



DIY Lab Operations Manual v1.0

INTERNAL USE ONLY

Evin Safdia

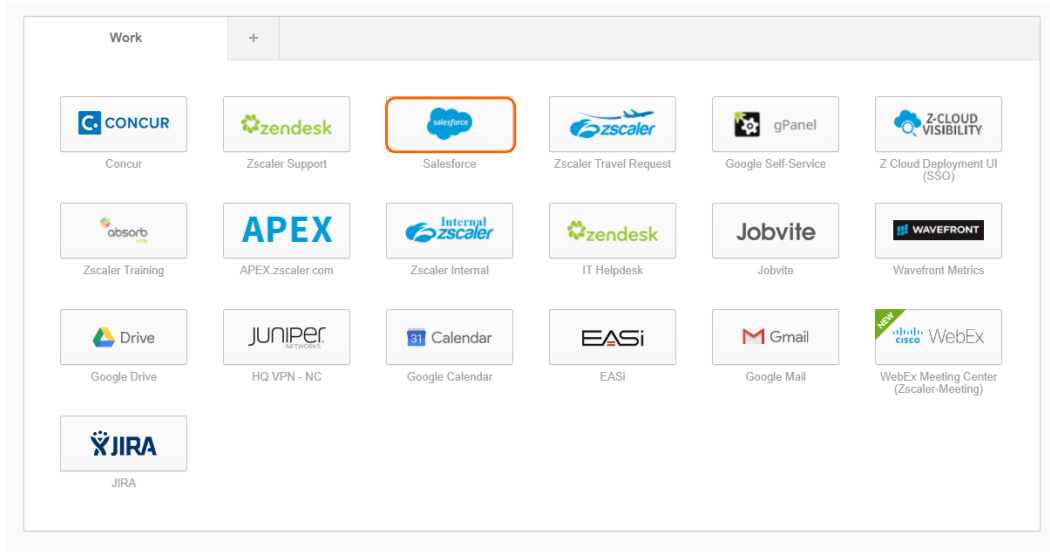
December 2017

Table of Contents

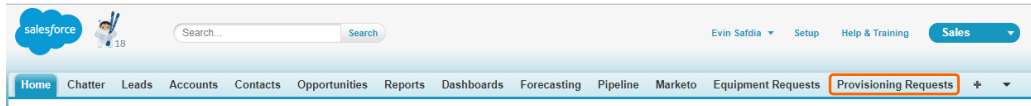
Table of Contents	2
Request Zscaler Provisioning.....	3
Traffic Forwarding	5
GRE Tunnel	5
Tunnel Provisioning	5
Creating a GRE Tunnel on Ubiquiti ER-X.....	6
Creating a Firewall Rule for Sending Traffic to GRE Tunnel on Ubiquiti ER-X	7
Using the Zscaler App.....	8
Authentication	11
Hosted Database	11
Okta.....	13
SAML Configuration for Zscaler.....	13
Active Directory Integration.....	20
Nanolog Streaming Service (NSS).....	27
Deploying a NSS Server – Virtual Appliance on ESXi	27
Creating a NSS Feed – Splunk Enterprise	33
Virtual ZEN (VZEN).....	38
Zscaler Private Access (ZPA).....	39
Appendix I - Hardware	40
Appendix II – Software	41
Appendix III – Additional Guidance.....	42
Installing VMware ESXi 6.5.....	42
Creating a Windows Server 2012R2 Virtual Machine	47
Installing Active Directory Domain Services.....	53
Installing Splunk Enterprise.....	59

Request Zscaler Provisioning

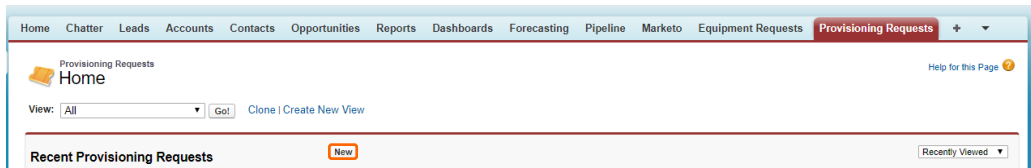
1. Log in to Zscaler Corporate Okta: <https://zscaler.okta.com>
2. Click **Salesforce**:



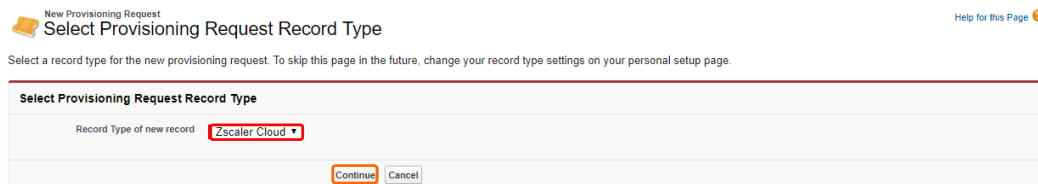
3. Okta will launch Salesforce in a new tab. From the Salesforce interface, click **Provisioning Requests**.



4. On the Provisioning Request page, click **New**.



5. On the Select Provisioning Request Record Type, ensure **Zscaler Cloud** is selected and click **Continue**.



6. In the **Information** section of the provisioning request, fill out the following fields:

Organization Domain	Must be unique, example: Safdia.com
Preferred Cloud	Mandatory, contact SE Leader/Buddy for Insight
Internal User	Please ensure this is checked

Information Required Information

Organization Domain: Safdia.com

Preferred Cloud?: Zscloud.net

Additional Organization domains: [Empty]

Provisioning Type: [Empty]

GEO SE Director Email: [Empty]

Account: Click lookup icon...

Opportunity: [Empty]

Internal User?:

Z-App for existing customer?:

Z-App Deployment Form: [Empty]

Comments for provisioning team: [Empty]

Extension Justification: [Empty]

7. In the **Contact Information** section, fill out these fields:

Send Initial Login Credentials To	Ensure SE is Added to the Chosen Column
SE	Click the Magnifying Glass and Search for Yourself

Contact Information

Send Initial Login Credentials To: Available Customer Partner

Chosen: SE

SE: User

Customer Contact: [Empty]

Partner Contact: [Empty]

Evin Safdia

8. Scroll to the bottom and click **Save**.

System Information

Provisioning Status: --None--

Provisioning Date: [12/11/2017]

Org ID: [Empty]

Record Type: Zscaler Cloud

Users Last Week: [Empty]

Owner: Evin Safdia

Save Save & New Cancel

9. The provisioning request will be created and displayed. Scroll to the **POC Products** section and click **Add/Manage Products**.

POC Products Add/Manage Products POC Products Help

No records to display

10. On the Add/Manage Products Page, add the relevant items and click **Save**. See your buddy / SE Leader if you need more information.

Save Cancel

Products Added			
Action	Product Name	SKU	Category
Delete	ZIA Secure Transformation Bundle	ZIA-TRANS-BUNDLE	User Based
Delete	Zscaler Internet Security Platform	ZSC-SIP	Platform

Products Available			
Action	Product Name	SKU	Category
Add	Device Protection	Z-DEVICE-GB	User Based
Add	ZIA Business Bundle	ZIA-BUS-BUNDLE	User Based
Add	ZIA Professional Bundle	ZIA-PRO-BUNDLE	User Based
Add	Priority Categorization Service	ZSC-PRI-CAT	User Based
Add	Advanced Threat Protection	ZSEC-ATP	User Based
Add	Light Application Access Connection	ZPA-AAC-S1-PRE	Maintenance Fee
Add	ThreatLabZ Threat Insights Service	Z-TLZ-TI-PRE	User Based
Add	Cloud Sandbox	ZSEC-WEB-ABA	Security
Add	Zscaler Web Access Control	ZSEC-WEB-WAC	Security

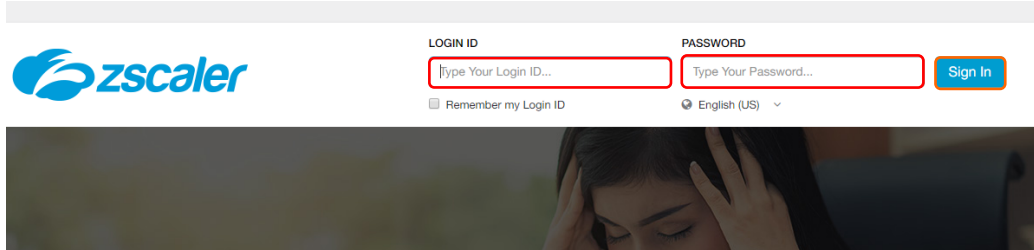
11. Your provisioning request is now complete. You will receive an email with login information, you can check status from the Provisioning Requests tab at any time.

Traffic Forwarding

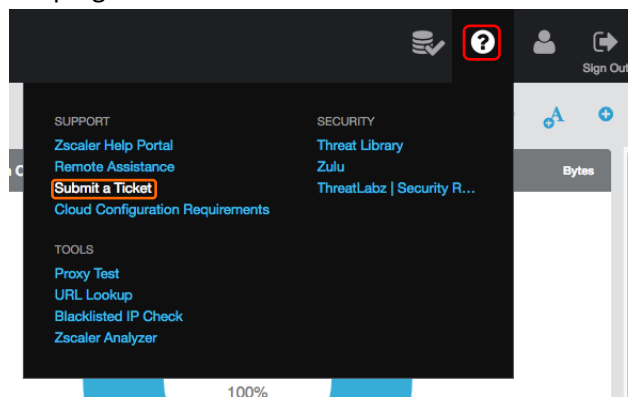
GRE Tunnel

Tunnel Provisioning

1. Log in to the Zscaler Cloud Portal using your admin credentials.



2. Hover over the ? in the top right and then click **Submit a Ticket**.



3. On the Submit a Ticket Page, enter the required information and click **Submit**.

Contact Email	Your email address
Issue Subject	GRE Provisioning
Description	Please include your Public IP Address and Physical Location.
Customer Type	Future Customer – Prospect or POC
Ticket Type	Task
Priority	Low
Area	Provisioning
Provisioning	GRE Tunnel
Contact Name	Your name
Requestor Time Zone	Your time zone

Contact Email*

Issue Subject*

CC List (separate multiple email addresses with a comma)

Description*

Customer Type*

Ticket Type*

Priority*

Area*

Provisioning*

Contact Name*

Organization*

Contact Phone

Requester Time Zone*

Upload a file (often helps troubleshoot issues) No file chosen

4. Your GRE provisioning request is now submitted. You will receive a reply shortly (usually 24-48 hours) from Zscaler Support with the required information.

Creating a GRE Tunnel on Ubiquiti ER-X

1. Use Terminal (OSX) or Putty (Windows) to SSH into your Ubiquiti ER-X
2. Enter the following commands to provision a GRE Tunnel to Zscaler. You can use tab to auto complete.

	Command	Notes
1.	configure	Enables configuration mode
2.	set interfaces tunnel tun0 encapsulation gre	tun0 is the name of the created tunnel
3.	set interfaces tunnel tun0 local-ip x.x.x.x	This is the IP address of switch0 on your ER-X
4.	set interfaces tunnel tun0 remote-ip x.x.x.x	This is the Primary Destination IP provided to you by support.
5.	set interfaces tunnel tun0 address x.x.x.x/24	IP picked at random from RFC6598
6.	commit	
7.	exit	

Alternatively, you can use the Config Tree to create the tunnel. If you load the dashboard, you should see tun0 is connected, but no traffic is being passed:

tun0	tun0	tunnel	100.64.205.1/24	1476	0 bps	0 bps	Connected
------	------	--------	-----------------	------	-------	-------	-----------

Creating a Firewall Rule for Sending Traffic to GRE Tunnel on Ubiquiti ER-X

	Command	Notes
1.	configure	Enables configuration mode
2.	set protocols static table 1 interface-route 0.0.0.0/0 next-hop-interface tun0	
3.	set firewall modify vzen-gre rule 10 action modify	Creates Firewall Rule vzen-gre
4.	set firewall modify vzen-gre rule 10 modify table 1	
5.	set firewall modify vzen-gre rule 10 source address x.x.x.x-x.x.x.x	IP range of traffic you want to send through the GRE tunnel
6.	set interfaces switch switch0 firewall in modify vzen-gre	
7.	commit	
8.	exit	

Now that this rule has been created and committed, you should see traffic flowing through the tunnel (assuming you have an active client on the source IP range you specified).

Open a web browser from a machine in the IP range being sent through the tunnel and navigate to <https://ip.zscaler.com>

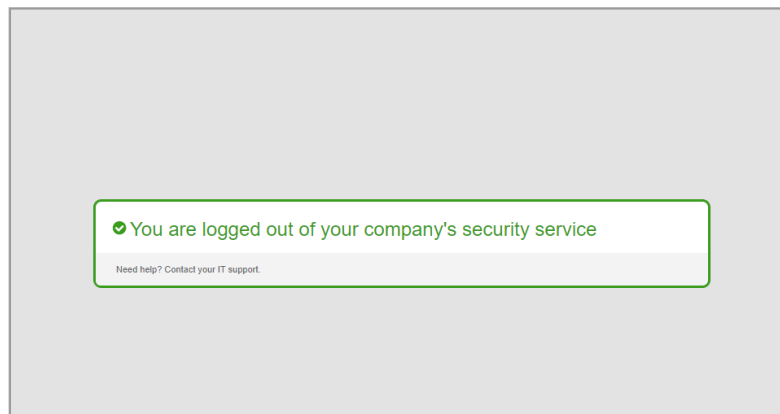
If everything is working properly, you should see a screen like below:

You are accessing this host via a Zscaler proxy hosted at Dallas I in the zsccloud.net cloud.

Your request is arriving at this server from the IP address 165.225.34.129

The Zscaler proxy virtual IP is 165.225.34.36.

The Zscaler hostname for this proxy appears to be zsc-dfw1a1.



Using the Zscaler App

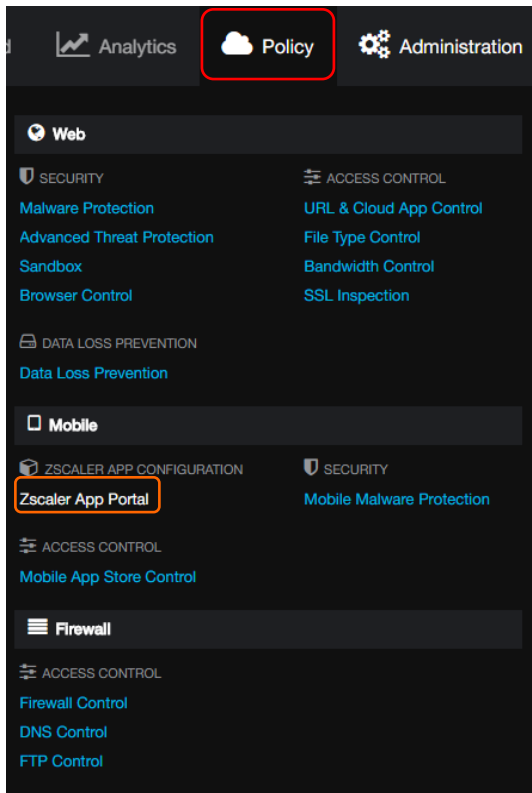
1. Login to your Zscaler cloud portal.



