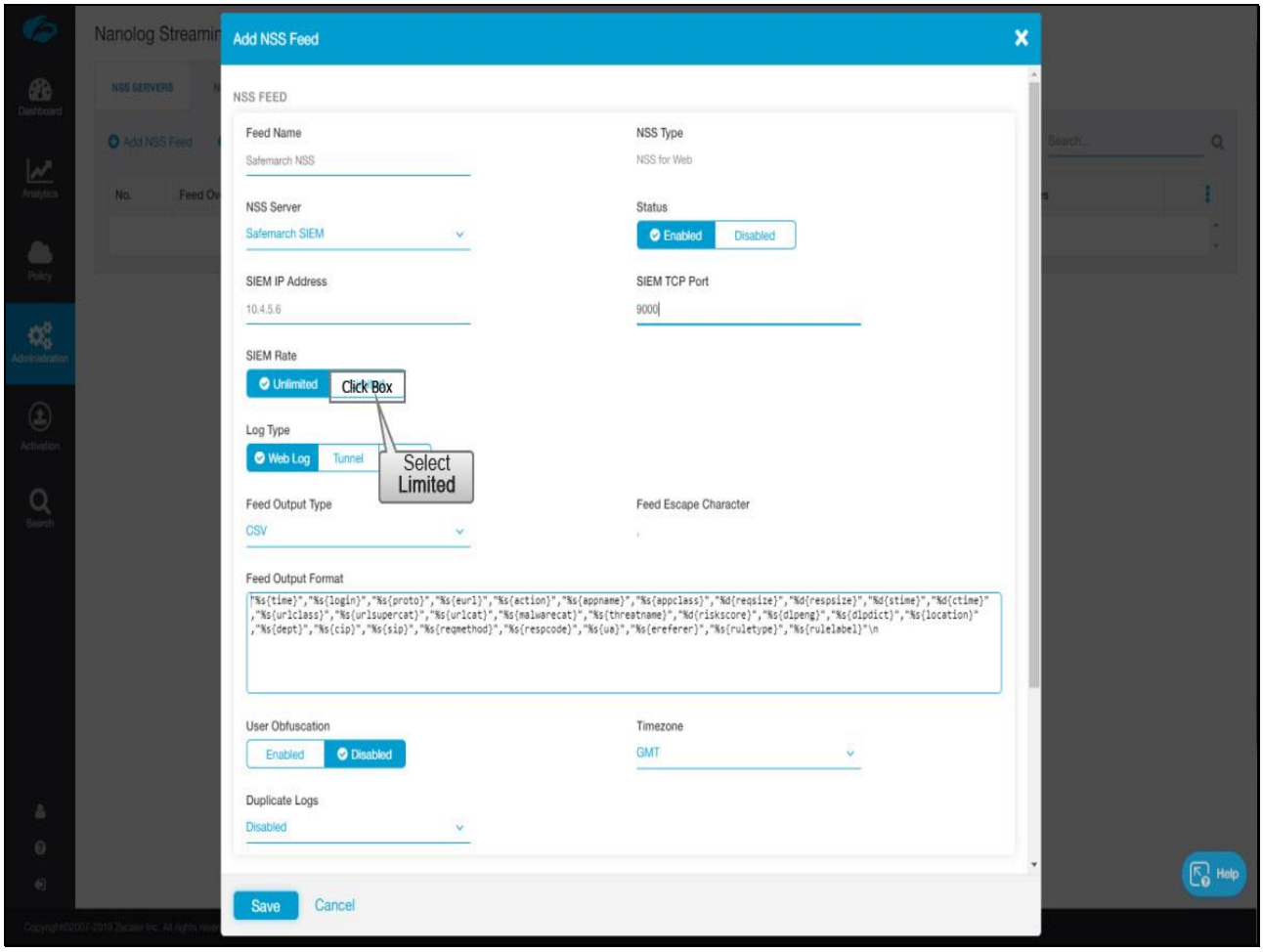


Slide notes

Enter the IP address and TCP port of your SIEM.

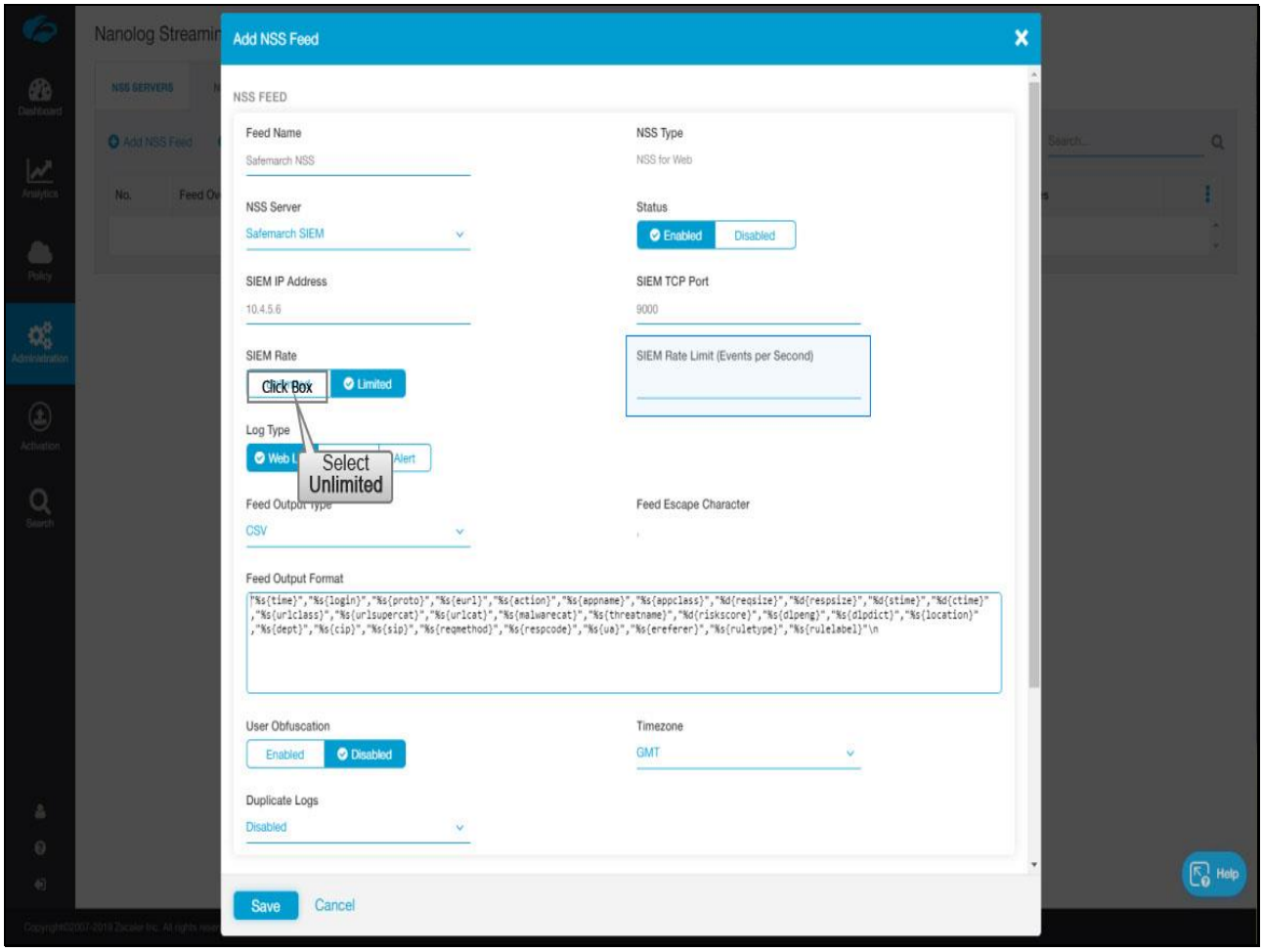

Nanolog Streamin
Add NSS Feed
NSS FEED
Feed Name
Safemarch NSS
NSS Type
NSS for Web
NSS Server
Safemarch SIEM
Status
Enabled
Disabled
SIEM IP Address
10.4.5.6
SIEM TCP Port
Type "9000" then hit enter
SIEM Rate
Unlimited
Limited
Log Type
Web Log
Tunnel
Alert
Feed Output Type
CSV
Feed Escape Character
Feed Output Format
"%s{time}","%s{login}","%s{proto}","%s{eurl}","%s{action}","%s{appname}","%s{appclass}","%d{reqsize}","%d{respsize}","%d{stime}","%d{ctime}"
,"%s{urlclass}","%s{urlsupercat}","%s{urlcat}","%s{malwarecat}","%s{threatname}","%d{riskscore}","%s{dlpeng}","%s{dlpdict}","%s{location}"
,"%s{dept}","%s{cip}","%s{sip}","%s{reqmethod}","%s{respcode}","%s{ua}","%s{ereferer}","%s{ruletype}","%s{rulelabel}"\n
User Obfuscation
Enabled
Disabled
Timezone
GMT
Duplicate Logs
Disabled
Save
Cancel
Help

Slide notes

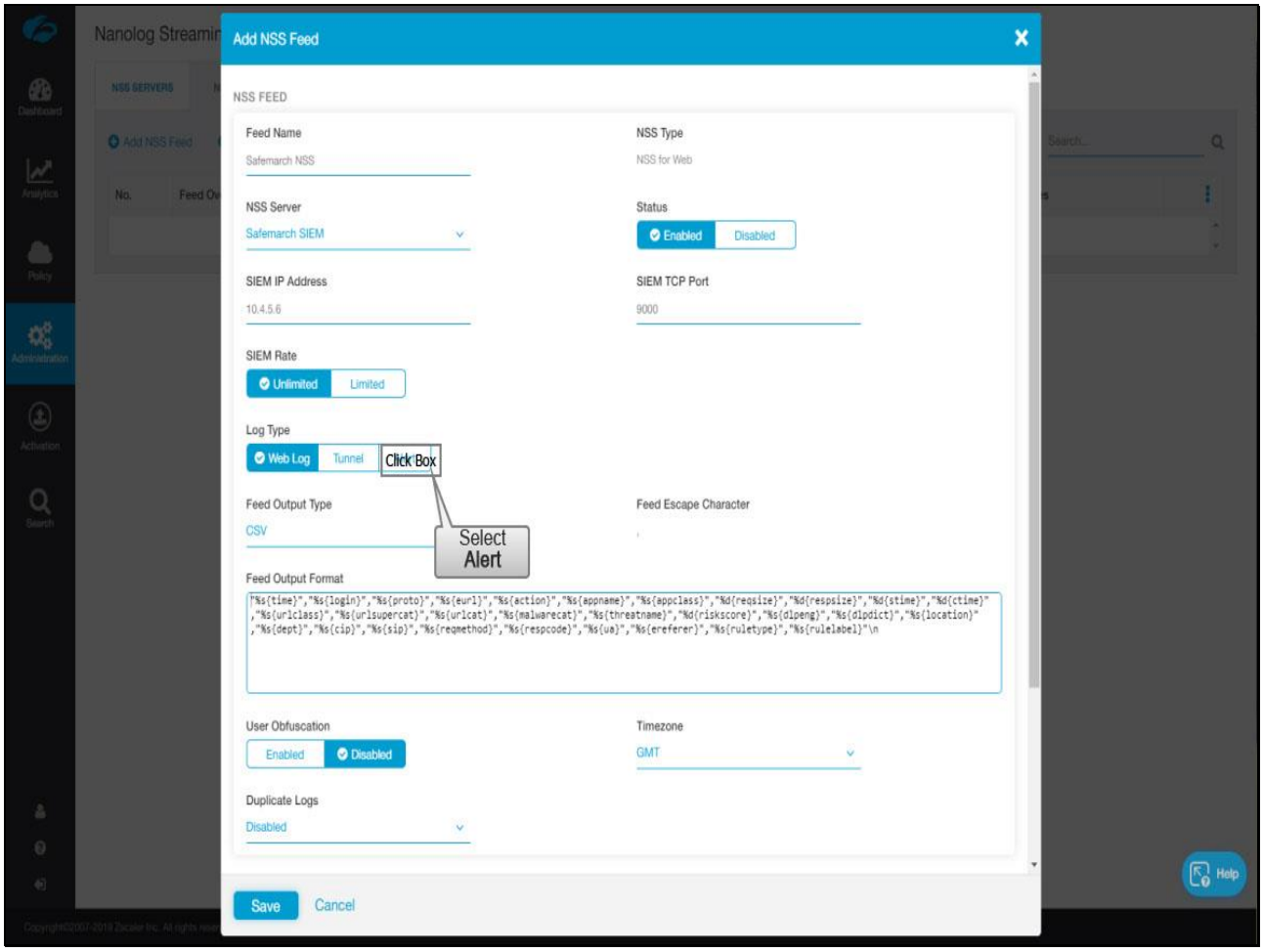


Slide notes

You can throttle the number of events per second that are streamed to your SIEM. Click Limited.