LOGIN ID: PASSWORD:

Remember my Login ID

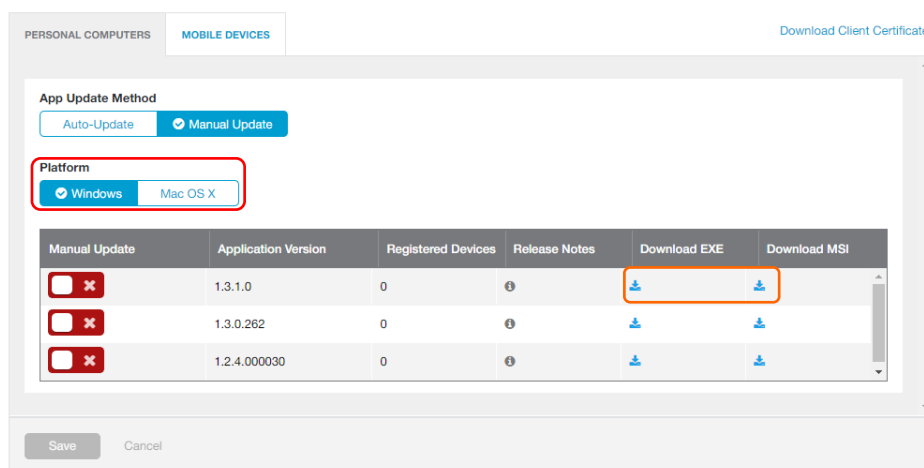
2. Hover over Policy and click **Zscaler App Portal**.



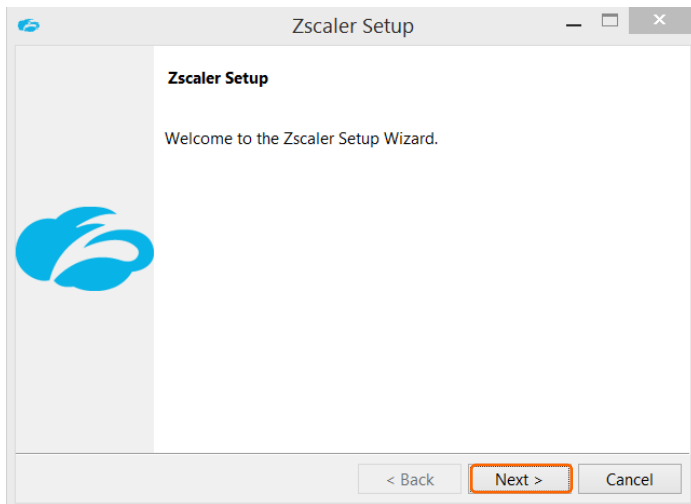
3. From the Zscaler App Portal, click **Administration**.



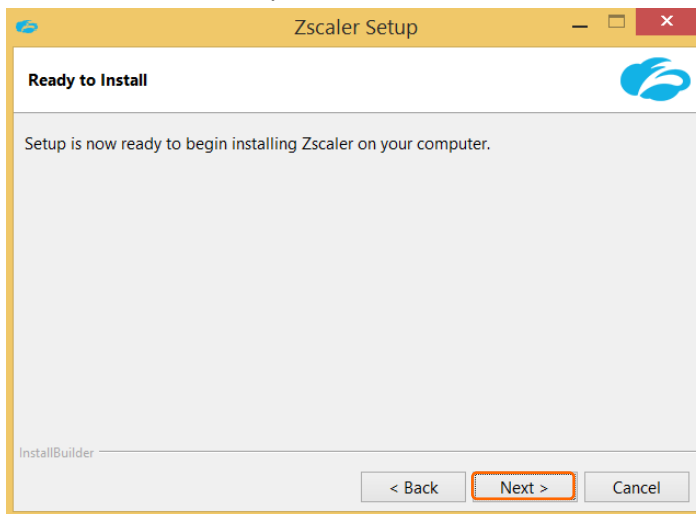
4. Download the latest version of the application for the operating system you want to install it on.



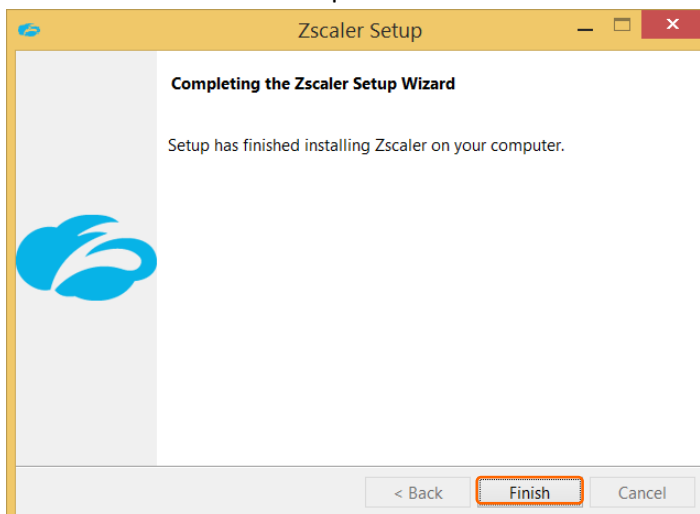
5. Launch the installer on your desired client machine. Click **Next**.



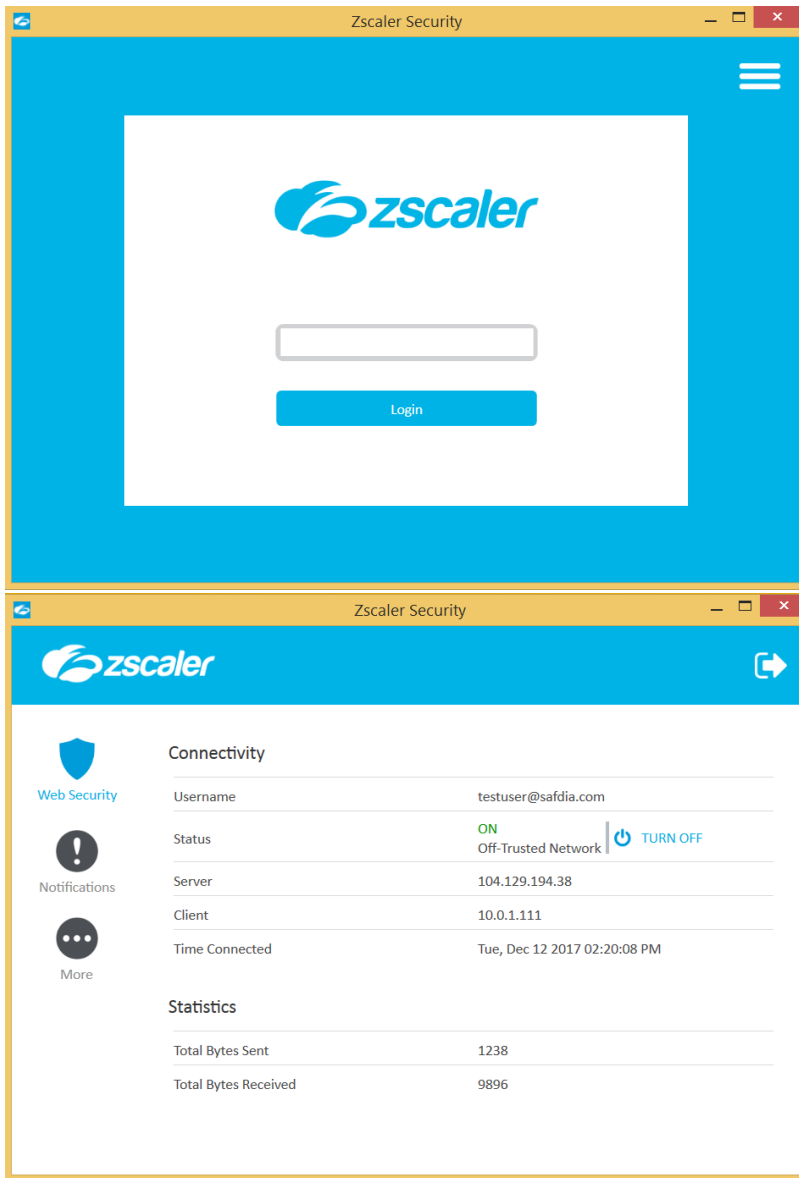
6. Click **Next** on the ready to install screen.



7. Wait for installation to complete and click **Finish**.



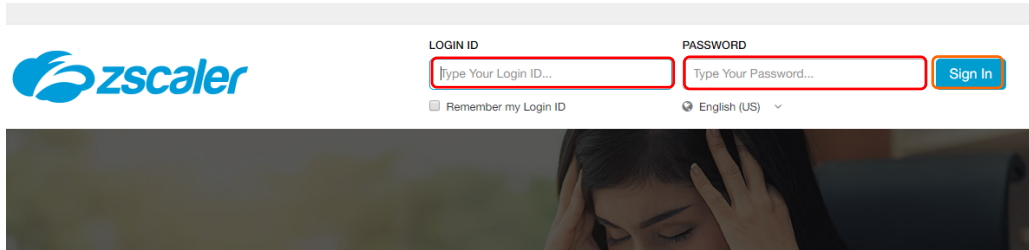
- The Zscaler App launches automatically. Authenticate with a user that you have added to the hosted database or via a configured authentication method to connect and begin sending traffic to Zscaler. See the Authentication section for more information.



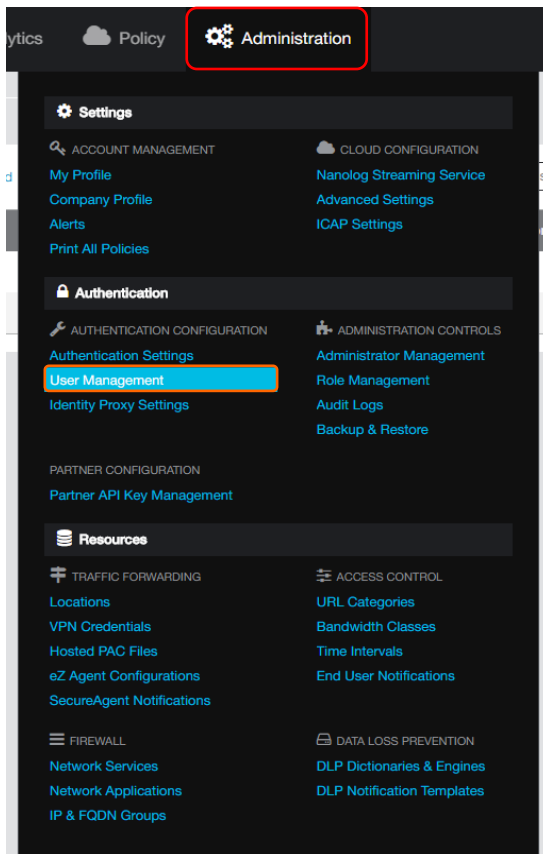
Authentication

Hosted Database

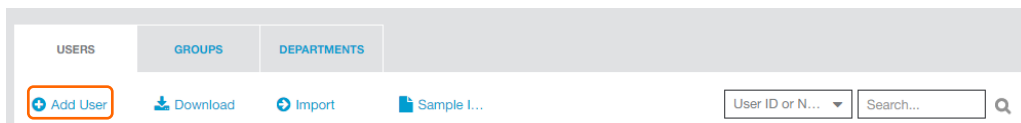
1. Login to the Zscaler Cloud Portal using your admin credentials.



2. Hover over Administration and click **User Management**.



3. Click **Add User**.



4. Enter the following information and click **Save**.

User ID	Desired Username
User Display Name	

Groups	You can create new groups with the +
Department	You can create new departments with the +
Password	
Confirm Password	

Add User

User

User ID: Test @ safdia.com

User Display Name: TEST USER

Groups: Test Users

Department: Test Users

Comments

Password

Password: [masked]

Confirm Password: [masked]

Save Cancel

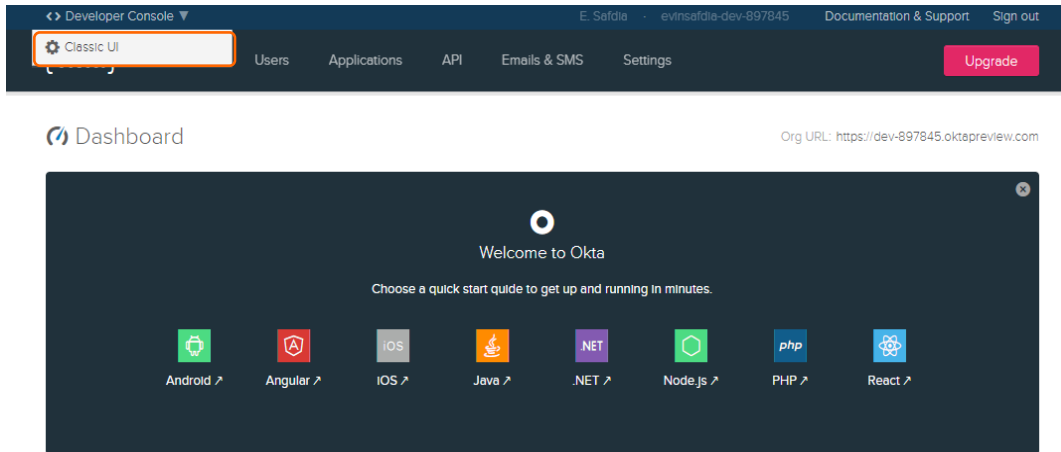
5. You have now created a user that can authenticate to the Zscaler cloud you are provisioned on.

Okta

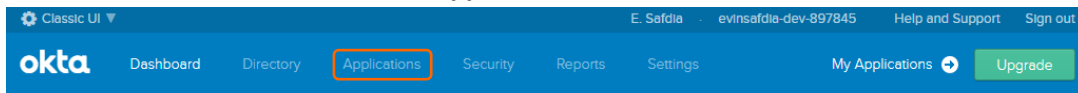
SAML Configuration for Zscaler

Note: An Okta developer account is required, see Appendix II for details. Optionally, an Active Directory Server is used to synchronize users, for help setting one up, see Appendix III.

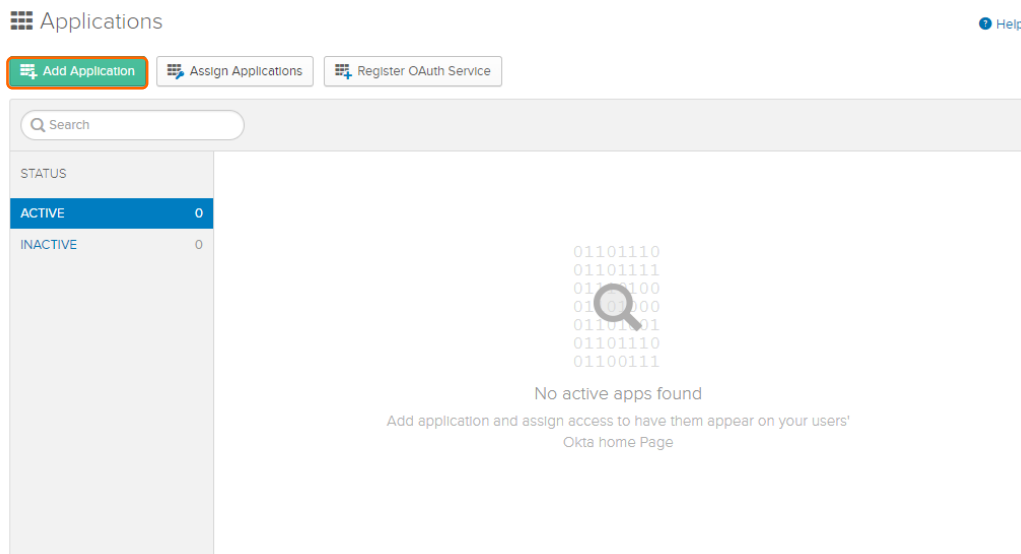
1. Login to your Okta developer instance (<https://dev-#####.admin.oktapreview.com>)
2. From the Dashboard, hover over Developer Console at the top left and click **Classic UI**.