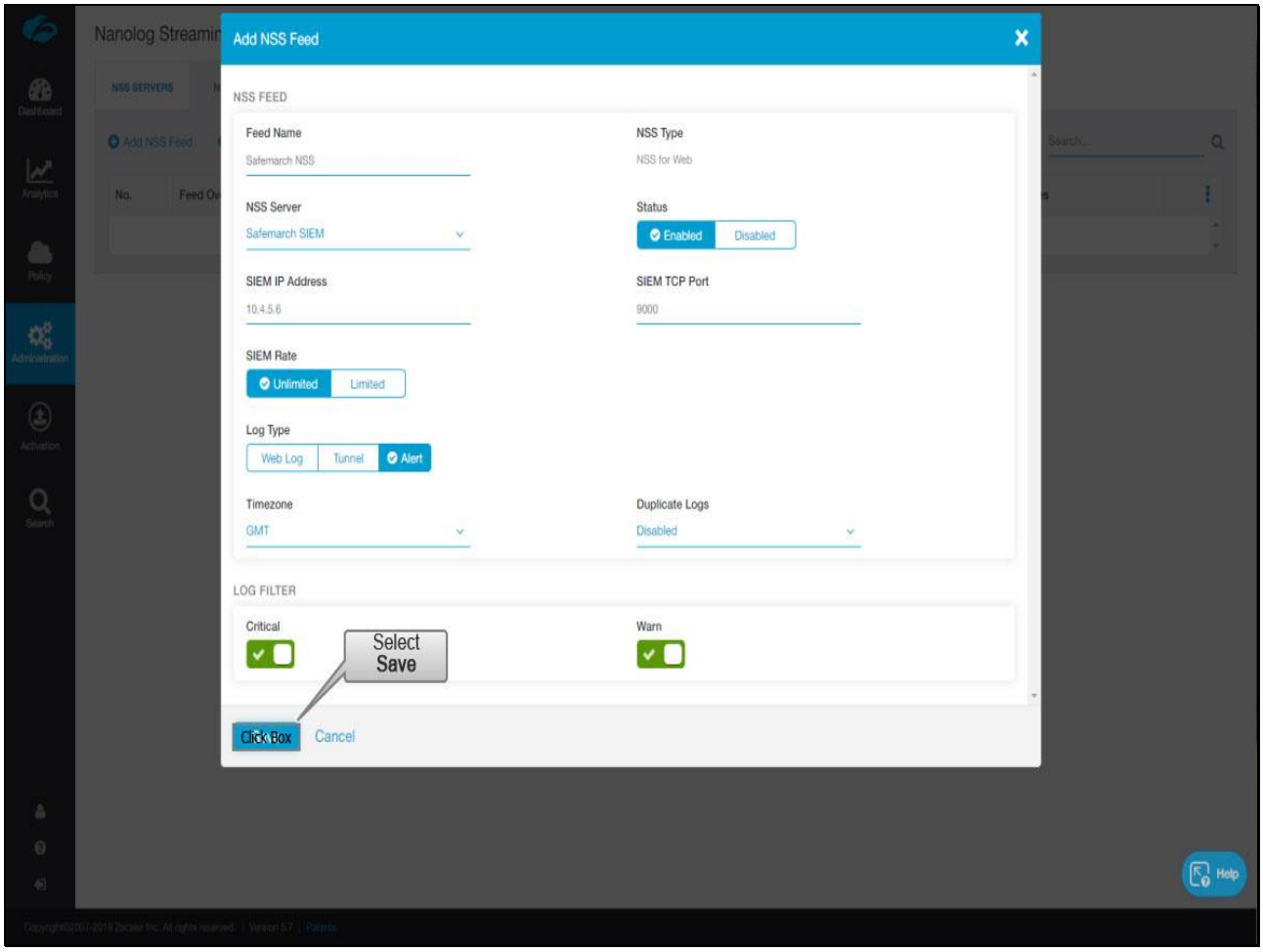

Add NSS Feed
NSS FEED
Feed Name
Safemarch NSS
NSS Type
NSS for Web
NSS Server
Safemarch SIEM
Status
Enabled
Disabled
SIEM IP Address
10.4.5.6
SIEM TCP Port
9000
SIEM Rate
Click Box
Limited
SIEM Rate Limit (Events per Second)
Log Type
Select Unlimited
Feed Output Type
CSV
Feed Escape Character
Feed Output Format
User Obfuscation
Enabled
Disabled
Timezone
GMT
Duplicate Logs
Disabled
Save
Cancel
Help

Slide notes



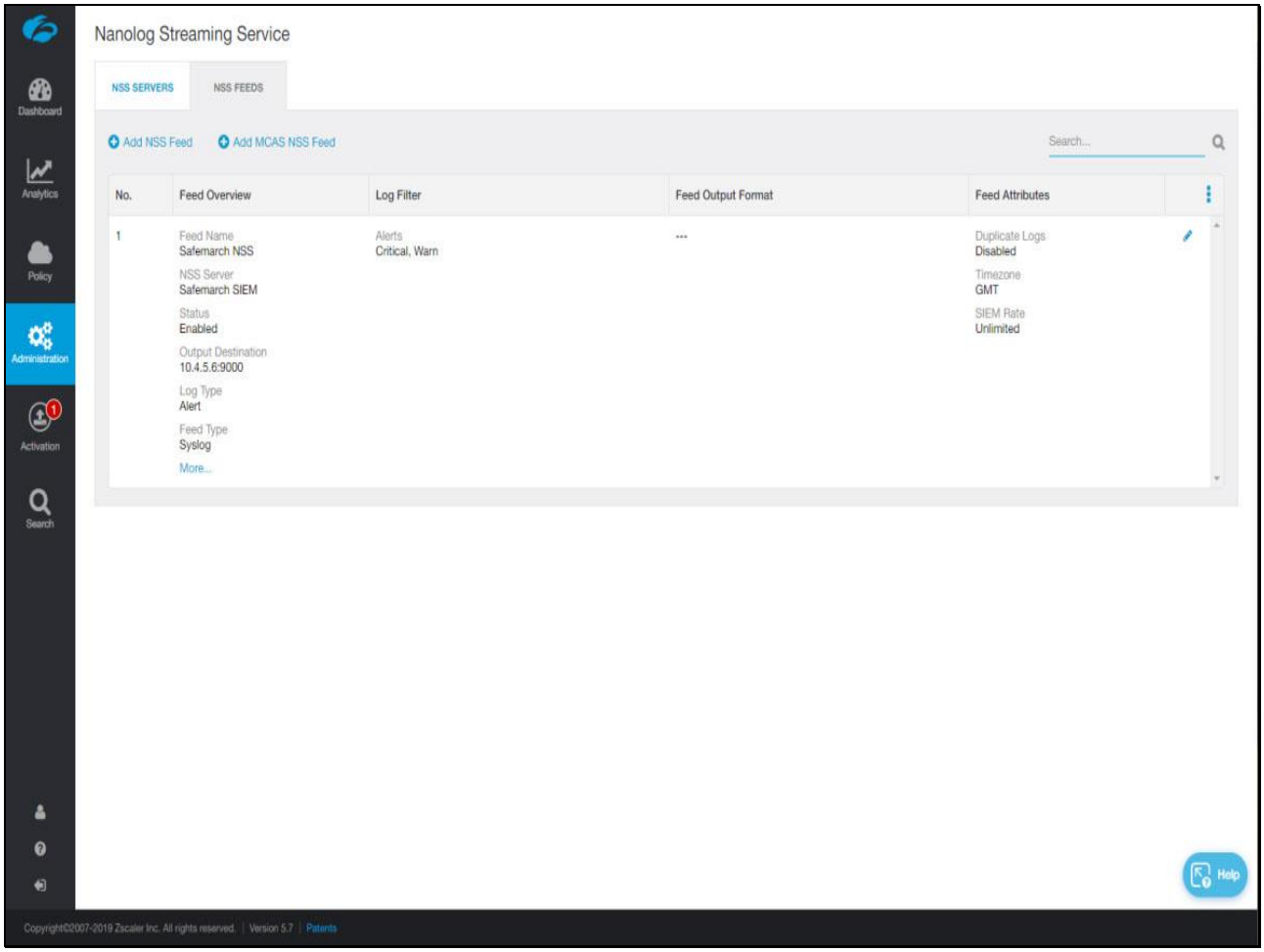
Slide notes

For log type click “Alert”.