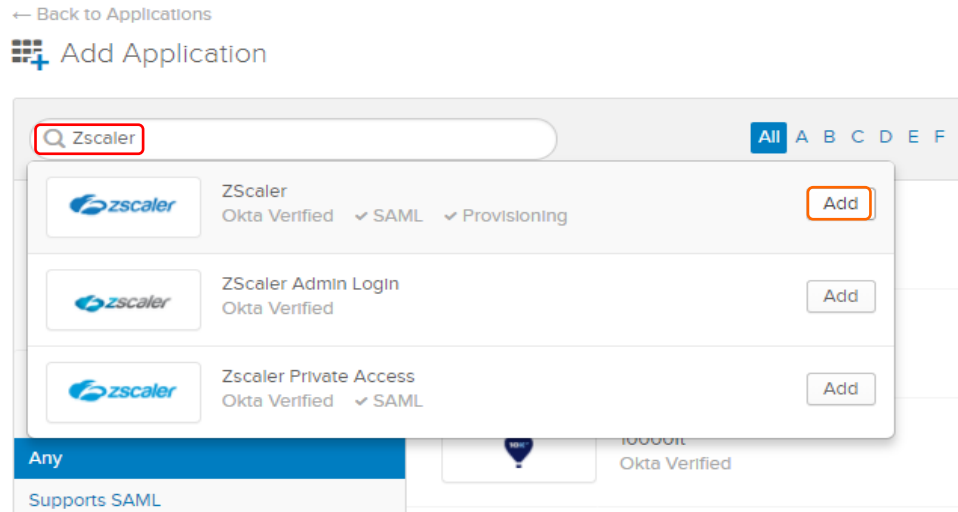
3. From the Classic UI Dashboard click **Applications**.



4. From the applications page click **Add Application**.



- In the search box type in **“Zscaler”** and then click **Add** next to the first Zscaler option.



- Fill in the following fields and click **Next**. Leave other fields at default values.

Your Zscaler Domain	The Zscaler Domain your account is provisioned one (zscloud, zscalertwo, etc.)
User Display Name	Push Okta First & Last name
Department Name	Push AD Department
Group Name	Push Okta Group Name

Application label: ZScaler
This label displays under the app on your home page

Your ZScaler Domain: zscalerbeta.net
Enter your ZScaler URL. For example, if you log into https://admin.zscaler.net/, enter: zscaler.net

User Display Name (optional): Push Okta First & Last name
Select push option to have ZScaler Display Name set to Okta user's first and last name.

Department Name (optional): Push AD Department
Select department attribute value from Okta to map to the SAML Response Attribute statement

Group Name (optional): Push Okta Group Name
When push is enabled, Okta will send the user's first 8 Groups to ZScaler. Use the Group Filter to only send groups that match the configured regular expression.

Group Filter (optional):
Create an expression that will be used to filter groups. If the Okta group name matches the expression, the group name will be included in the SAML Response Attribute statement
 Example:
 zscaler.*
 would include all groups prefixed with the string "zscaler_". Uses regular expression syntax

Application Visibility:
 Do not display application icon to users
 Do not display application icon in the Okta Mobile App

Browser plugin auto-submit:
 Automatically log in when user lands on login page

Cancel Next

7. On the Sign-On options page, select **SAML 2.0** and the click **View Setup Instructions**.

Sign-On Options - Required

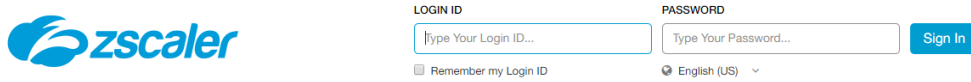
The screenshot shows the 'SIGN ON METHODS' section of the Okta configuration page. The 'SAML 2.0' radio button is selected and highlighted with a red box. Below it, the 'Default Relay State' field is empty. A yellow callout box contains the text 'SAML 2.0 is not configured until you complete the setup instructions.' and a 'View Setup Instructions' button, which is also highlighted with a red box. Below this, the 'CREDENTIALS DETAILS' section shows 'Application username format' set to 'Okta username' and 'Password reveal' disabled. A blue information box states 'Password reveal is disabled, since this app is using SAML with no password.' At the bottom, there are 'Previous', 'Cancel', and 'Done' buttons.

8. The SAML 2.0 instructions will open in a new tab, keep these open for later use. Switch back to the main Okta tab and click **Done**.

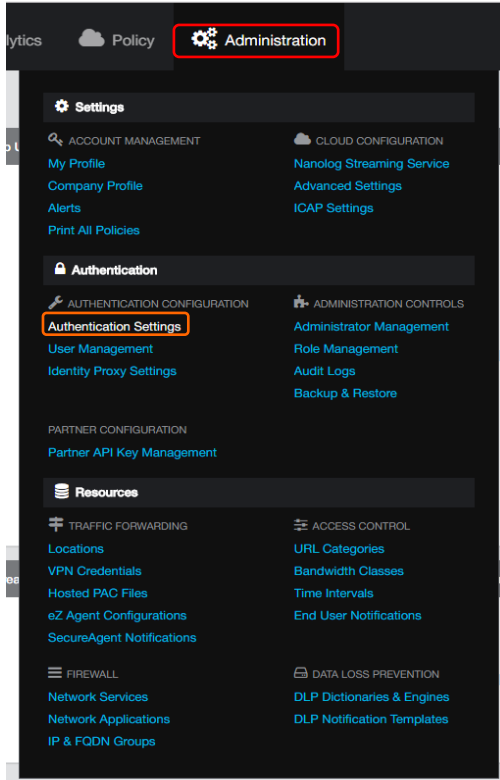
Sign-On Options - Required

This screenshot is identical to the previous one, showing the 'SIGN ON METHODS' and 'CREDENTIALS DETAILS' sections. The 'SAML 2.0' radio button is selected. The 'View Setup Instructions' button is highlighted with a red box. The 'Done' button at the bottom right is also highlighted with a red box.

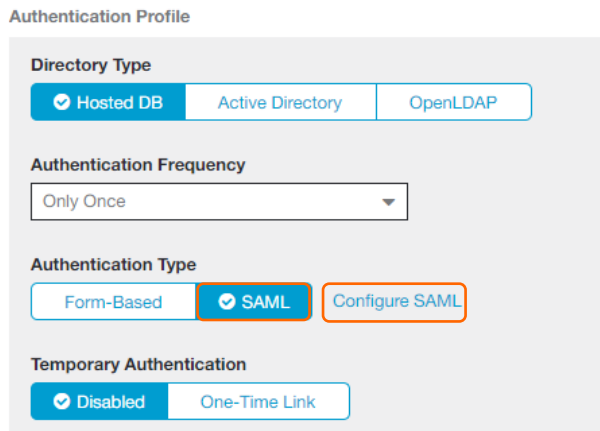
9. Open a new browser tab and navigate to the Cloud portal for your Zscaler instance. (admin.zscloud.net, admin.zscalertwo.net, etc) Sign in with your admin credentials.



10. Hover over **Administration** and click **Authentication Settings**.



11. Under Authentication Profile, click **SAML** and then click **Configure SAML**.



12. Configure the options as pictured below. SAML Portal URL and the Public SSL certificate are available from the Okta instructions tab we opened earlier Set Login Name Attribute to NameID.

When finished, scroll down to configure Auto-Provisioning options

Identity Provider (IDP) Options

SAML Portal URL:

Login Name Attribute:

Public SSL Certificate:

Service Provider (SP) Options

Sign SAML Request:

Signature Algorithm: SHA-1 (160-bit) SHA-2 (256-bit)

Request Signing SSL Certificate:

SP's Public SSL Certificate:

SP's Metadata:

13. **Enable** SAML Auto-Provisioning and enter the following attributes, then click **Save**.

User Display Name Attribute	DisplayName
Group Name Attribute	memberOf
Department Name Attribute	Department

Auto-Provisioning Options

Enable SAML Auto-Provisioning:

User Display Name Attribute:

Group Name Attribute:

Department Name Attribute:

14. Click **Save** at the bottom of the Authentication Settings Page, then click **OK** in the confirmation dialog.

Force Reauthentication for All Users

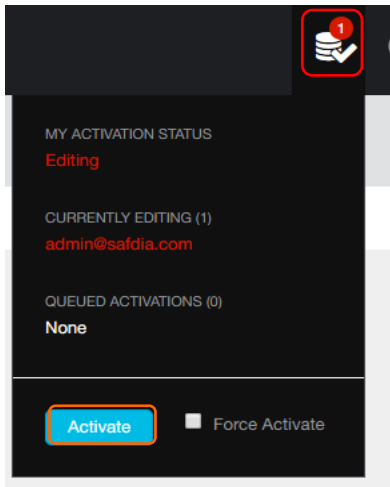
Last Reauthentication: ---

Force Reauthentication:

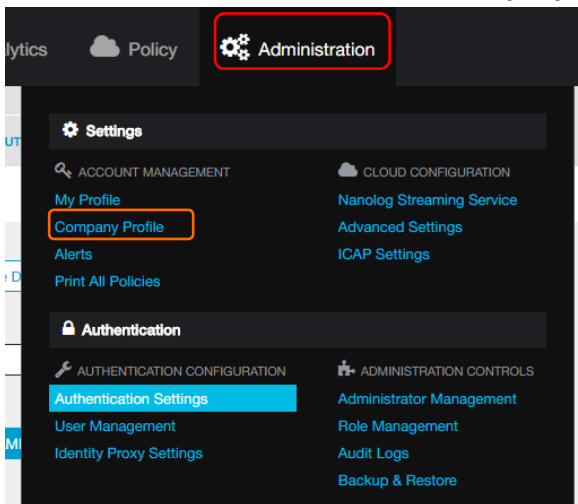
Confirm
✕

If you enable SAML Single Sign-on, all your users will be redirected to the SSO login portal (Identity provider) for authentication. Please confirm the change.

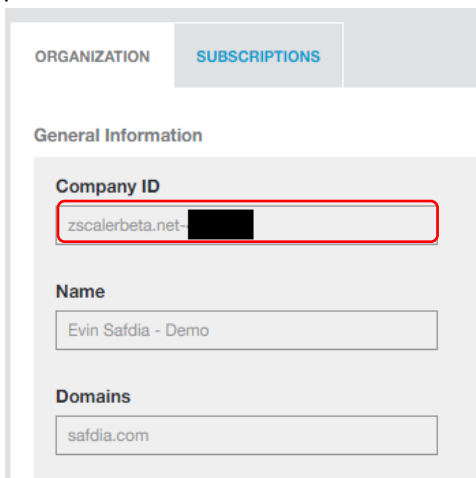
15. Activate your changes by hovering over the activation icon at the top right of the console and click **Activate**.



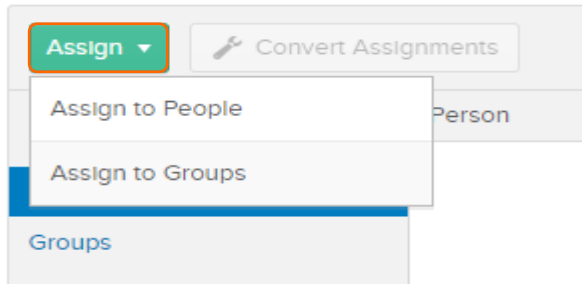
16. Hover over administration and select **Company Profile**.



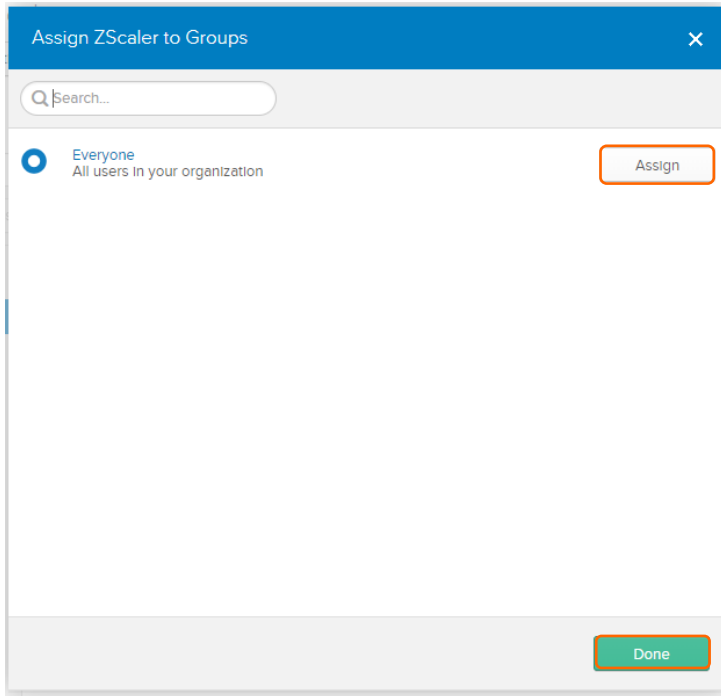
17. Under General Information copy the Company ID, we will need this a few steps later in the Okta portal.



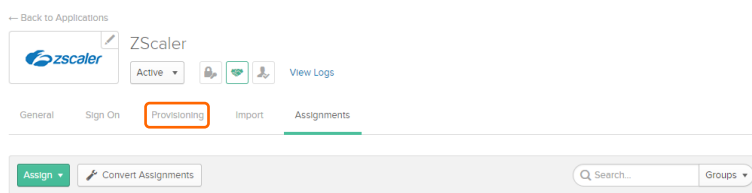
18. Return to the Okta console, you should be on the Assignments page for the Zscaler Application you created. Click **Assign > Assign to Groups**.



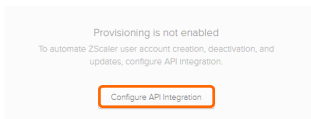
19. Click **Assign** next to the Everyone group and then click **Done**.



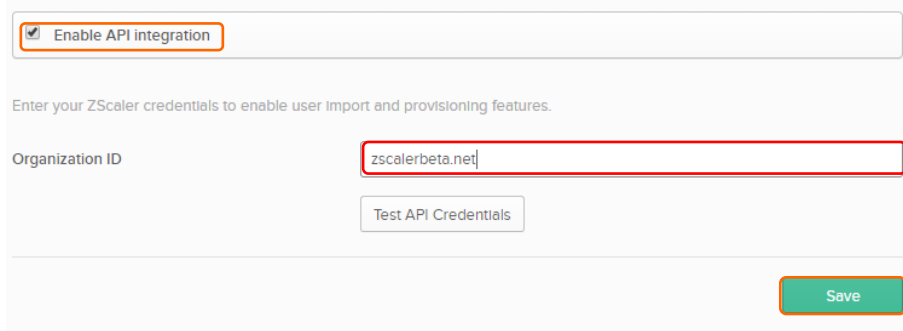
20. Click **Provisioning**.