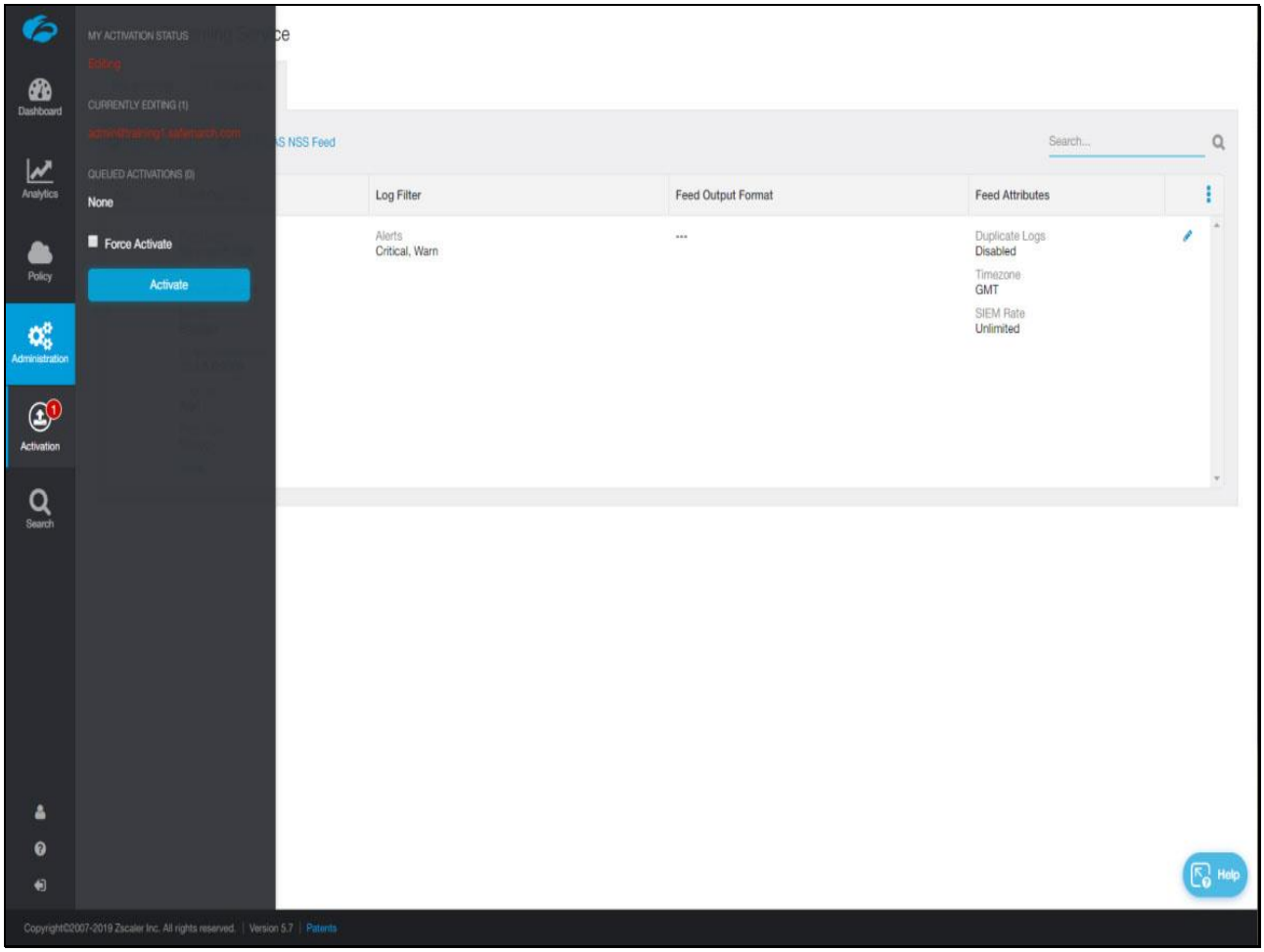
Slide notes

Click “Save”.

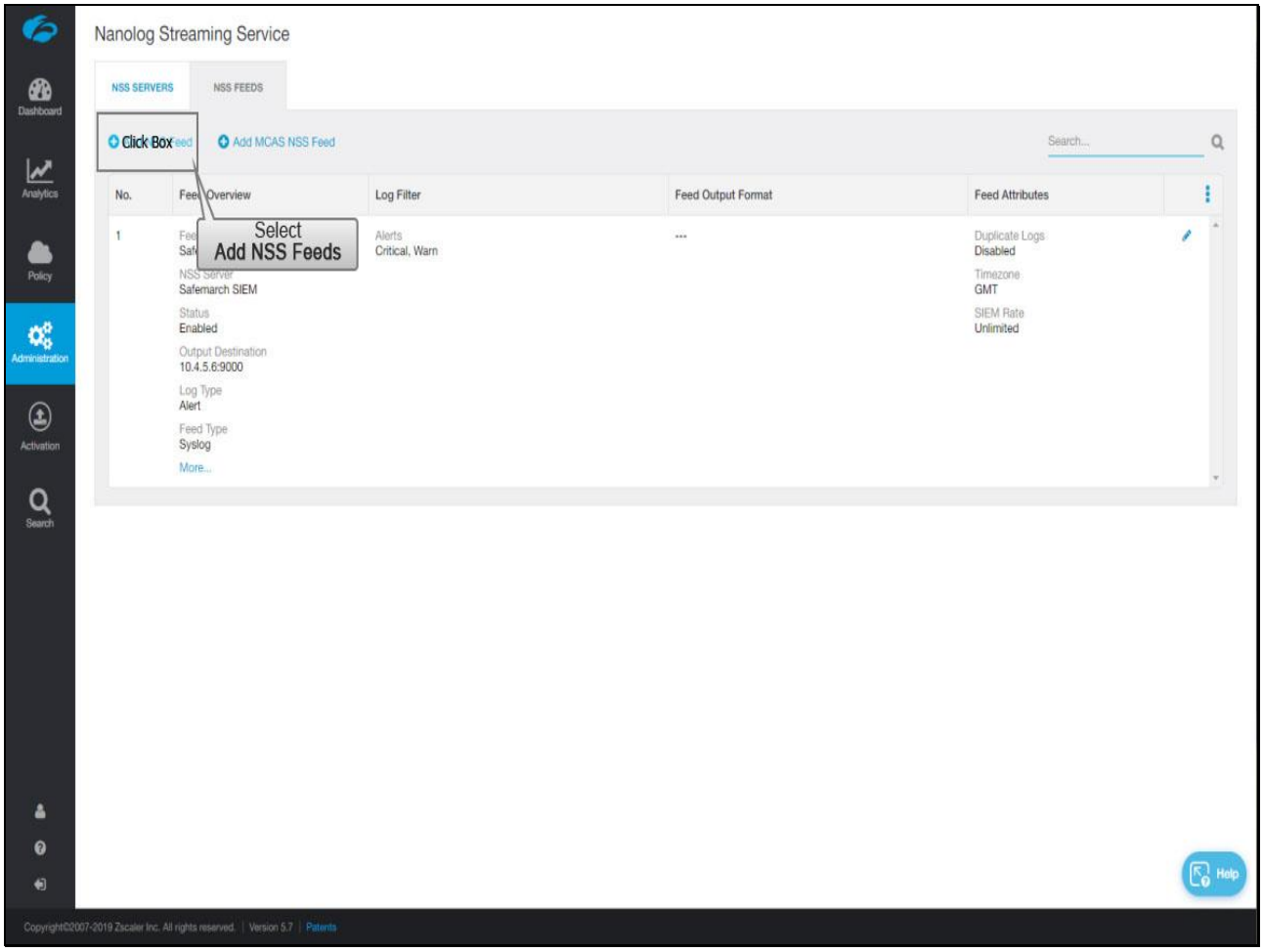


Slide notes

Then **Activate** your changes.

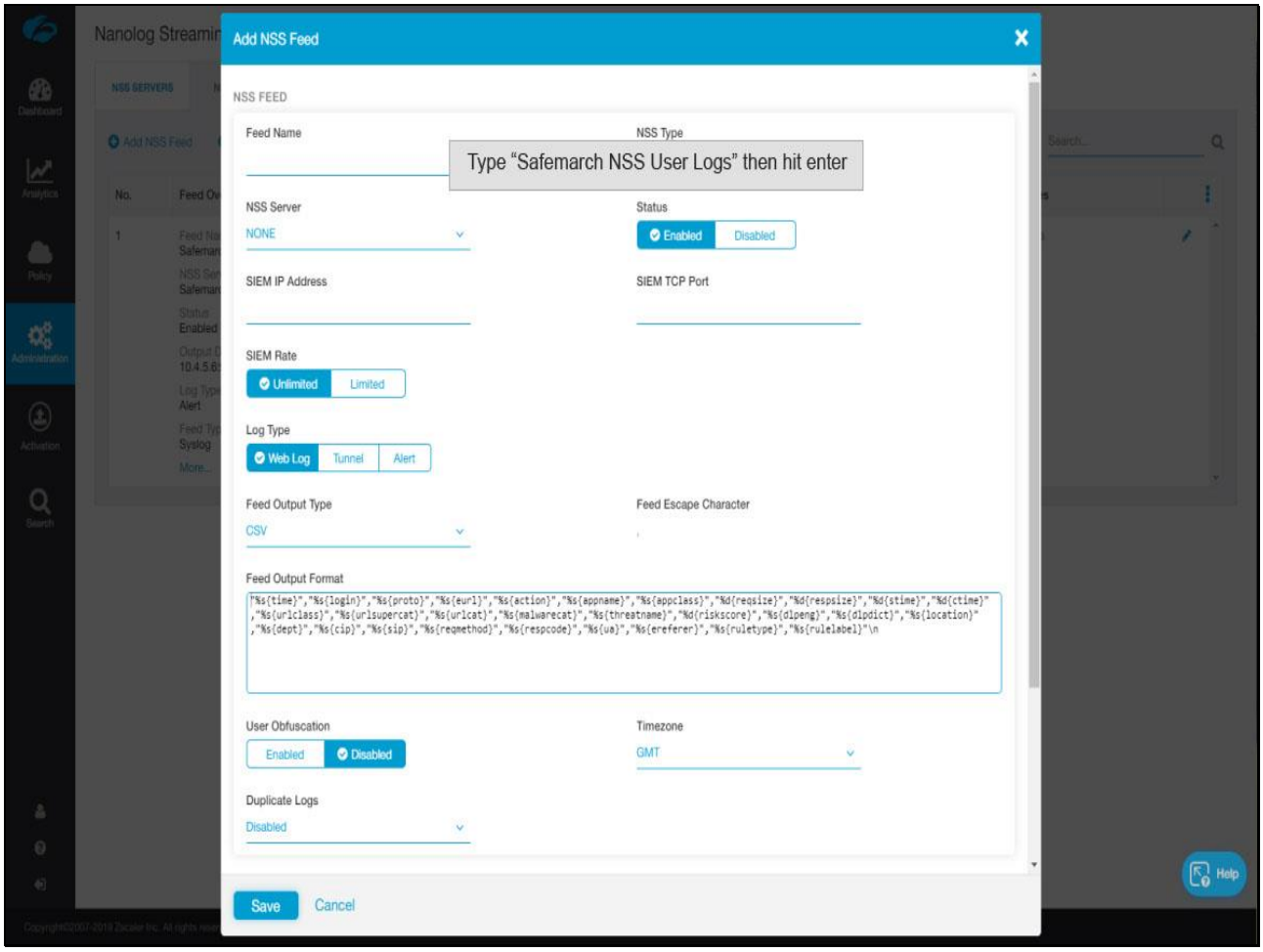

MY ACTIVATION STATUS
Editing
CURRENTLY EDITING (1)
QUEUED ACTIVATIONS (0)
None
Force Activate
Activate
Dashboard
Analytics
Policy
Administration
Activation
Search
Search...
Log Filter
Feed Output Format
Feed Attributes
Alerts
Critical, Warn
Duplicate Logs
Disabled
Timezone
GMT
SIEM Rate
Unlimited
Help
Version 5.7
Patents