21. Click **Configure API Integration**.



22. Check the box next to **Enable API integration**, paste the organization ID we copied earlier and then click **Save**.



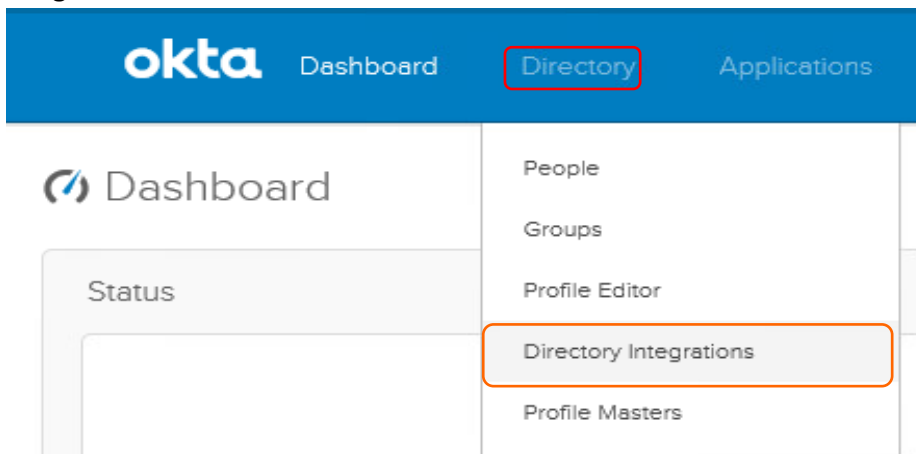
The screenshot shows a configuration form for enabling API integration. At the top, there is a checkbox labeled "Enable API integration" which is checked. Below this, a text input field for "Organization ID" contains the text "zscalerbeta.net". A "Test API Credentials" button is located below the input field. At the bottom right of the form, there is a green "Save" button.

23. You have successfully configured Okta Authentication via SAML 2.0 for Zscaler.

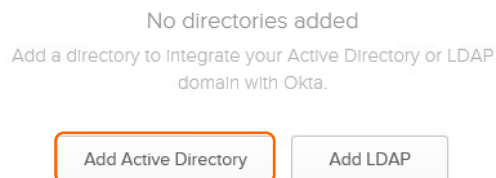
Active Directory Integration

Note: For the sake of simplicity, your Active Directory Domain should match your Zscaler organization domain.

1. From the desktop of your Active Directory VM, login to the Okta portal. (Ensure IE ESC is disabled from Server Manager). Hover over Directory from the top menu and click **Directory Integrations**.



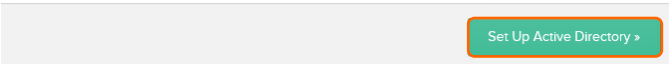
2. Click **Add Active Directory**.



3. Review the installation requirements, scroll down and click **Set Up Active Directory**.

INSTALLATION REQUIREMENTS

- Install on Windows Server 2008 or later
You need access to a Windows server to install the Okta Active Directory agent. You don't need to install the agent on the domain controller itself.
- Must be a member of your Active Directory domain
The agent's host server must be a member of the same Windows domain as your Active Directory users.
- Consider the agent a part of your IT infrastructure
The Windows server where the agent resides must be on at all times. In other words, don't install it on your laptop. The agent host server must have a continuous connection to the Internet so it can communicate with Okta.
- Run this setup wizard from the host server
We recommend running this setup wizard in a web browser on the Windows server where you want to install the agent. Otherwise, you will need to transfer the agent installer to the agent host server, then run the installer.



4. Click **Download Agent**.

A Download the Okta Active Directory agent

The Okta Active Directory agent is a lightweight, secure connector that allows Okta to integrate with your Active Directory domain. The agent enables Okta features such as user import and delegated authentication.

Download Agent

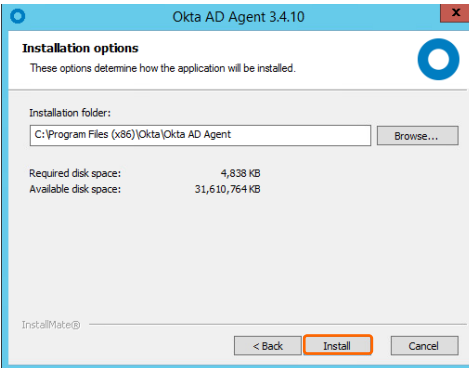
5. On the Internet Explorer download prompt, click **Run**.



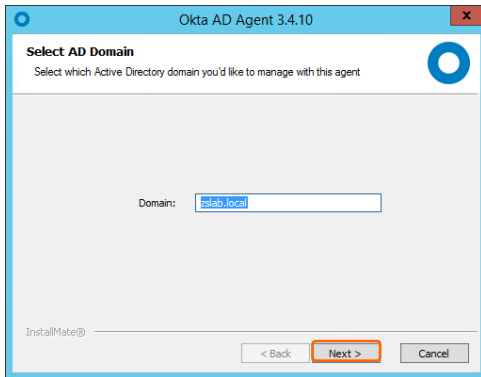
6. The Okta AD Agent will open, click **Next**.



7. Accept the default installation location and click **Install**.



8. Ensure your domain name is listed in the Domain field and click **Next**.



Okta AD Agent 3.4.10

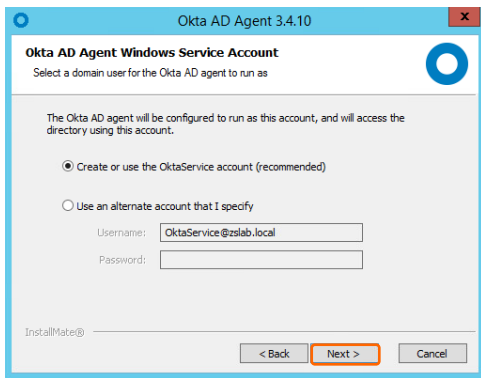
Select AD Domain
Select which Active Directory domain you'd like to manage with this agent

Domain: zslab.local

InstallMate@ _____

< Back Next > Cancel

9. On the Service Account page, either allow the installer to create an account or specify one to use. Click **Next**.



Okta AD Agent 3.4.10

Okta AD Agent Windows Service Account
Select a domain user for the Okta AD agent to run as

The Okta AD agent will be configured to run as this account, and will access the directory using this account.

Create or use the OktaService account (recommended)

Use an alternate account that I specify

Username: OktaService@zslab.local

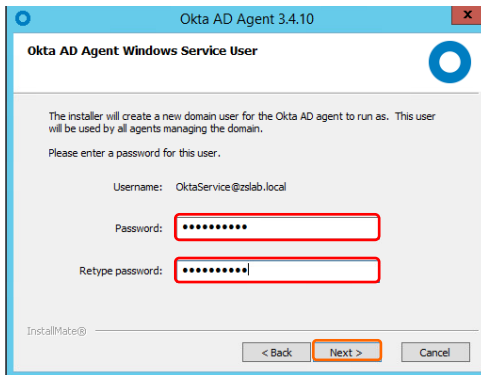
Password: _____

Retype password: _____

InstallMate@ _____

< Back Next > Cancel

10. If you selected to allow the creation of the OktaService account, you will be prompted to specify a password. Enter a password in both fields and click **Next**.



Okta AD Agent 3.4.10

Okta AD Agent Windows Service User

The installer will create a new domain user for the Okta AD agent to run as. This user will be used by all agents managing the domain.

Please enter a password for this user.

Username: OktaService@zslab.local

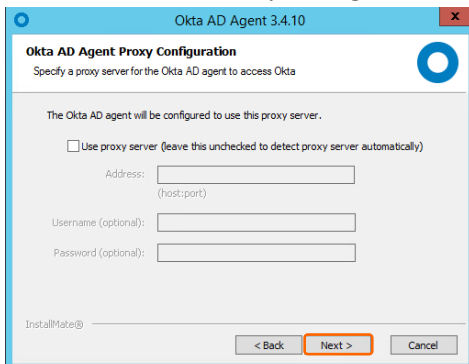
Password: [masked]

Retype password: [masked]

InstallMate@ _____

< Back Next > Cancel

11. Click **Next** on the Proxy Configuration screen.



Okta AD Agent 3.4.10

Okta AD Agent Proxy Configuration
Specify a proxy server for the Okta AD agent to access Okta

The Okta AD agent will be configured to use this proxy server.

Use proxy server (leave this unchecked to detect proxy server automatically)

Address: _____
(host:port)

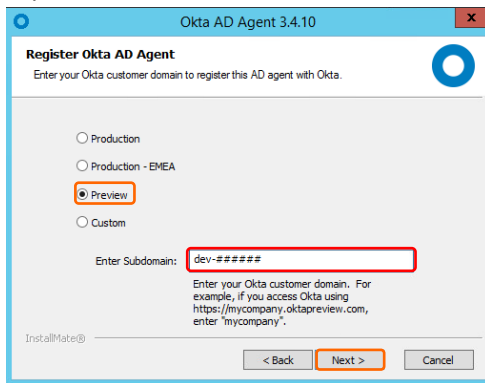
Username (optional): _____

Password (optional): _____

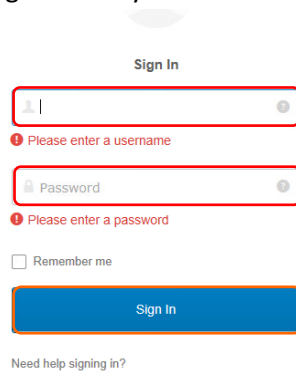
InstallMate@ _____

< Back Next > Cancel

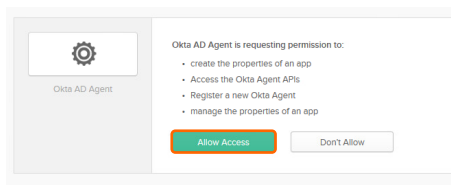
12. Select **Preview** and enter your subdomain name, it should be listed on the Okta page in Internet Explorer. Click **Next**.



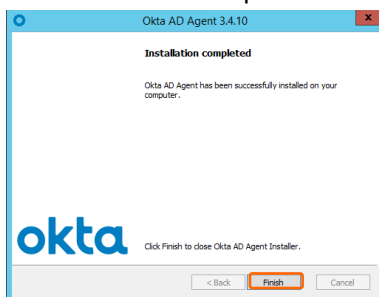
13. Sign In with your Okta Developer admin account.



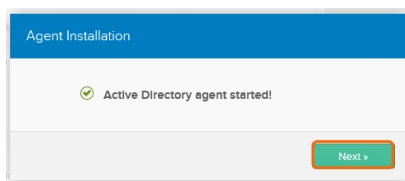
14. Click **Allow Access**.



15. Installation will complete. Click **Finish**.



16. Return to Internet Explorer and the Okta page should show confirmation that the Agent has started. Click **Next**.



17. Select the Organizational Units you would like to sync users and groups from and click **Next**.

Select the Organizational Units (OUs) that you'd like to sync Users from:

- dc=zslab,dc=local
 - computers
 - foreignsecurityprincipals
 - managed service accounts
 - users
 - domain controllers
 - zslab

Show more

Select the Organizational Units (OUs) that you'd like to sync Groups from:

- dc=zslab,dc=local
 - computers
 - foreignsecurityprincipals
 - managed service accounts
 - users
 - domain controllers
 - zslab

Show more

Okta username format:
 Select the username that people imported from AD use to log into Okta.

Activate Windows
Go to System Settings to activate Windows. **Next >**

18. Click **Next** on the configuration confirmation.

Import AD Users and Groups

✔ Active Directory agent configured!

Next >

19. On the attributes page click **Next** to use the default values.

Set Up Active Directory

1 Agent Started 2 Basic Settings Configured 3 Build User Profile 4 Done!

3 Select the attributes to build your Okta User profile

Search... Refresh Attribute List **Next >**

<input type="checkbox"/>	Attribute Name	Type	Description	Imported Attributes
<input checked="" type="checkbox"/>	USNInterSite	integer	USN-InterSite	Base Schema (required)

20. Click **Done**.

4 Agent Setup Complete

Your Active Directory domain is now integrated with Okta.
You can now sync your AD users to Okta and turn on useful authentication features. We recommend installing multiple agents for high availability. Read Next Steps to learn more.

Done

21. Click **Import** at the top.

Back to Directory Integrations

Active Directory zslab.local Active View Logs

People Settings **Import**

Agent Monitors

22. On the Import page, click **Import Now**.

Back to Directory Integrations

Active Directory zslab.local Active View Logs

People Settings **Import**

Agent Monitors

Import Results

Import Now 0 Imported users need review - 0 Imported users confirmed

23. Select **Full Import** and click **Import**.

Import from Active Directory

What type of import would you like to do?

The following actions are performed by both import types:

- New users created in Active Directory will be created in Okta
- Existing users modified in Active Directory will be modified in Okta
- Users disabled in Active Directory will be deactivated in Okta
- Group and OU changes in Active Directory will be reflected in Okta

Incremental import (fastest)

Only imports Active Directory users that were created or updated since your last import. Matching rules are only evaluated on these users. This is the type of import performed by automatic scheduled imports.

Full import (could take a while)

Imports all new and existing Active Directory users. Matching rules are evaluated on all unconfirmed users. This is the type of import that occurs the first time you integrate Okta with Active Directory (Deleted users, and users moved out of the OU, are deactivated in Okta only during Full Imports)

Import Cancel

24. Import will complete and discover your users and groups. Click **OK**.

2 users scanned!

- 0 new users imported
- 0 existing users updated
- 2 existing users unchanged
- 0 users removed

1 groups scanned!

- 0 new groups imported
- 0 existing groups updated
- 1 existing groups unchanged
- 0 groups removed

OK

25. On the Import Results page, select the account you want to import and click **Confirm Assignments**.

Import Results

Import Now 2 imported users need review · 0 imported users confirmed

ALL NO EXACT PARTIAL IGNORED Search Confirm Assignments 2

Show 10 Showing 1 - 2 of 2 First Previous 1 Next Last

Imported User	Okta User Assignment
NO Okta user matches found Test1 User test1@zslab.local	ASSIGN TO → NEW Okta user Test1 User test1@zslab.local test1@zslab.local
NO Okta user matches found Test2 User test2@zslab.local	ASSIGN TO → NEW Okta user Test2 User test2@zslab.local test2@zslab.local

Show 10 Showing 1 - 2 of 2 First Previous 1 Next Last

Confirm Assignments 2

26. On the confirmation dialog, check the box for **Auto-activate users after confirmation** and then click **Confirm**.

Confirm Imported User Assignments

Click Confirm to complete the following assignments:

- 2 new Okta users will be created from Active Directory users
- 0 existing Okta users will be assigned to Active Directory users
- 0 Active Directory users will be ignored

Auto-activate users after confirmation

Confirm Cancel

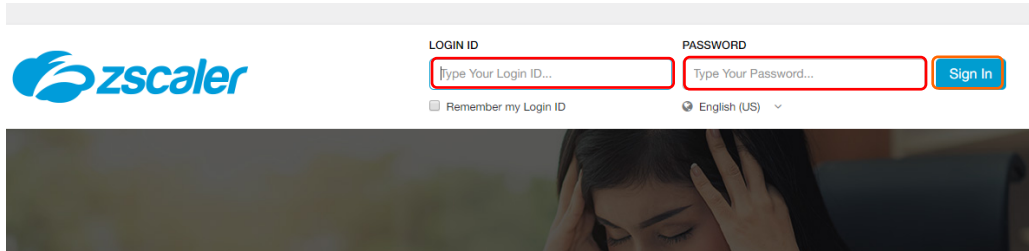
27. Active Directory integration is now complete, you may want to configure scheduled import or periodically import manually.