Slide notes



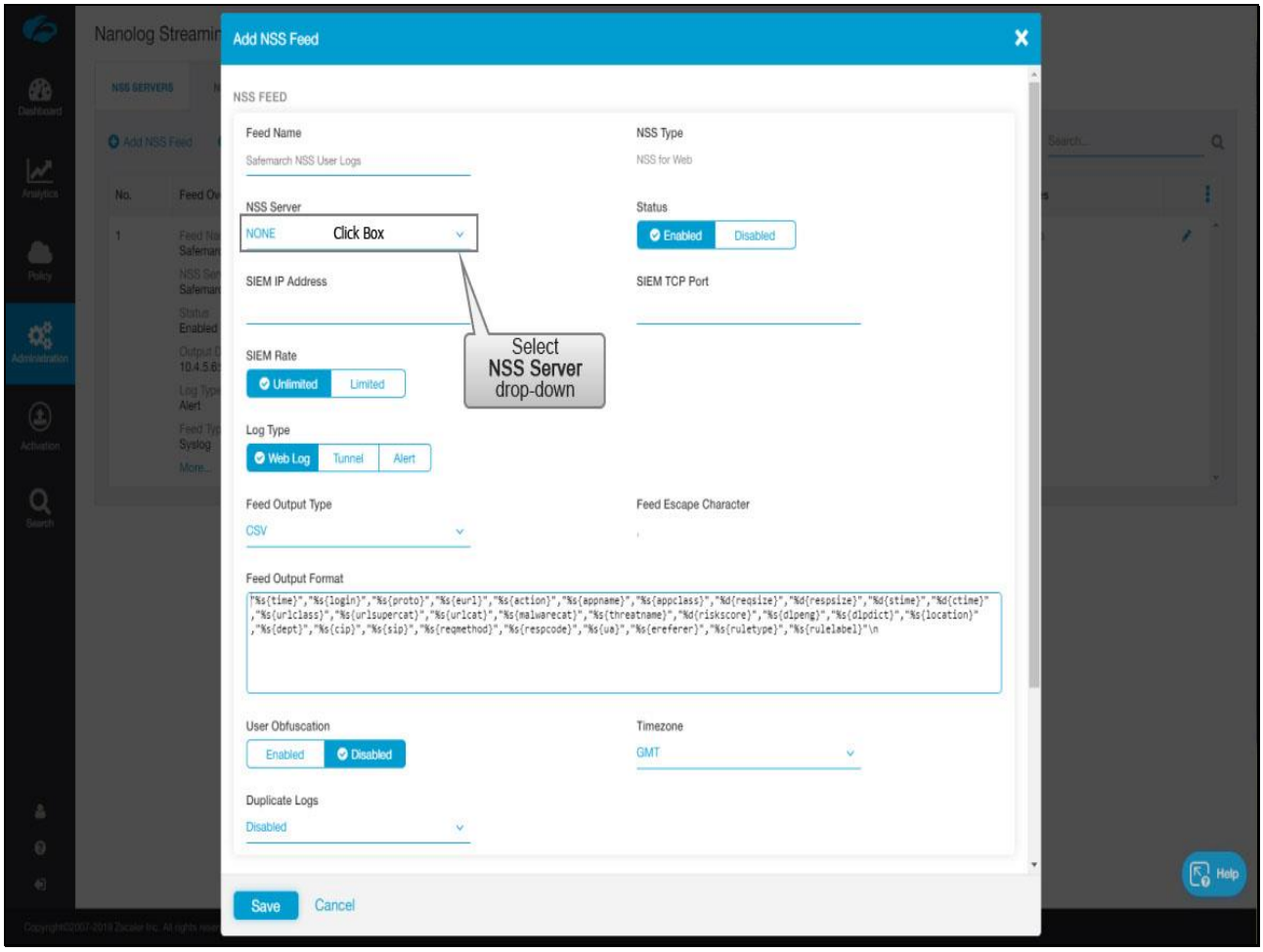
Slide notes

Now we'll configure the log feed. Click "Add NSS Feed".



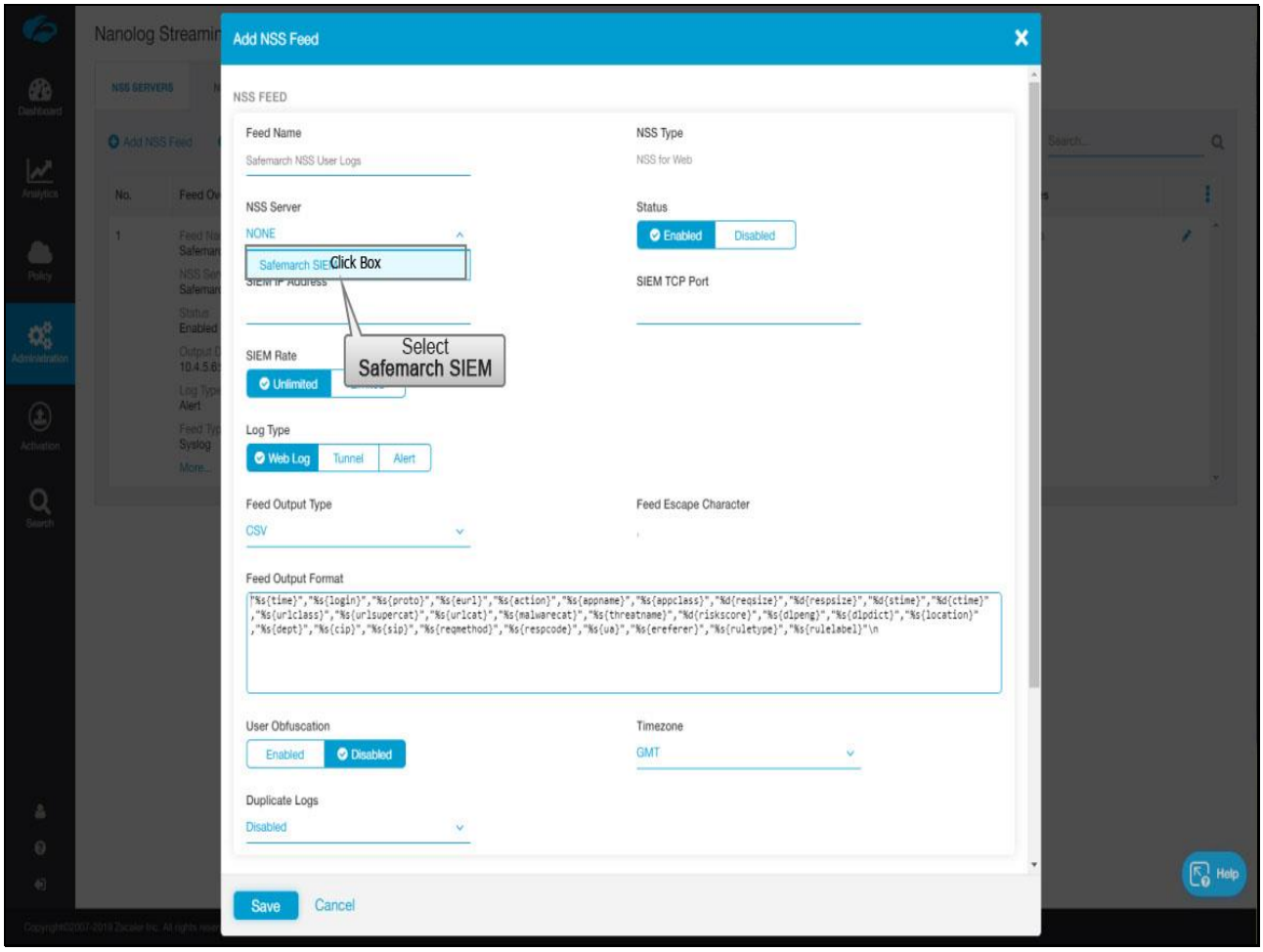
Slide notes

Enter a name for the feed

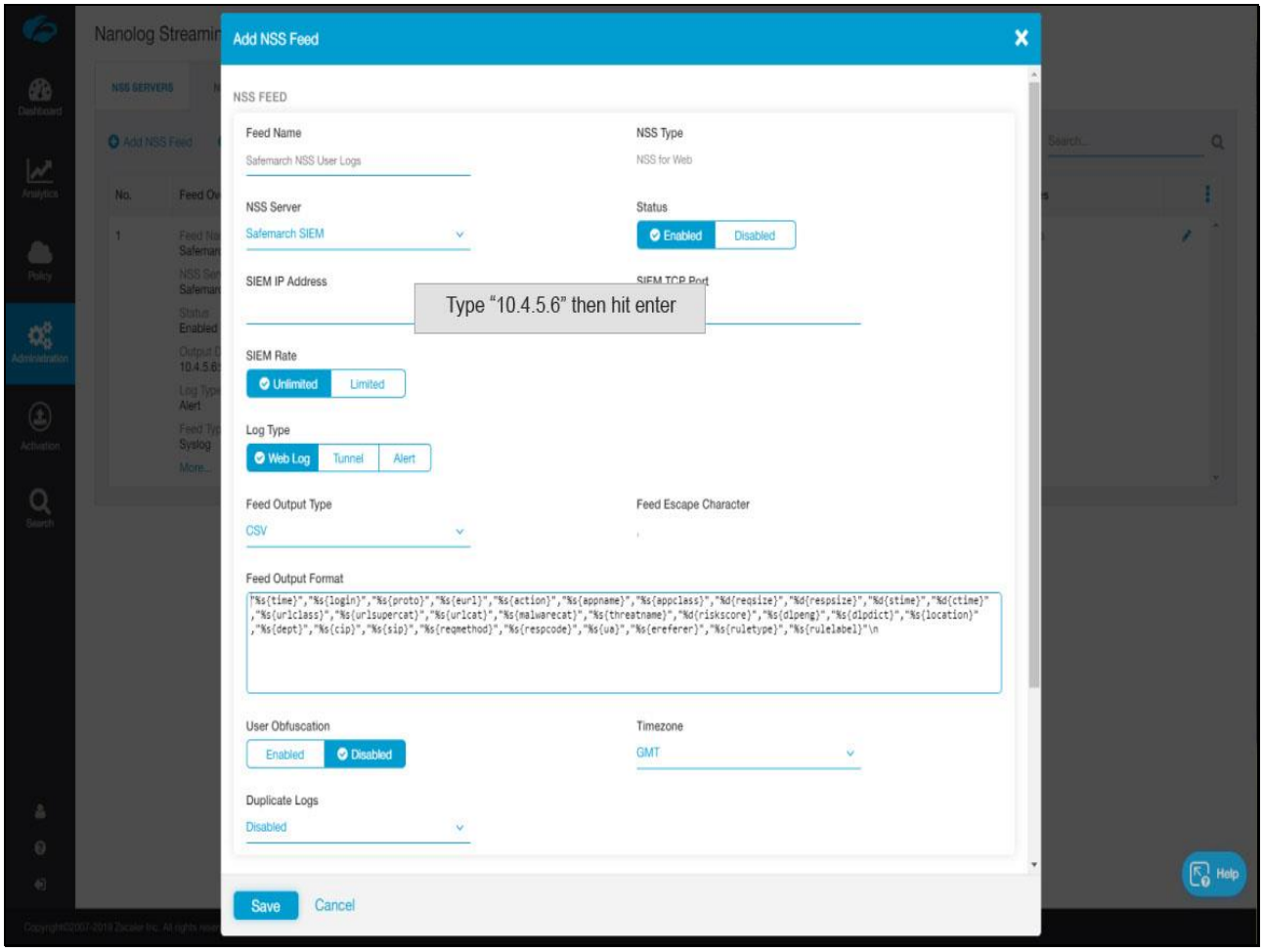


Slide notes

and select the NSS server.