Nanolog Streaming Service (NSS)

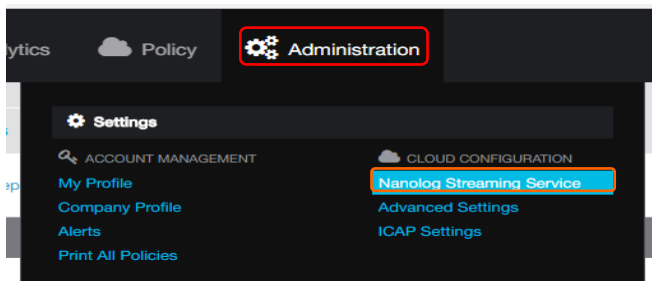
NSS is used to pull log data from the cloud and send it to a customer's SIEM product. Ensure that you have NSS provisioned on your Zscaler instance, if you do not have it in your cloud portal, submit a provisioning request or support ticket to add it.

Deploying a NSS Server – Virtual Appliance on ESXi

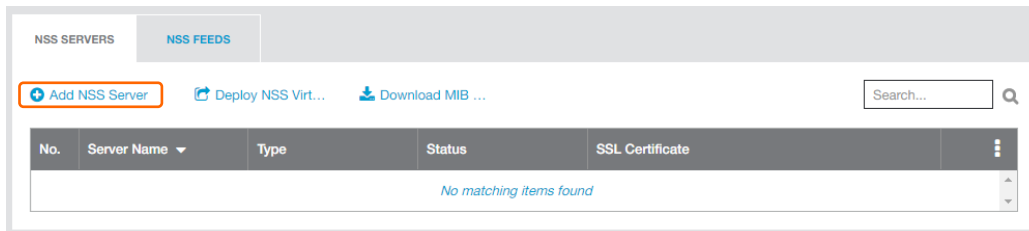
1. Login to the Zscaler Cloud Portal using your Admin credentials.



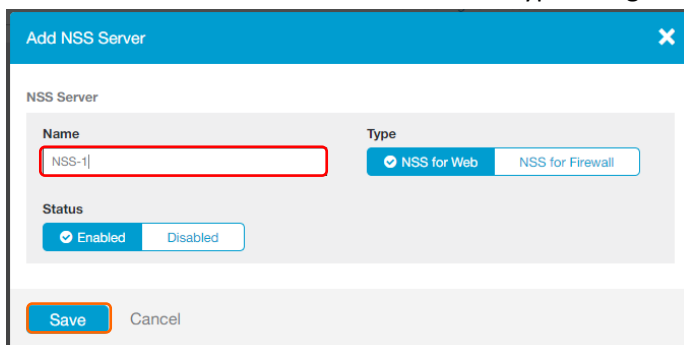
2. Hover over Administration and click **Nanolog Streaming Service**.



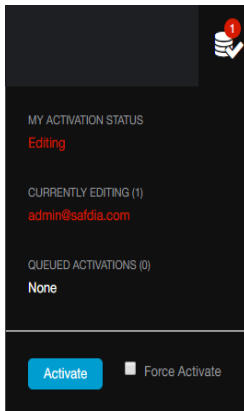
3. From the NSS Page, click **Add NSS Server**.



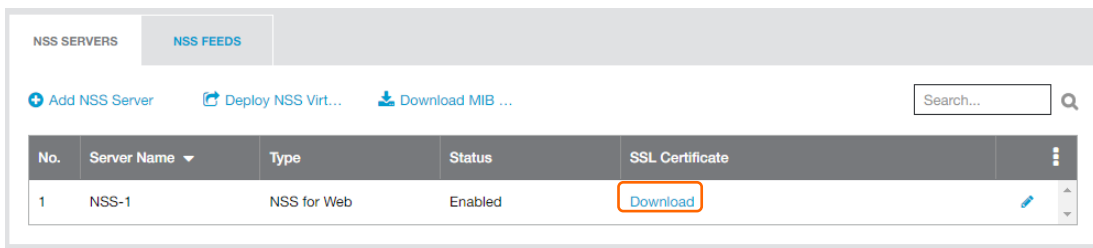
4. Enter a name for the server and select the type of logs it will be used for. Click **Save**.



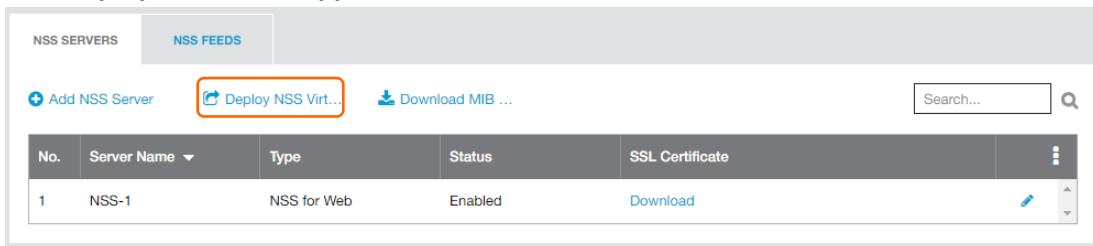
5. Don't forget to activate your changes.



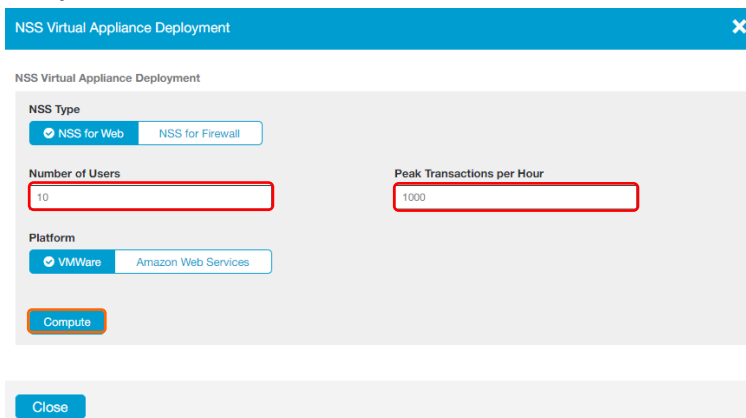
6. Now that the server is added, click **Download** under SSL Certificate. Save this certificate for later, it will be installed on the NSS Virtual Appliance to allow it to authenticate to the Zscaler cloud.



7. Click **Deploy NSS Virtual Appliance**.



8. On the NSS Virtual Appliance Deployment dialog, select NSS type and enter numbers for Users and Peak Transactions per hour. Since this is for a Lab you can use small numbers. Click **Compute**.



9. Click **Download NSS Virtual Appliance**.

Recommended VM Specs

RAM 4 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 0.01 Mbps	NSS Virtual Machine Download NSS Virtual Appliance

10. The NSS appliance will download in OVA format. Click **Close**.

[Close](#)

11. When the Virtual Appliance finishes downloading, login to your ESXi console and click **Create/Register VM** from the top menu.



12. On the Select creation type screen, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

New virtual machine

1 Select creation type

- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select creation type
How would you like to create a Virtual Machine?

Create a new virtual machine

[Deploy a virtual machine from an OVF or OVA file](#)

Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

Back [Next](#) Finish Cancel

13. Enter a name for your NSS Virtual Appliance and select the NSS OVA file that you downloaded. Click **Next**.

New virtual machine - Nanolog Stream Server

1 Select creation type

- 2 **Select OVF and VMDK files**
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select OVF and VMDK files
Select the OVF and VMDK files or OVA for the VM you would like to deploy

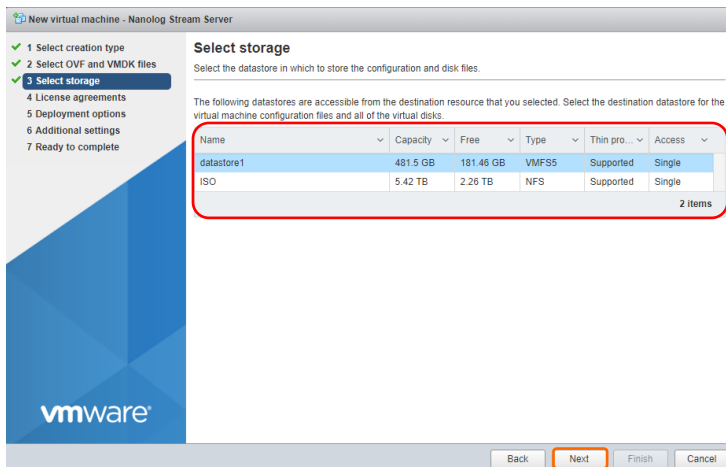
Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

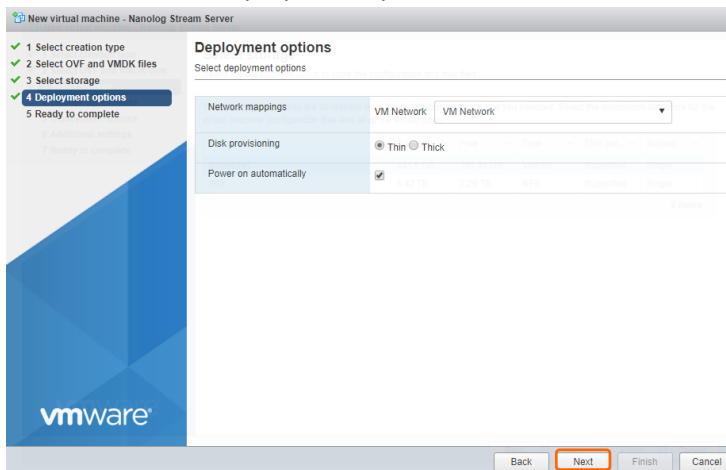
VMDEMO.ova

Back [Next](#) Finish Cancel

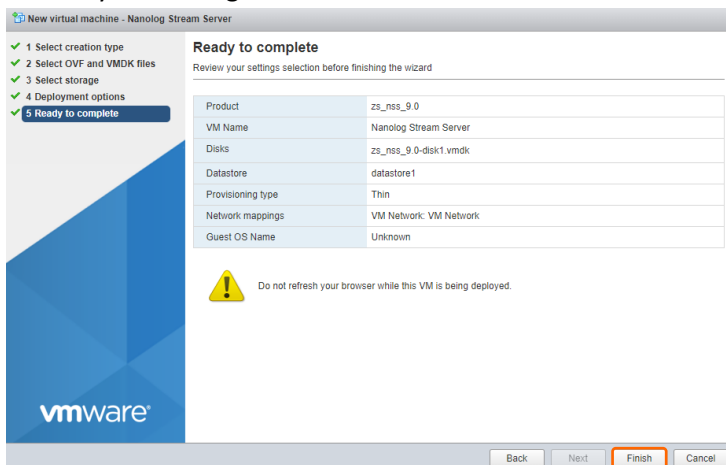
14. Select datastore for the Virtual Appliance and click **Next**.



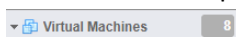
15. Click **Next** on the deployment options screen.



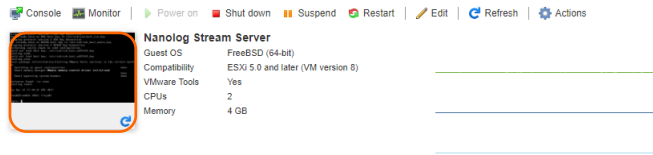
16. Review your settings and click **Finish**.



17. The Virtual Appliance will be imported. Once imported, you can access it from the **Virtual Machines** menu option.



- Open the NSS Virtual Appliance console.



- Login to NSS with the Username: zsroot and the password zsroot. It is recommended that you change the default password with the passwd command.

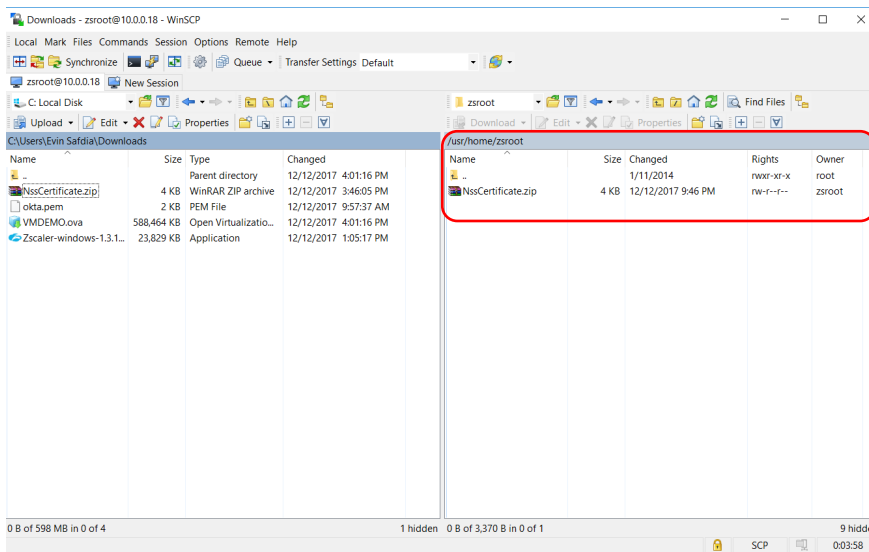
```
FreeBSD/amd64 (NSS) (ttyv0)
login: zsroot
Password:
```

- Type in **sudo nss configure** to configure network settings. You will configure the following settings:

DNS Server IP Address	x.x.x.x
Management Interface IP Address with CIDR netmask	x.x.x.x\16
Default Gateway for Management IP	x.x.x.x
Service IP Address with CIDR netmas	x.x.x.x\16
Default Gateway for Service IP	x.x.x.x

```
nameserver (Resolver IP address) [10.0.0.30]:
Do you wish to add a new nameserver? <n:no y:yes> [n]:
ifconfig_em0 (Management interface IP address with netmask) []: 10.0.0.18/16
defaultrouter (Management interface default gateway IP address) []: 10.0.0.1
snet_dev=em1 (Service interface IP address with netmask) []: 10.0.0.19/16
snet_dflt_gw (Service interface default gateway IP address) []: 10.0.0.1
Successfully applied changes
[zsroot@NSS ~]$_
```

- Using a utility like WinSCP or CyberDuck, upload the NssCertificate.zip file to the management IP of the NSS VM.