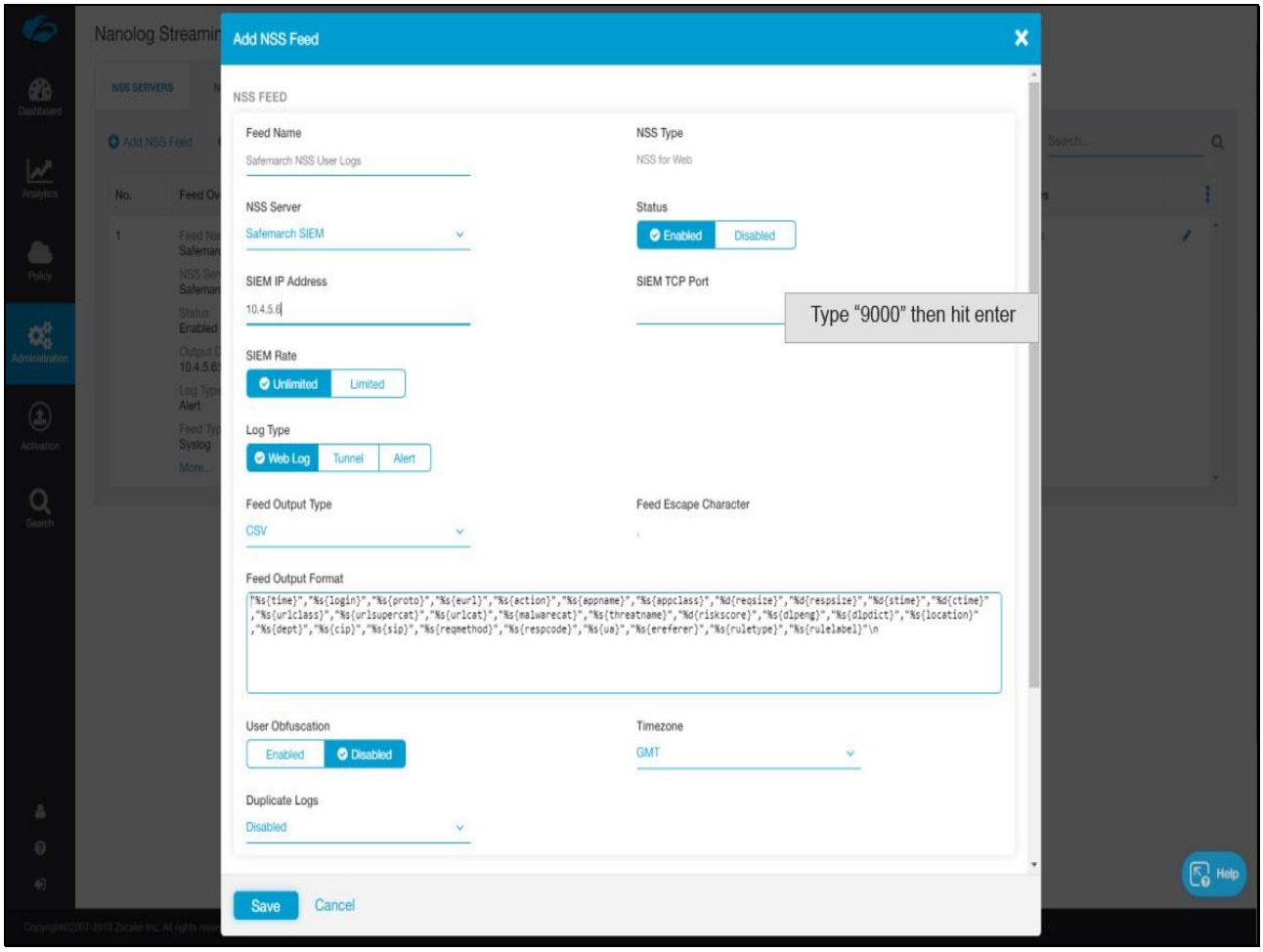

Add NSS Feed
NSS FEED
Feed Name
Safemarch NSS User Logs
NSS Type
NSS for Web
NSS Server
NONE
Safemarch SIEM
Click Box
Status
Enabled
Disabled
SIEM IP Address
SIEM TCP Port
Select
Safemarch SIEM
SIEM Rate
Unlimited
Log Type
Web Log
Tunnel
Alert
Feed Output Type
CSV
Feed Escape Character
Feed Output Format
"%s{time}","%s{login}","%s{proto}","%s{eurl}","%s{action}","%s{appname}","%s{appclass}","%d{reqsize}","%d{respsize}","%d{stime}","%d{ctime}"
,"%s{urlclass}","%s{urlsupercat}","%s{urlcat}","%s{malwarecat}","%s{threatname}","%d{riskscore}","%s{dlpeng}","%s{dlpdict}","%s{location}"
,"%s{dept}","%s{cip}","%s{sip}","%s{reqmethod}","%s{respcode}","%s{ua}","%s{ereferer}","%s{ruletype}","%s{rulelabel}"\n
User Obfuscation
Enabled
Disabled
Timezone
GMT
Duplicate Logs
Disabled
Save
Cancel
Help

Slide notes

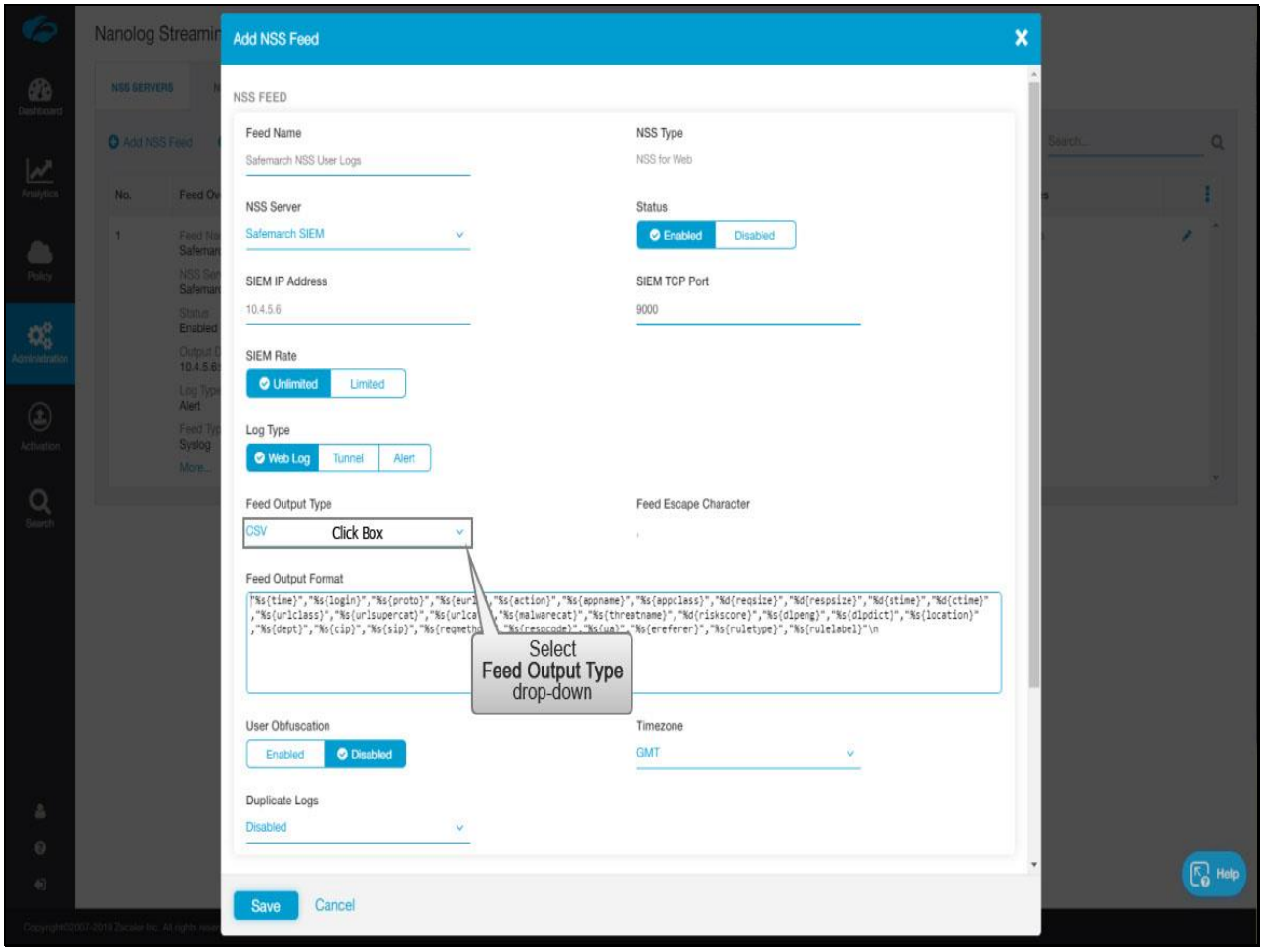


Slide notes

Enter the IP address and TCP port of your SIEM.

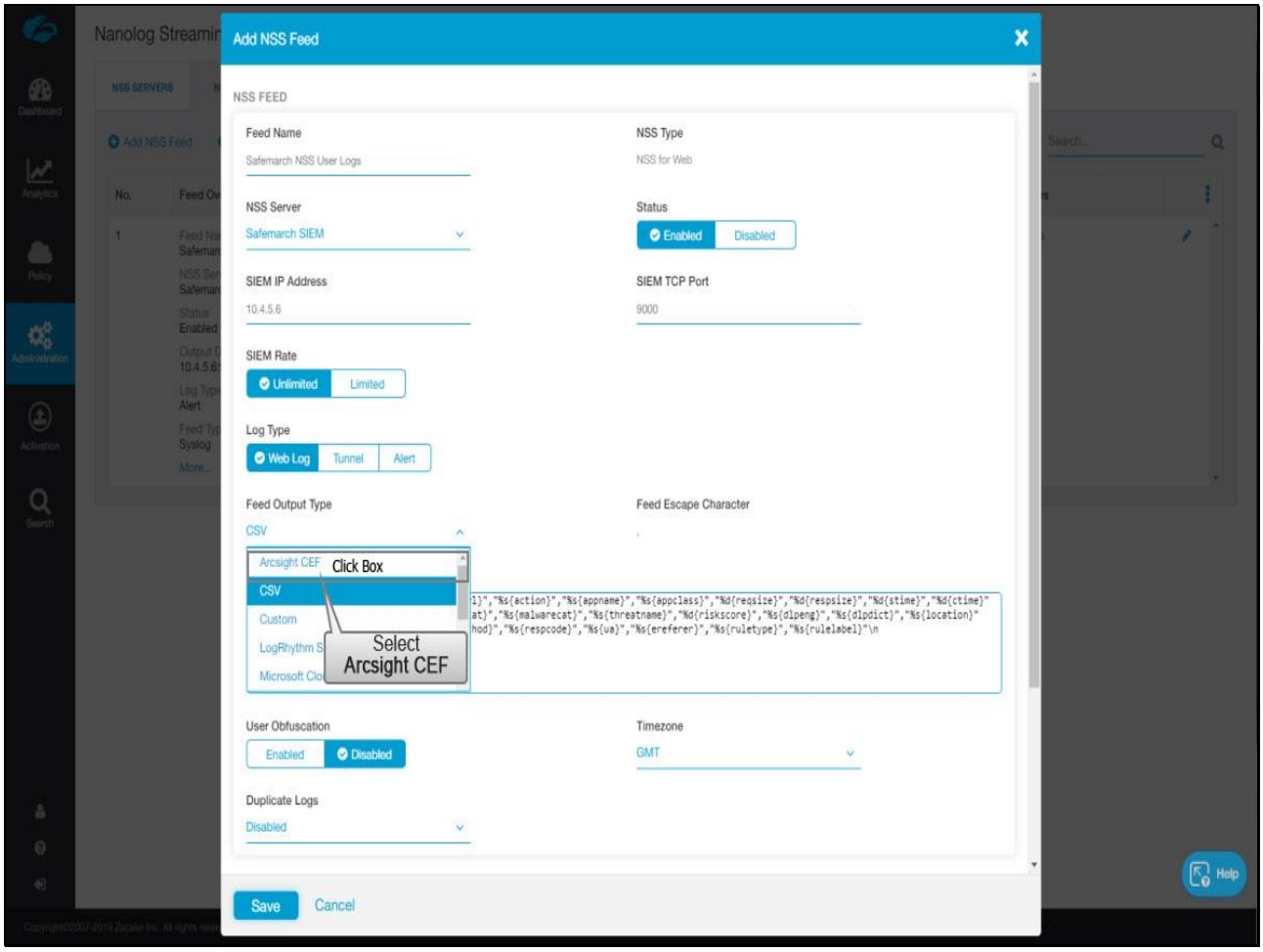

Add NSS Feed
NSS FEED
Feed Name
Safemarch NSS User Logs
NSS Type
NSS for Web
NSS Server
Safemarch SIEM
Status
Enabled
Disabled
SIEM IP Address
10.4.5.6
SIEM TCP Port
Type "9000" then hit enter
SIEM Rate
Unlimited
Limited
Log Type
Web Log
Tunnel
Alert
Feed Output Type
CSV
Feed Escape Character
Feed Output Format
"%s{time}","%s{login}","%s{proto}","%s{eurl}","%s{action}","%s{appname}","%s{appclass}","%d{reqsize}","%d{respsize}","%d{stime}","%d{ctime}"
,"%s{urlclass}","%s{urlsupercat}","%s{urlcat}","%s{malwarecat}","%s{threatname}","%d{riskscore}","%s{dlpeng}","%s{dlpdict}","%s{location}"
,"%s{dept}","%s{cip}","%s{sip}","%s{reqmethod}","%s{respcode}","%s{ua}","%s{ereferer}","%s{ruletype}","%s{rulelabel}"\n
User Obfuscation
Enabled
Disabled
Timezone
GMT
Duplicate Logs
Disabled
Save
Cancel
Help