- Return to the NSS console and enter the command **sudo nss install-cert**

```
[zsroot@NSS ~]$_ sudo nss install-cert
```

- Assuming you uploaded the certificate bundle to /usr/home/zsroot; enter **/usr/home/zsroot/NssCertificate.zip** and press the **Enter** key. The console should display the

message "Certificates Successfully Installed."

```
[zsroot@NSS ~]# sudo nss install-cert
Password:
Please enter complete path to the certificate bundle(.zip): /usr/home/zsroot/Nss
Certificate.zip
Certificates successfully installed
[zsroot@NSS ~]#
```

24. Check your configuration by running the command **sudo nss dump-config**.

```
[zsroot@NSS ~]# sudo nss dump-config
Configured Values:
  CloudName:zscalerbeta.net
  nameserver:10.0.0.30
  Mgmt IP:10.0.0.18/16
  Default gateway for Mgmt IP:10.0.0.1
  Service IP:10.0.0.19/16
  Default gateway for Service IP:10.0.0.1
[zsroot@NSS ~]#
```

25. Next we will download the NSS binaries. Enter the command **sudo nss update-now** and press the **Enter** key.

```
[zsroot@NSS ~]# sudo nss update-now
Connecting to server...
Downloading latest version
Installing build /sc/smdsc/nss_upgrade.sh
Dec 12 17:35:37 NSS Zscaler: Update [1693] sucessfully disabled upgrade
Dec 12 17:35:37 NSS Zscaler: Update [1693] Sudo is ok!
Dec 12 17:35:37 NSS Zscaler: Update [1693] No migration of sc.conf required
Finished installation!
[zsroot@NSS ~]#
```

26. Finally, run the command **sudo nss start** to start the NSS service. You can enable automatic start on reboot with the command **sudo nss-enable-autostart**.

```
[zsroot@NSS ~]# sudo nss start
Password:
em1: allocated ZSCOMM 0xfffff8000df8000 of 1246976 bytes
em1: started for 1882: err=0, cur=1
NSS service running with pid 1882
[zsroot@NSS ~]#
```

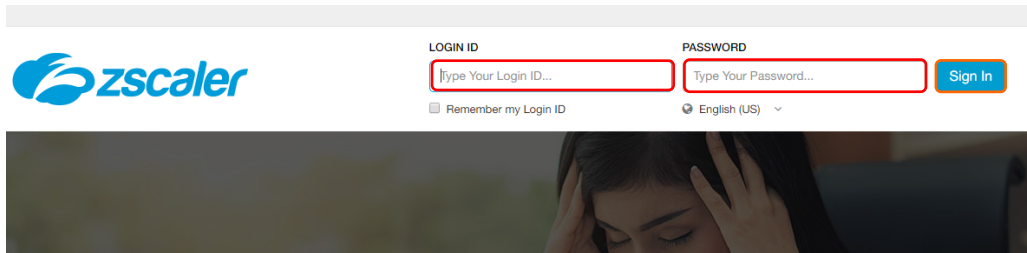
27. Your NSS VM should now be configured and connected to the Zscaler cloud. You can verify your configuration with the command **sudo nss troubleshoot netstat|grep tcp**.

```
[zsroot@NSS ~]# sudo nss troubleshoot netstat|grep tcp
Password:
//+SHARED MEMORY KEY 17 (/sc/)
tcp      0( 0%)    133( 0%) 10.0.0.19.3324      104.129.193.101.9422
ESTABLISHED
[zsroot@NSS ~]#
```

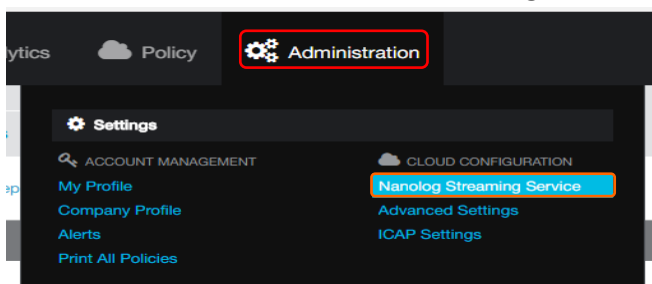
Creating a NSS Feed – Splunk Enterprise

For information on downloading and installing Splunk Enterprise, see Appendix III.

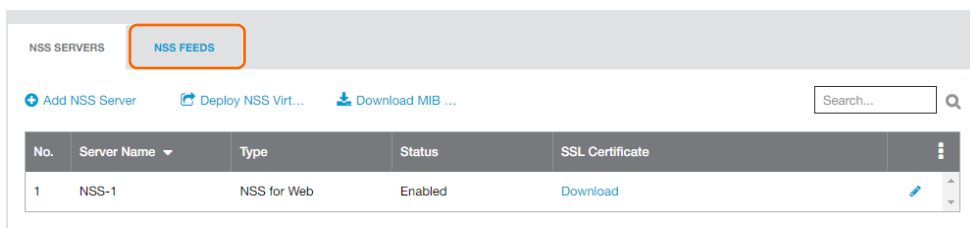
1. Login to the Zscaler Cloud Portal using your Admin credential.



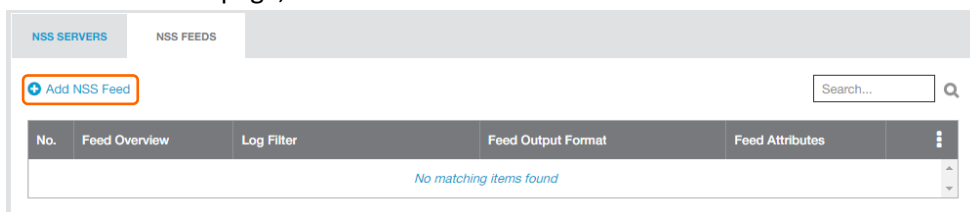
2. Hover over Administration and click **Nanolog Streaming Service**.



3. Click **NSS Feeds**.



4. On the NSS Feeds page, click **Add NSS Feed**.



5. Enter a **Feed Name**, the **SIEM IP Address** and a **SIEM TCP Port**. Select **Splunk CIM** from the Feed Output Type dropdown and your **NSS Server** from the NSS Server dropdown. The SIEM IP address is the local IP address that the NSS Virtual Appliance will use to communicate with the SIEM server, the SIEM TCP port is a port you have selected to use to communicate Zscaler logs to the SIEM, we will configure this in Splunk later. Click **Save**.

NSS Feed

Feed Name
Splunk

NSS Server
NSS-1

SIEM IP Address
10.0.0.17

Log Type
Web Log

Feed Output Type
Splunk CIM

Feed Output Format

```
%d(yy)-%02d(mth)-%02d(dd) %02d(hh):%02d(mm):%02d(ss)\treason=%s(reason)\tevent_id=%d(recordid)\tprotocol=%s(proto)\taction=%s(action)\ttran
sactionsize=%d(totalsize)\tresponsesize=%d(respsize)\trequestsize=%d(reqsize)\turlcategory=%s(urlicat)\tserverip=%s(sip)\tclienttranstime
=%s(ctime)\trequestmethod=%s(reqmethod)\trefererURL=%s(ereferef)\tuseragent=%s(ua)\tproduct=NSS\tlocation=%s(location)\tclientIP=%s(cip)\ts
tatus=%s(respcode)\tuser=%s(login)\turl=%s(eurl)\tvendor=Zscaler\thostname=%s(host)\tclientpublicIP=%s(cintip)\tthreatcategory=%s(malwarec
at)\tthreatname=%s(threatname)\tfiletype=%s(filetype)\tappname=%s(appname)\tpagerisk=%d(riskscore)\tdepartment=%s(dept)\turlsupercat
egory=%s(urlsupercat)\tappclass=%s(appclass)\tdlpengine=%s(dlpeng)\turiclass=%s(uriclass)\tthreatclass=%s(malwareclass)\tdlpdictionaries
=%s(dlpdict)\tfileclass=%s(fileclass)\tbwthrottle=%s(bwthrottle)\tservertranstime=%d(stime)\n
```

NSS Type
NSS for Web

Status
Enabled

SIEM TCP Port
15000

Feed Escape Character

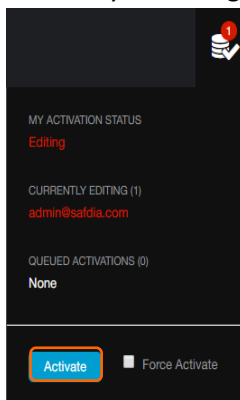
User Obfuscation
Disabled

Timezone
GMT

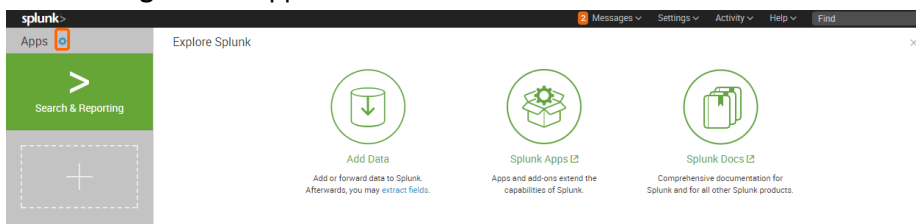
Duplicate Logs
Disabled

Save Cancel

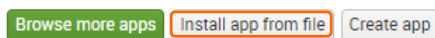
6. Activate your changes.



7. Switch back to the Splunk console, either on the desktop of your VM or in your web browser and click the Cog next to Apps.



8. Click **Install app from file**.



- Click **Choose File** and browse to the Zscaler Splunk app file. For information on downloading, see Appendix II. Click **Upload**.

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

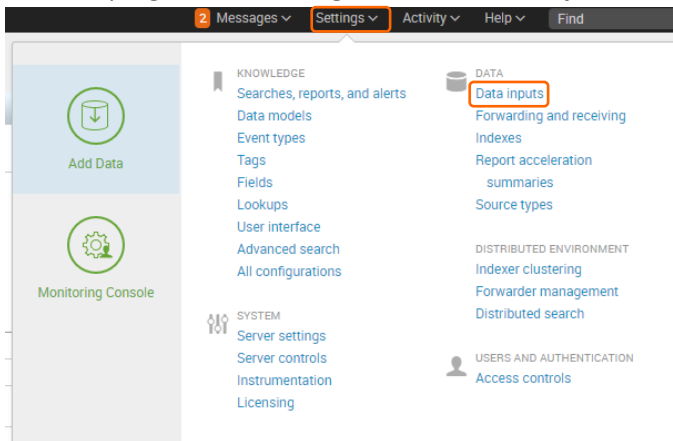
zscaler-app...1308301.tgz

Upgrade app. Checking this will overwrite the app if it already exists.

- The Zscaler App is now installed and will show in the App list.

Name	Folder name	Version	Update checking	Visible	Sharing
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions
Zscaler App for Splunk	ZscalerAppForSplunk	4.1M-201308301	Yes	Yes	App Permissions

- At the top right, click **Settings** and then **Data inputs**.



- Click **Add new** next to TCP under the Local inputs section.

Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	Add new
Files & directories Index a local file or monitor an entire directory.	6	Add new
Local performance monitoring Collect performance data from local machine.	0	Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	Add new

13. Enter the port you used when you created your NSS feed and click **Next**.

Add Data | Select Source | Input Settings | Review | Done | **Next >**

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP UDP

Port?
Example: 514

Source name override?
host:port

Only accept connection from?
example: 10.1.2.3, !badhost.splunk.com, *splunk.com

14. Select **Uncategorized > zscalerweblogs** for Source Type, **Zscaler App For Splunk** for app context and **zscalerlogs_index** for Index. Click **Review**.

Add Data | Select Source | **Input Settings** | Review | Done | **Review >**

Input Settings
Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context
Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More](#)

App Context

Host
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Method?

Index
Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index [Create a new index](#)

15. Review your settings and click **Submit**.

Add Data | Select Source | Input Settings | **Review** | Done | **Submit >**

Review

Input Type	TCP Port
Port Number	15000
Source name override	N/A
Restrict to Host	N/A
Source Type	zscalerweblogs
App Context	ZscalerAppForSplunk
Host	(DNS entry of the remote server)
Index	zscalerlogs_index

16. Your TCP data input has been created successfully. You can click **Start Searching** or return to the home screen and click the Zscaler App to see your data.

✓ TCP input has been created successfully.
 Configure your inputs by going to Settings > Data Inputs

Start Searching Search your data now or see examples and tutorials. [↗](#)

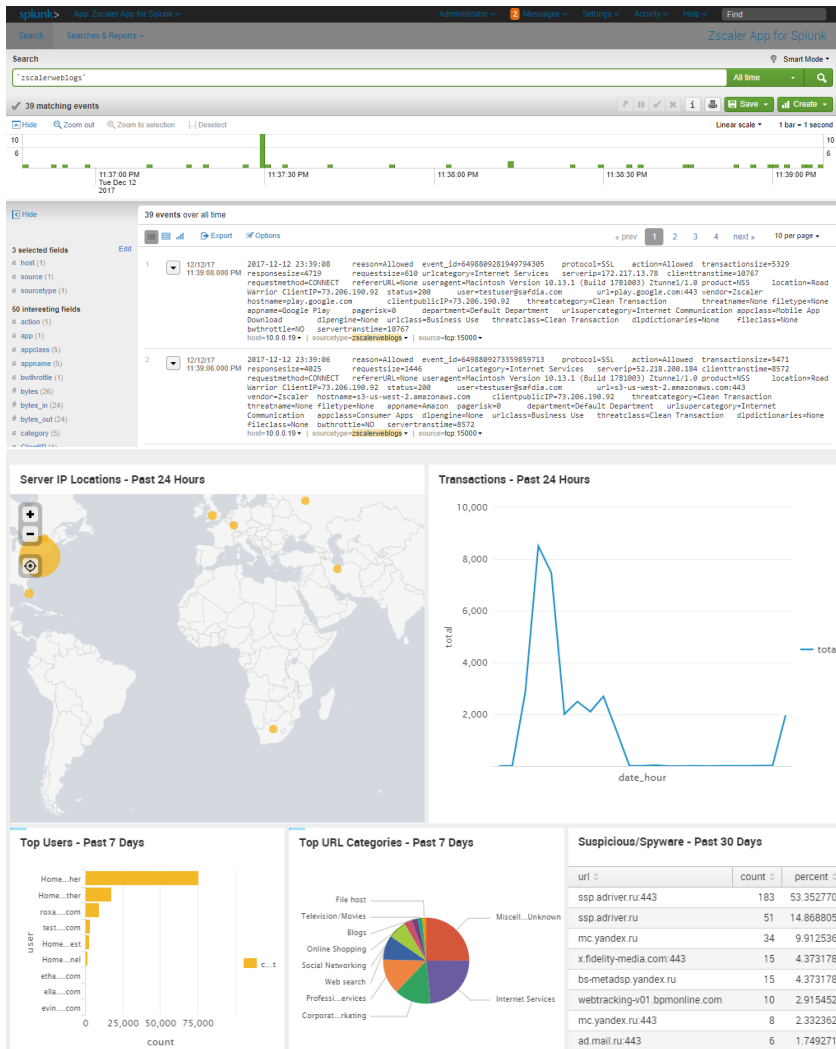
Extract Fields Create search-time field extractions. [Learn more about fields.](#) [↗](#)

Add More Data Add more data inputs now or see examples and tutorials. [↗](#)

Download Apps Apps help you do more with your data. [Learn more.](#) [↗](#)

Build Dashboards Visualize your searches. [Learn more.](#) [↗](#)

17. Assuming you have traffic flowing through Zscaler, you should see events when you search. You can use Splunk to build a dashboard to display this information graphically.



Virtual ZEN (VZEN)

Open a support ticket to request a VZEN for internal user. Be sure to specify if you want Small, Medium or Large.