Slide notes

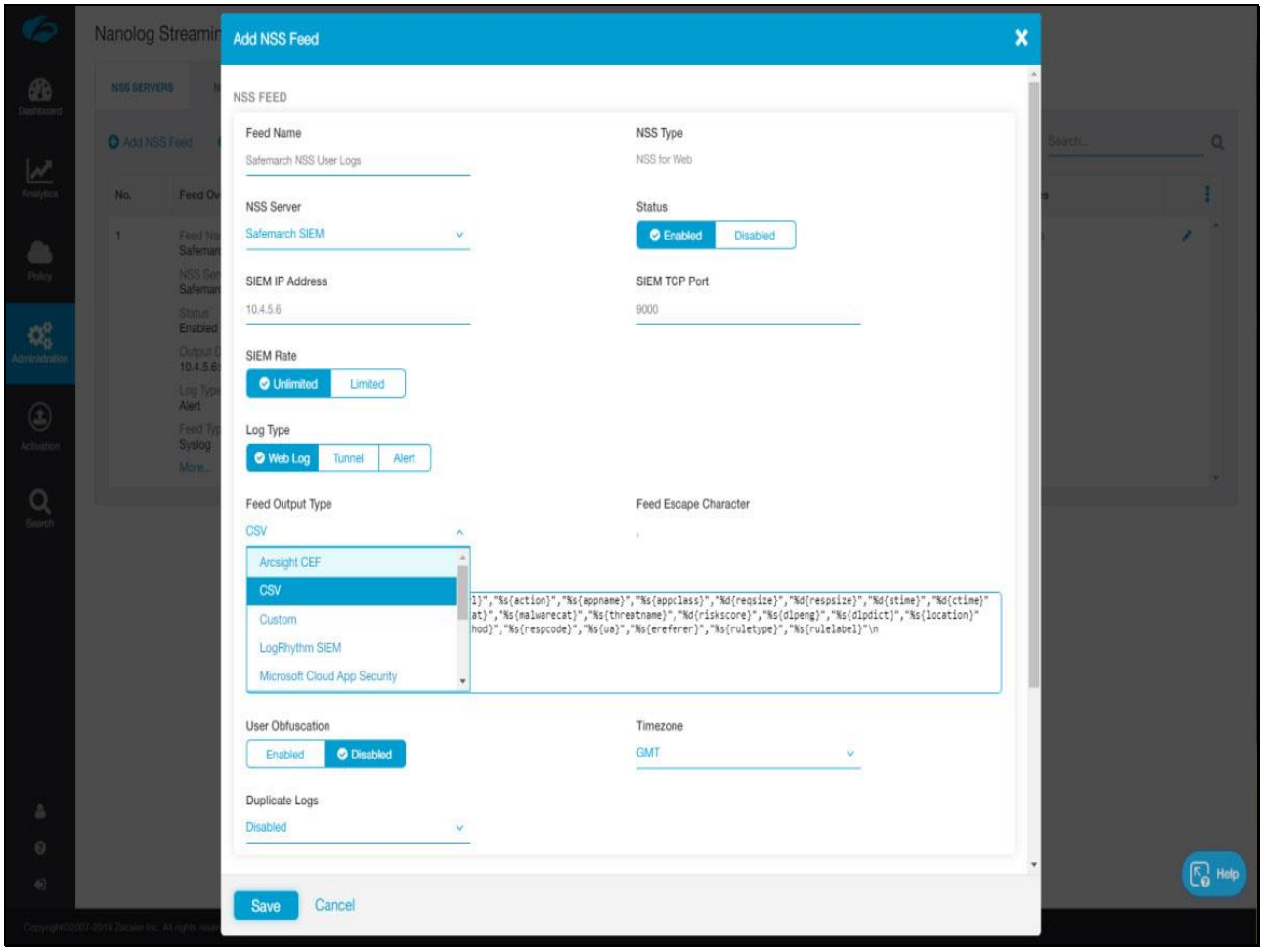


Slide notes

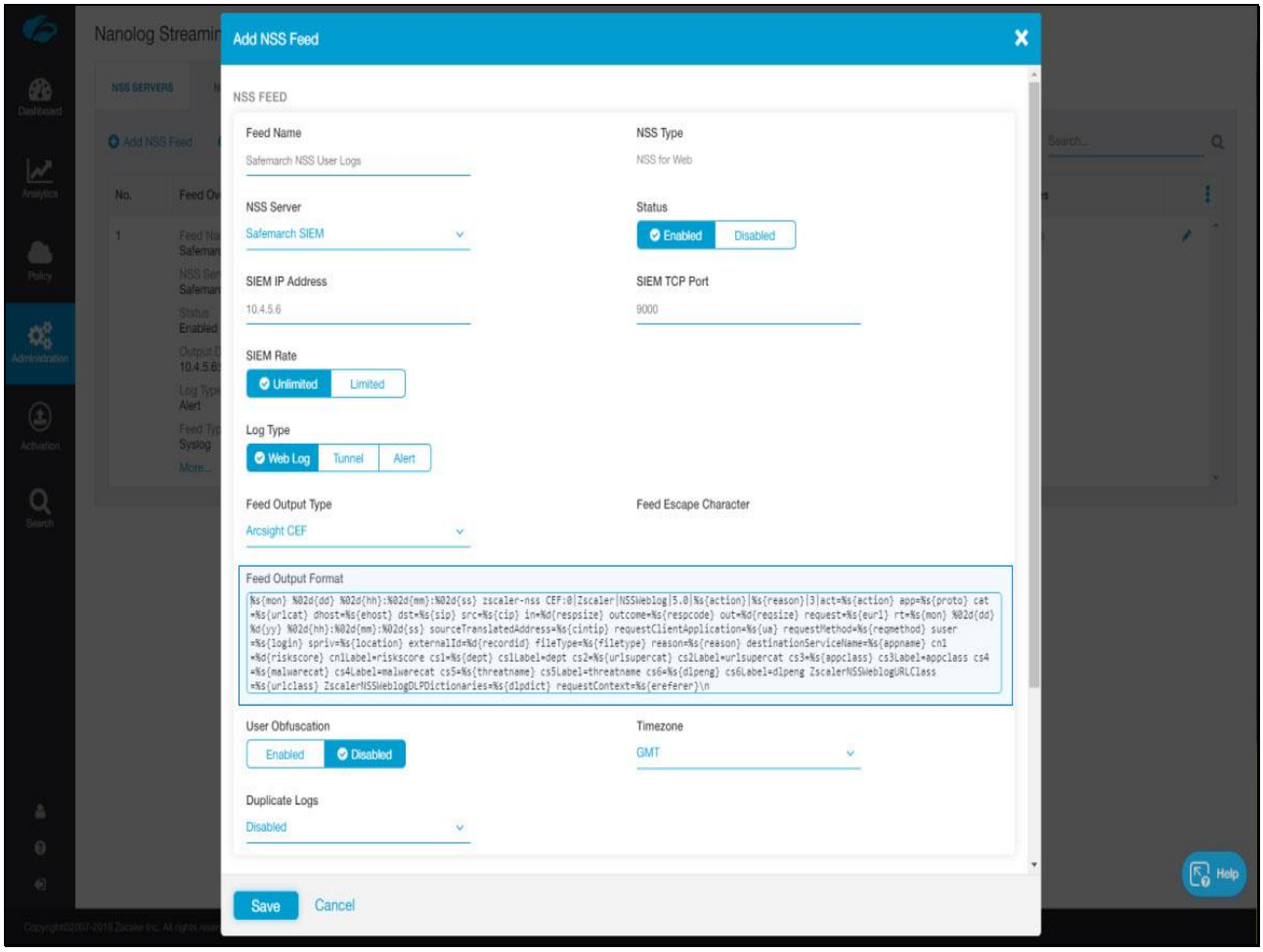
For Feed output type, choose you SIEM.


Add NSS Feed
NSS FEED
Feed Name
Safemarch NSS User Logs
NSS Type
NSS for Web
NSS Server
Safemarch SIEM
Status
Enabled
Disabled
SIEM IP Address
10.4.5.6
SIEM TCP Port
9000
SIEM Rate
Unlimited
Limited
Log Type
Web Log
Tunnel
Alert
Feed Output Type
CSV
Feed Escape Character
Arcsight CEF
Click Box
CSV
Custom
LogRhythm
Microsoft
Select
Arcsight CEF
User Obfuscation
Enabled
Disabled
Timezone
GMT
Duplicate Logs
Disabled
Save
Cancel
Help