Zscaler Private Access (ZPA)

Appendix I - Hardware



The Ubiquiti EdgeRouter-X is a cost effective solution for creating GRE/IPSEC tunnels to the Zscaler cloud.

https://www.amazon.com/Ubiquiti-Networks-ER-X-Router/dp/B0144R449W/ref=sr_1_1?ie=UTF8&qid=1513003584&sr=8-1&keywords=ubiquiti+ER_x



In order to leverage features like NSS, ZPA, VZEN, etc, it is ideal to have you own ESXi host server in order to run the necessary virtual machines. While ESXi can be difficult to use on non-approved hardware, HP Z420 is approved and affordable. You can pick up one with 32-64GB of RAM and an eight-core Xeon for around \$400. I added a 1TB SSD to mine to speed things up.

<https://www.ebay.com/sch/i.html?from=R40&trksid=p2380057.m570.l1313.TR12.TRC2.A0.H0.XHP+Z420.TRS0&nkw=HP+Z420&sacat=0>

Appendix II – Software

ESXi

<https://my.vmware.com/en/web/vmware/evalcenter?p=free-esxi6>

Splunk Enterprise

https://www.splunk.com/en_us/download/splunk-enterprise.html

Zscaler App for Splunk (A New Version is in Development)

<https://splunkbase.splunk.com/app/1580/>

Okta Developer

<https://developer.okta.com/signup/>

Rufus

<https://rufus.akeo.ie/>

Putty

<http://www.putty.org/>

WinSCP

<https://winscp.net/eng/download.php>

CyberDuck

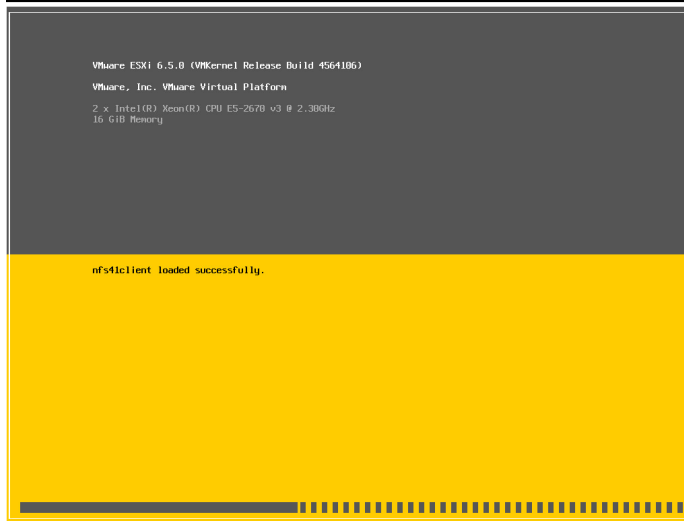
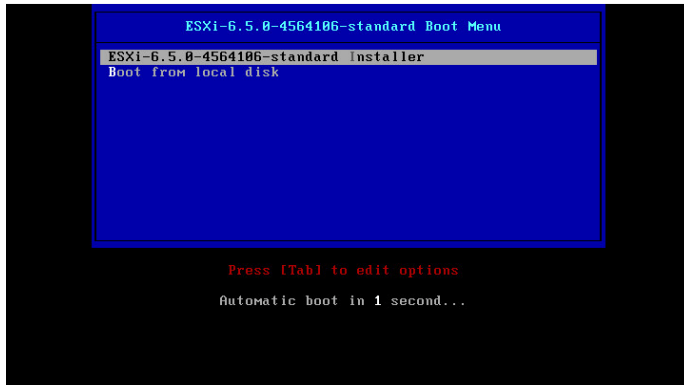
<https://cyberduck.io/?l=en>

Appendix III – Additional Guidance

Installing VMware ESXi 6.5

1. Either burn the ESXi ISO file to a disc or make a bootable USB using Rufus.
2. Boot the USB/Disc on your compatible hardware, see list:

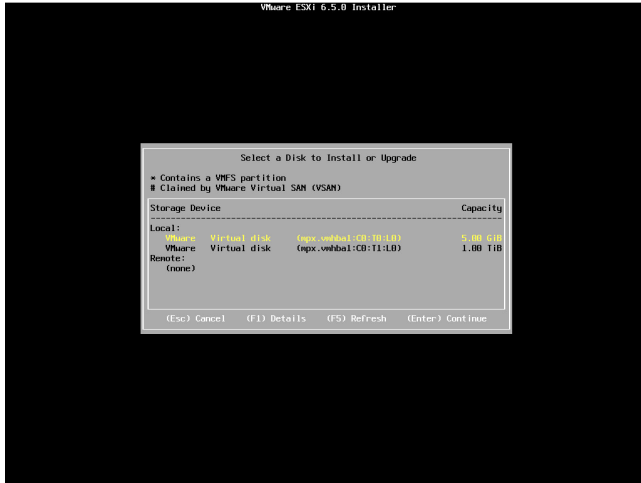
<https://www.vmware.com/resources/compatibility/search.php>



3. The installer will begin with the welcome message:



4. Press the enter key and then select the disk to install to:



5. Choose your language:



6. Set a root password:



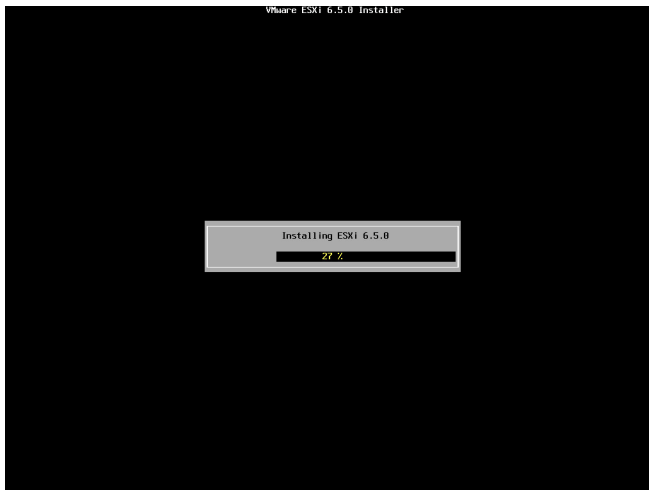
7. Now scanning for components will complete:



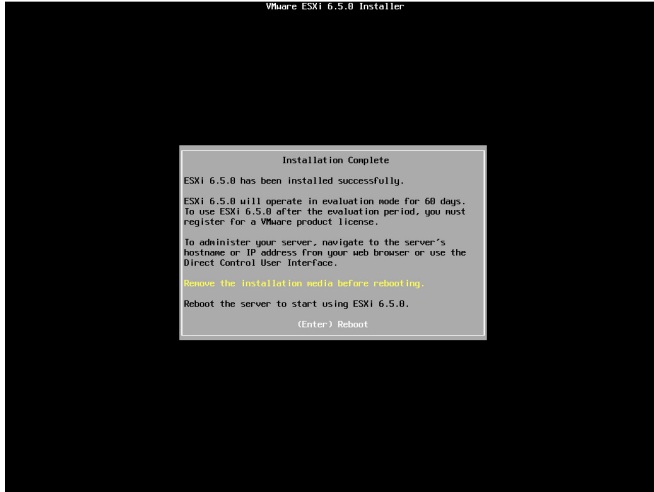
8. Press **F11** to repartition the disk and begin installation:



9. Wait for installation to complete:



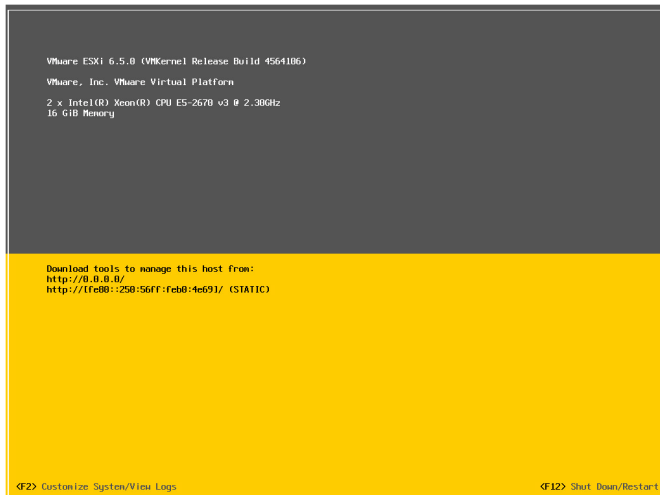
10. Once installation completes, press the **Enter Key** to reboot:



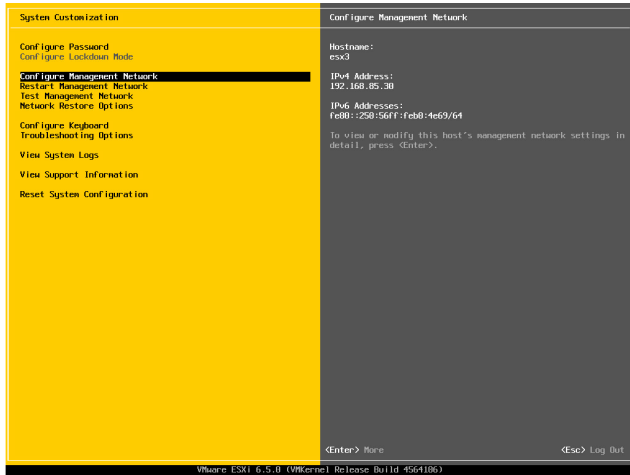
11. The host will reboot:



12. Once the host reboots, the DCUI splash screen will be displayed:



13. Press the **F2** Key to customize system settings:



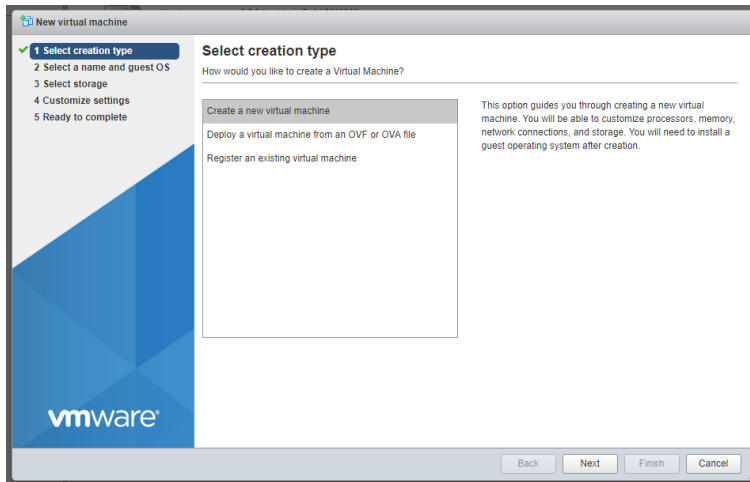
14. Once networking has been configured, you can navigate to the ESXi web console and begin to create Virtual Machines or configure additional settings.

Creating a Windows Server 2012R2 Virtual Machine

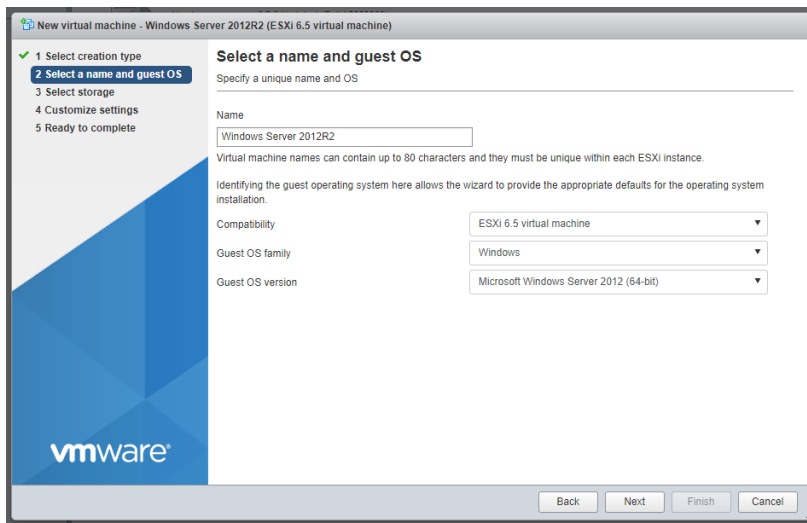
1. From the ESXi Web Console, click **Create / Register VM**:



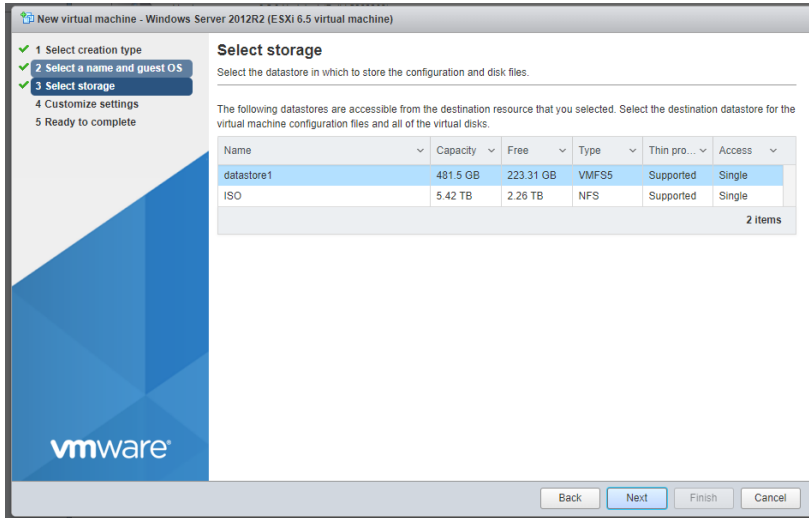
2. On the select creation type screen select **Create a new virtual machine** and click **Next**.



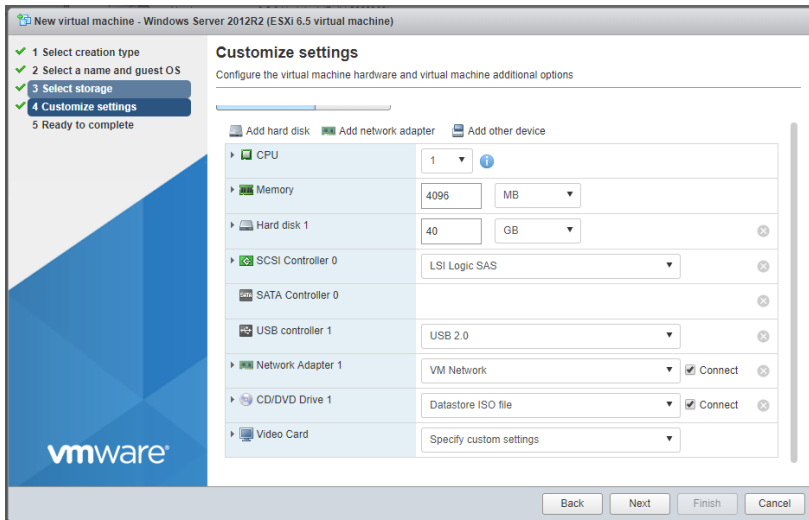
3. Enter a name for your Virtual Machine, select **Windows** and **Microsoft Windows Server 2012** from the appropriate dropdown boxes:



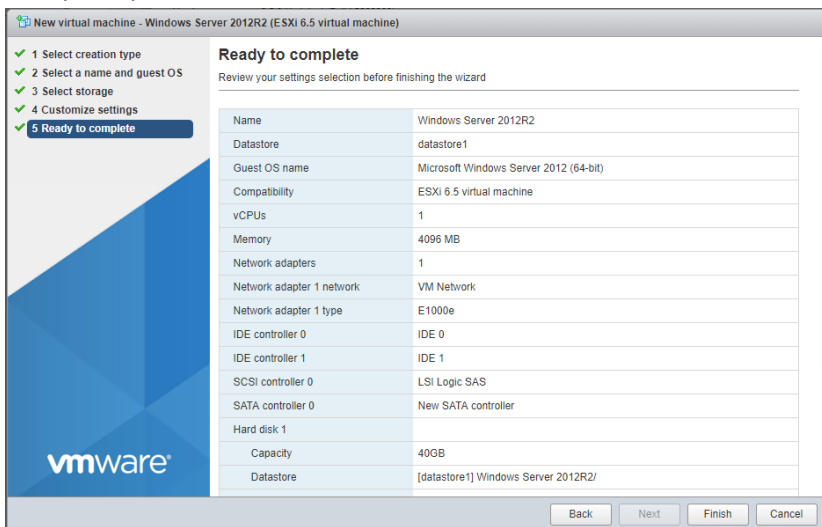
4. Select a storage location from your configured datastores and click **Next**.