Slide notes

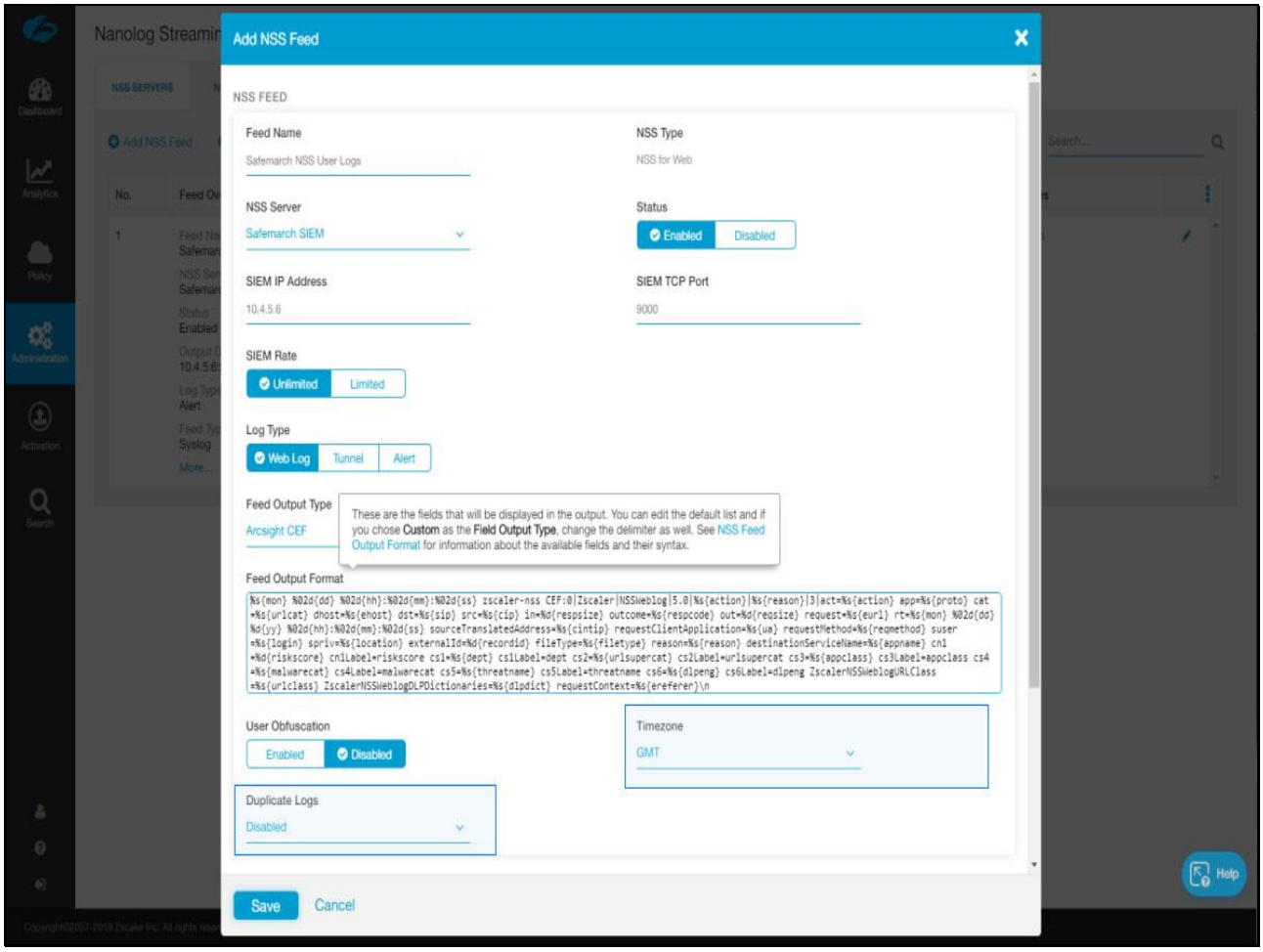

Add NSS Feed
NSS FEED
Feed Name
Safemarch NSS User Logs
NSS Type
NSS for Web
NSS Server
Safemarch SIEM
Status
Enabled
Disabled
SIEM IP Address
10.4.5.6
SIEM TCP Port
9000
SIEM Rate
Unlimited
Limited
Log Type
Web Log
Tunnel
Alert
Feed Output Type
CSV
Feed Escape Character
Arcsight CEF
CSV
Custom
LogRhythm SIEM
Microsoft Cloud App Security
User Obfuscation
Enabled
Disabled
Timezone
GMT
Duplicate Logs
Disabled
Save
Cancel
Help

Slide notes



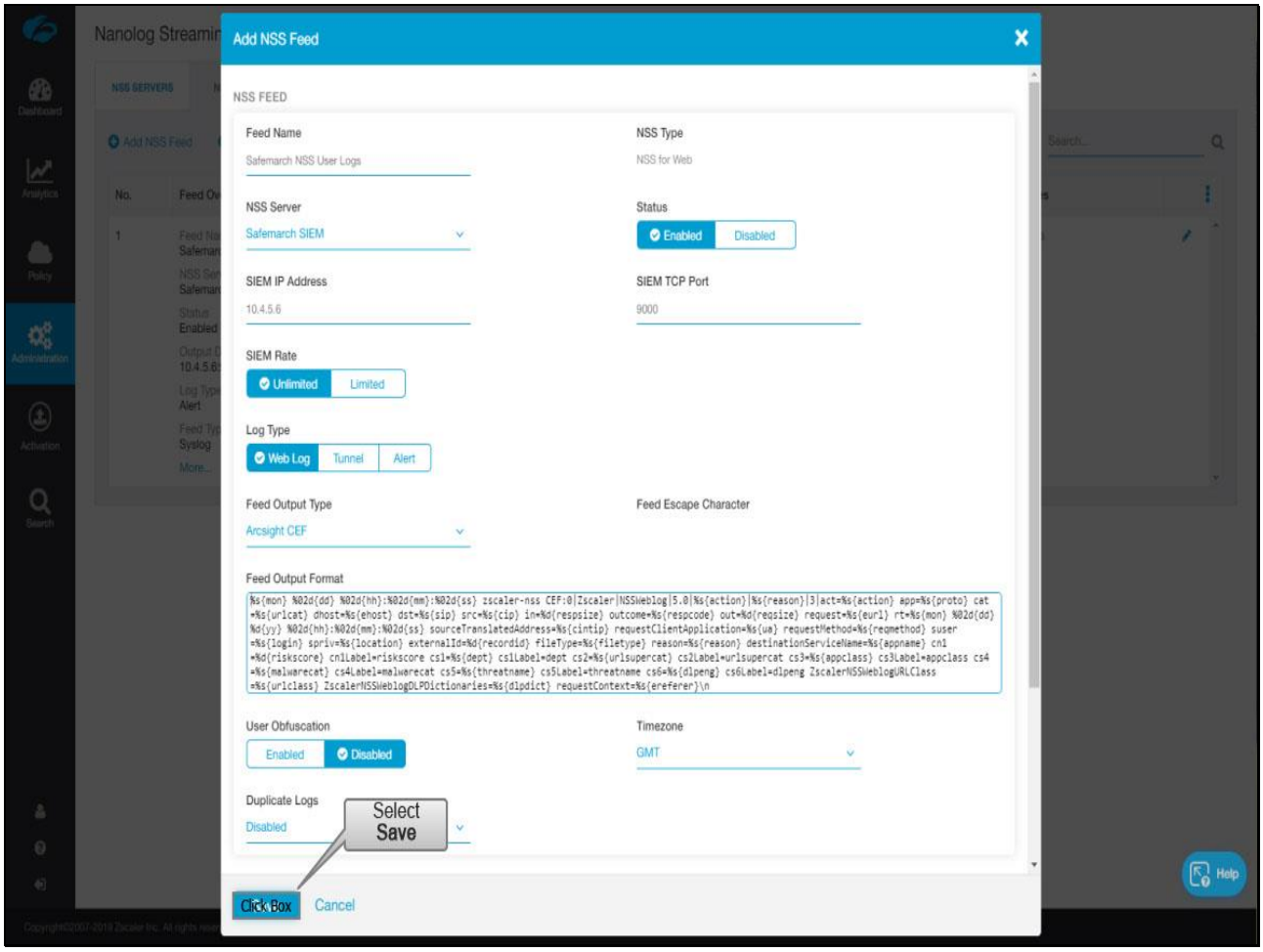
Slide notes

This will auto populate the Feed Output format. You can edit that field if you wish. If you click the tooltip it will open a page with details on all of the available fields.



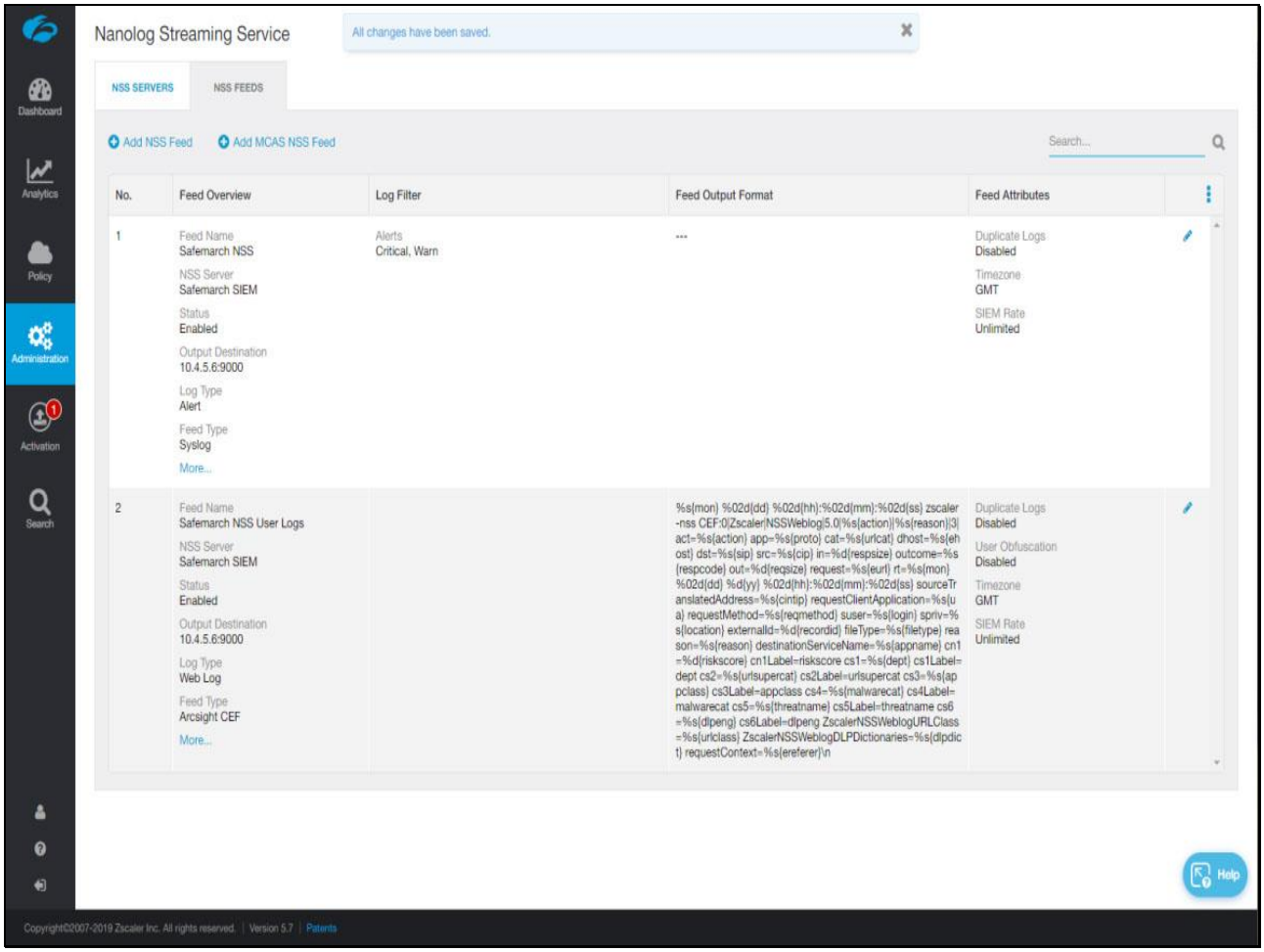
Slide notes

Time zone defaults to whatever is specified in the Company Profile. The Duplicate Logs setting specifies how far back in time NSS should resend logs after a connectivity loss between the NSS and SIEM.



Slide notes

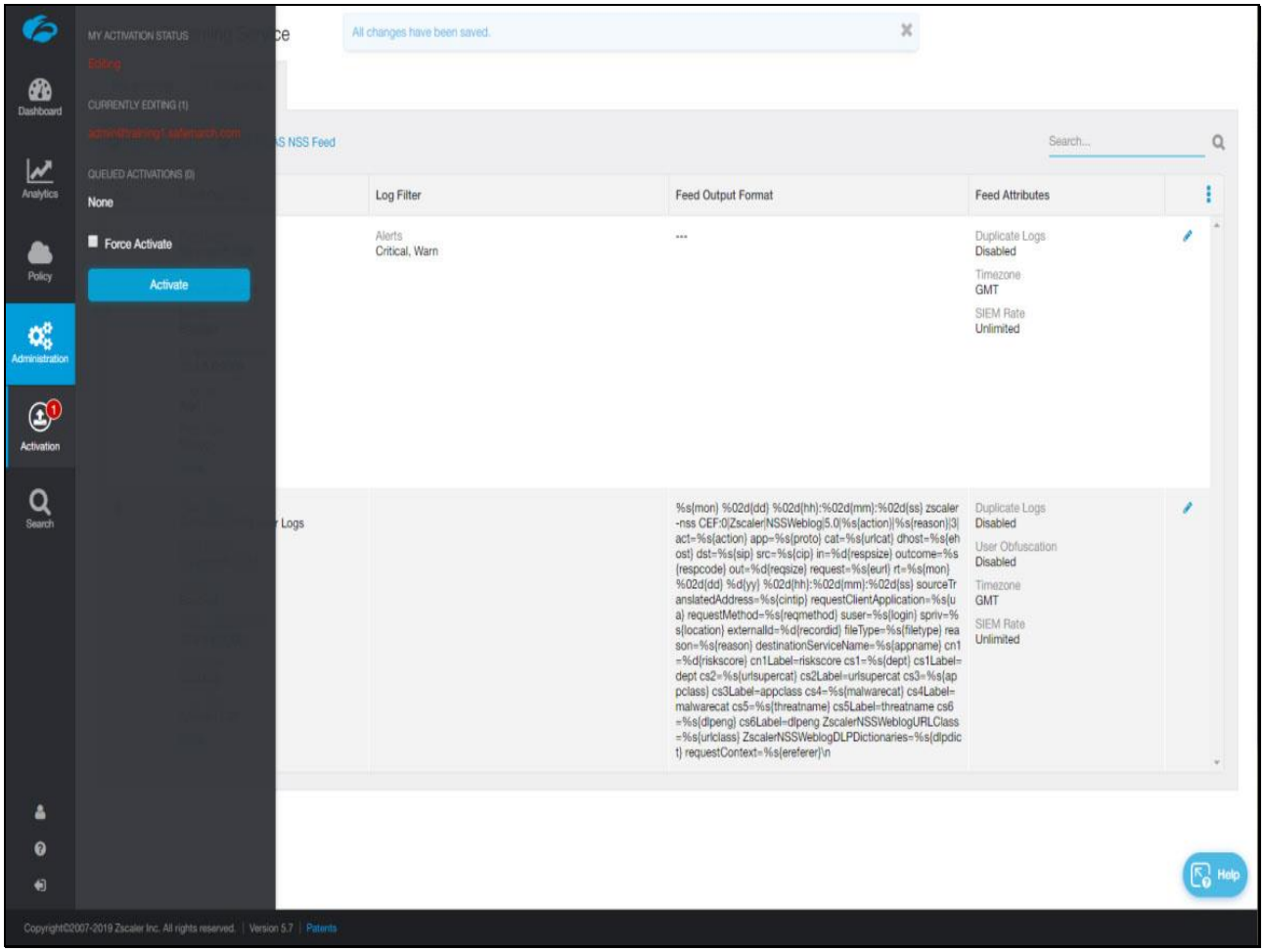
The last section allows you to apply filters to limit which logs are sent. In this example you will send everything so we will leave the defaults. You should check out the NSS Guide on the Help Portal for detailed information about the various filters available. Click “Save”.



Slide notes

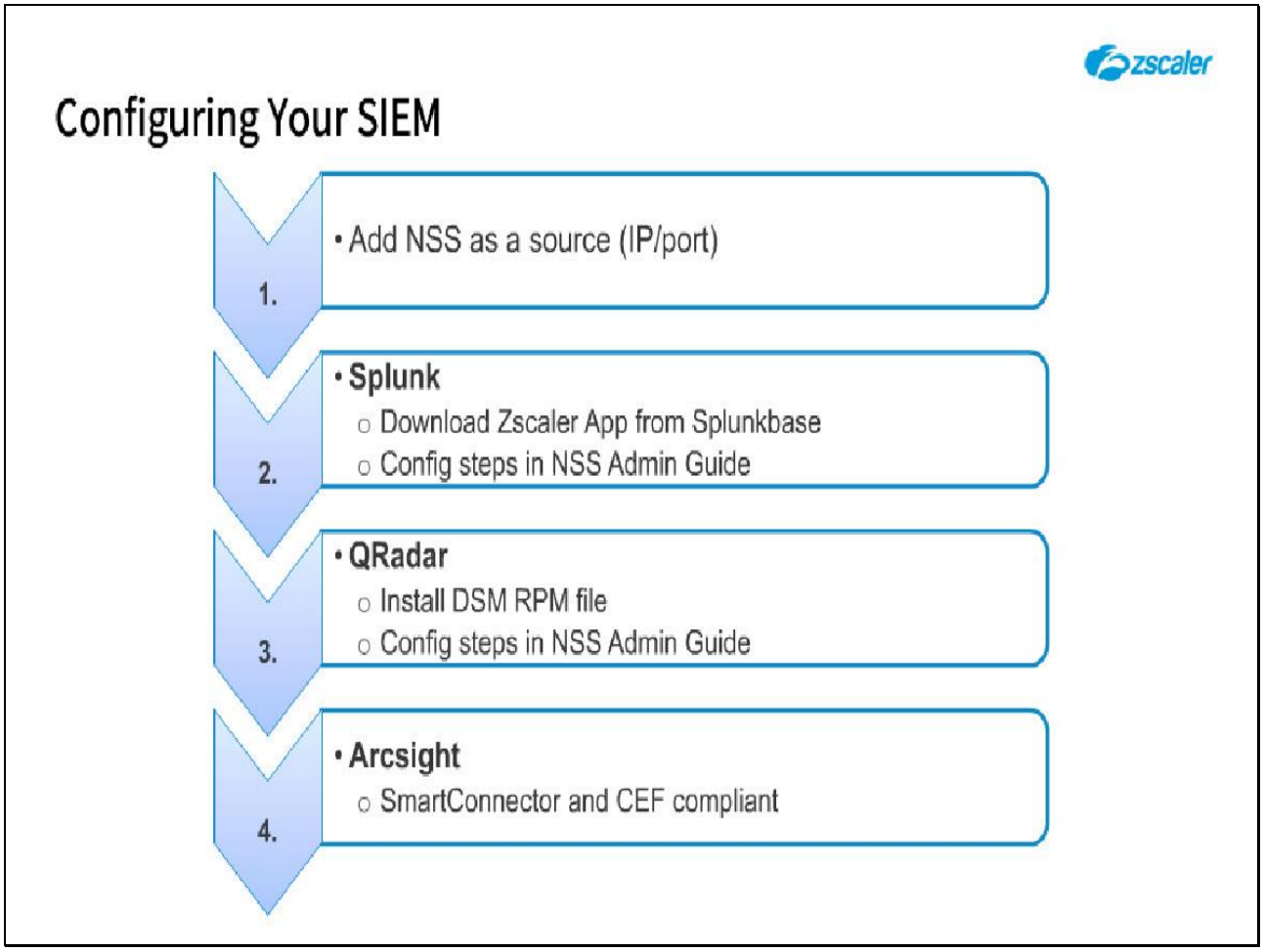
Then **Activate** your changes.

Slide 118 - Slide 118



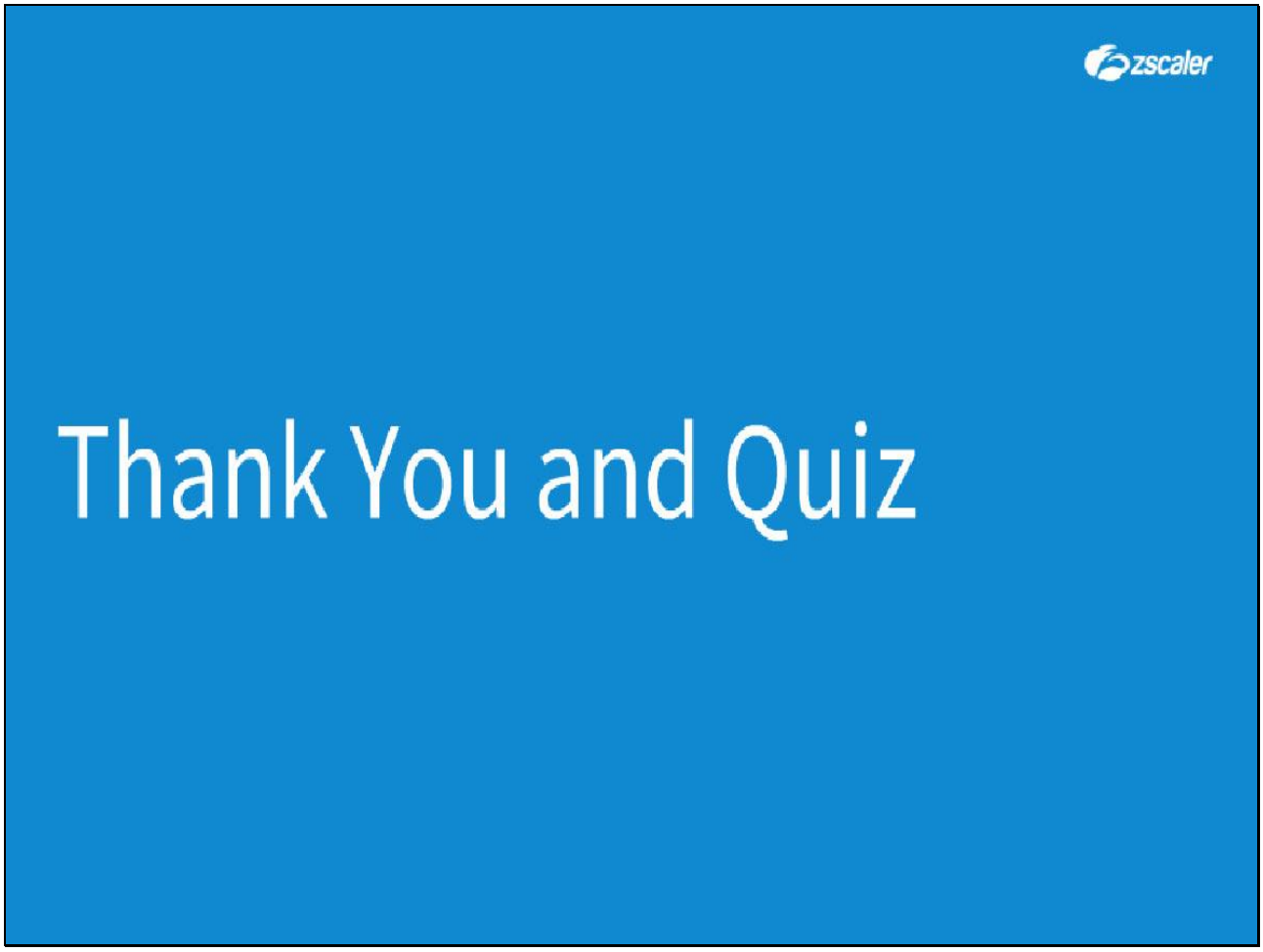
Slide notes

Slide notes



Slide notes

The last step is to configure your SIEM to accept logs from the NSS VM. There are config steps for a few SIEMs here and in the NSS Guide. If you're using a different SIEM you should follow your SIEM's documentation.



Slide notes

This completes the Zscaler Nanolog Streaming Service module. We hope this module has been useful to you and thank you for your time. What will follow is a short quiz to test your knowledge of the material presented in this module. You may retake the quiz as many times as necessary to pass.