5. Customize hardware settings or leave defaults and click **Next**. Please note that CD/DVD Drive can be set to host device if you have a physical 2012R2 installation disk in the host machine's optical drive or you can select an appropriate ISO datastore if you have configured one.



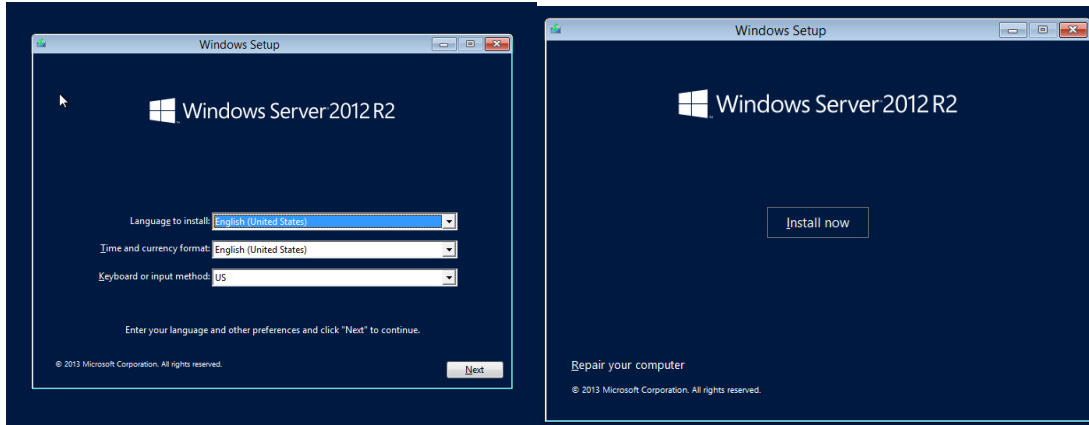
6. Verify all options and click **Finish** to create the VM.



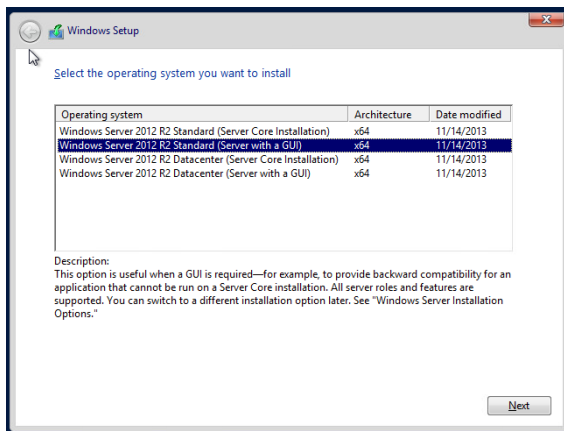
7. The VM will be created, power it on to begin installing Server 2012R2:



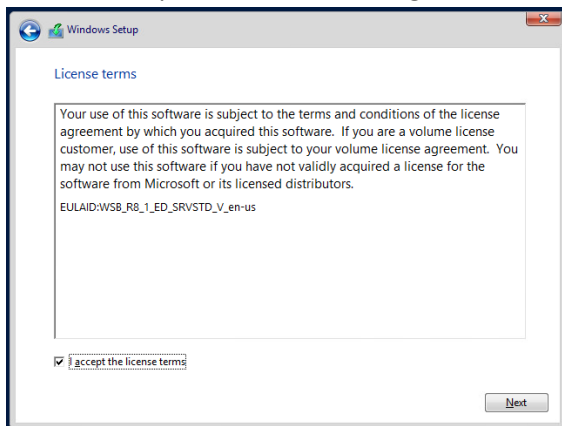
8. On the Setup screen click **Next** and then **Install Now**.



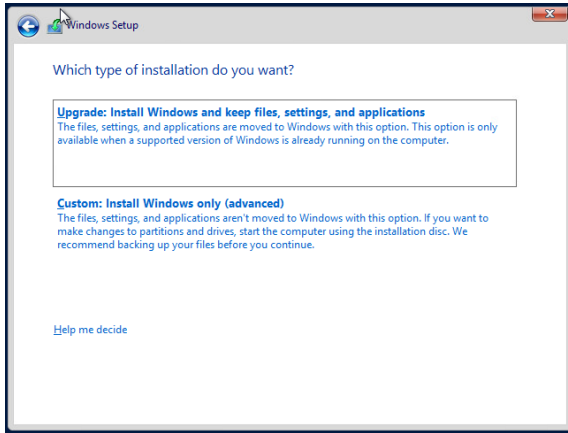
9. Wait for setup to initialize, select **“Windows Server 2012 Standard (Server with GUI)”** and click **Next**.



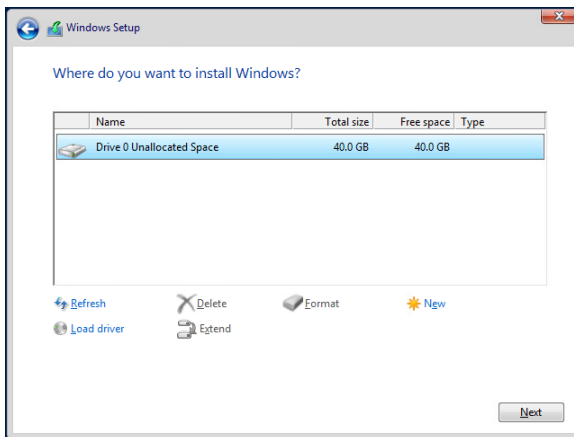
10. Read and respond to the license agreement, then click **Next**.



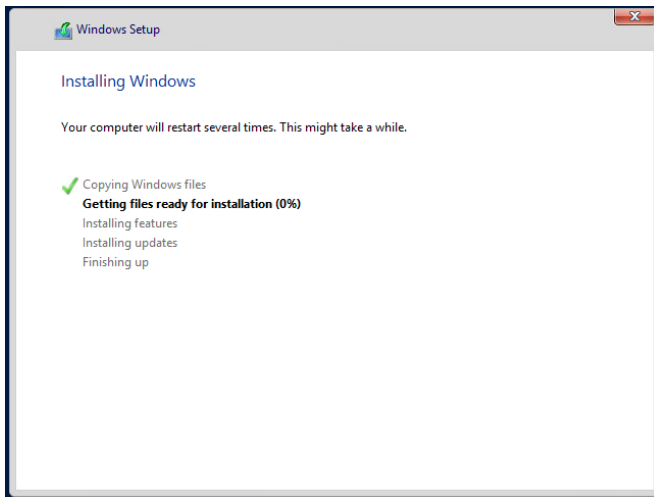
11. Select **“Custom: Install Windows only (advanced)”**



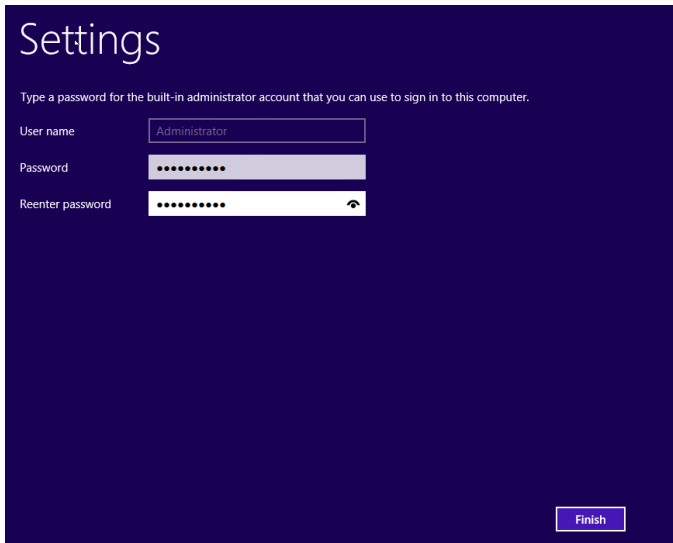
12. Click **Next** on the installation target page:



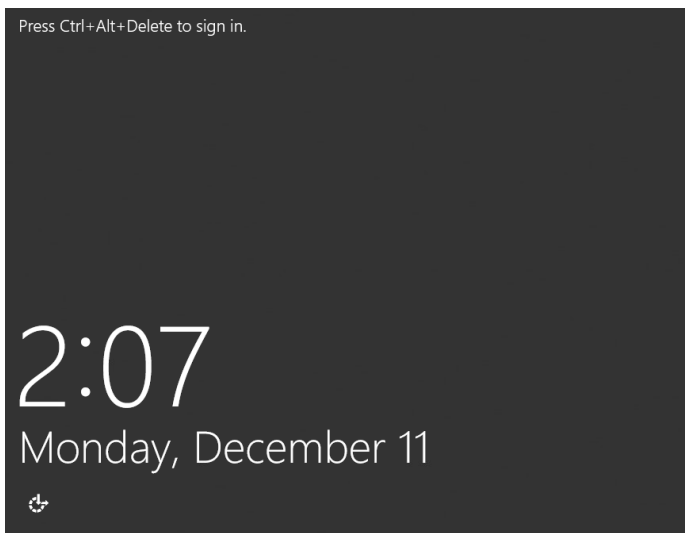
13. Wait for installation to complete:



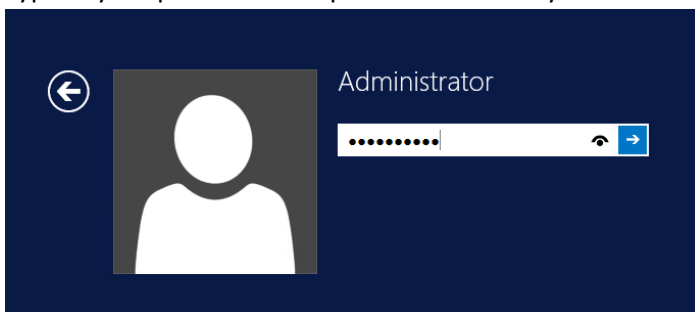
14. When setup is complete, the VM will reboot and prompt you to create a password for the built-in administrator account. Enter a password and click **Finish**.



15. Select actions at the top right of the virtual console and hover over Guest OS > Send Keys and click **Ctrl-Alt-Del**.



16. Type in your password and press the **Enter** key.



17. You have successfully created a Server 2012R2 Virtual Machine. Please name the machine, configure networking and apply a license key before proceeding. Also, don't forget to install the VMware tools from the Actions > Guest OS Menu.

Windows Server 2012R2 Server Manager Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

Role/Server Group	Count
File and Storage Services	1
Local Server	1

File and Storage Services

- Manageability
- Events
- Performance
- BPA results

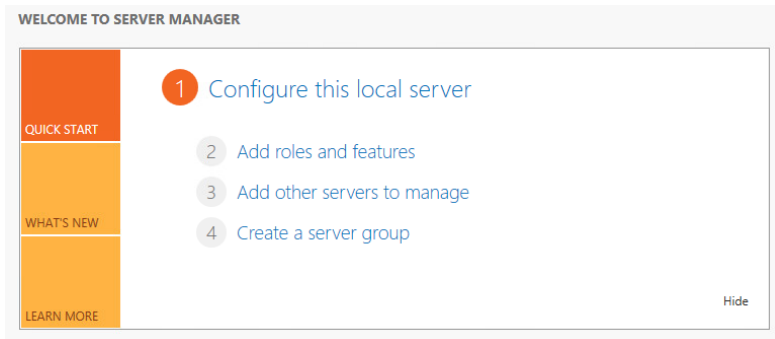
Local Server

- Manageability
- Events
- Services
- Performance
- BPA results

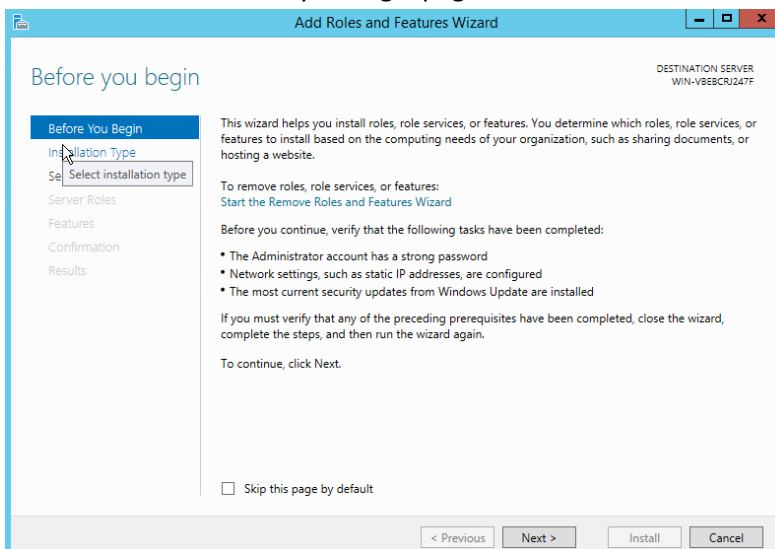
2:14 PM 12/11/2017

Installing Active Directory Domain Services

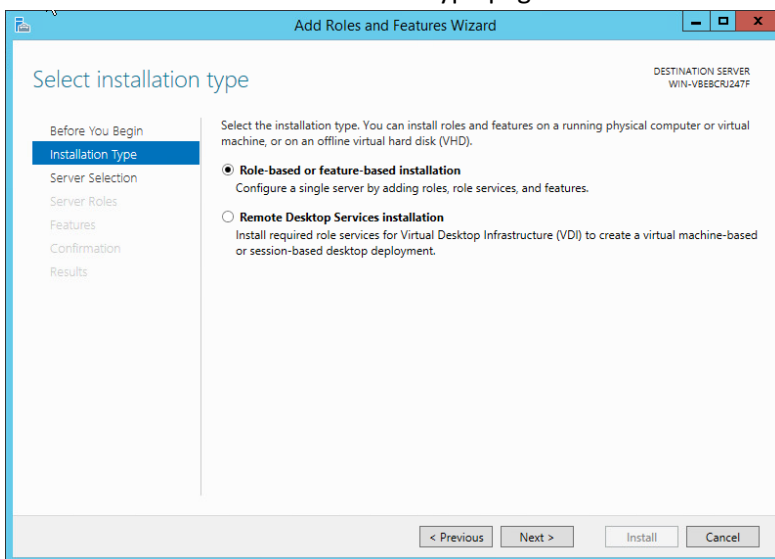
1. Select **Add roles and features** from the server manager dashboard.



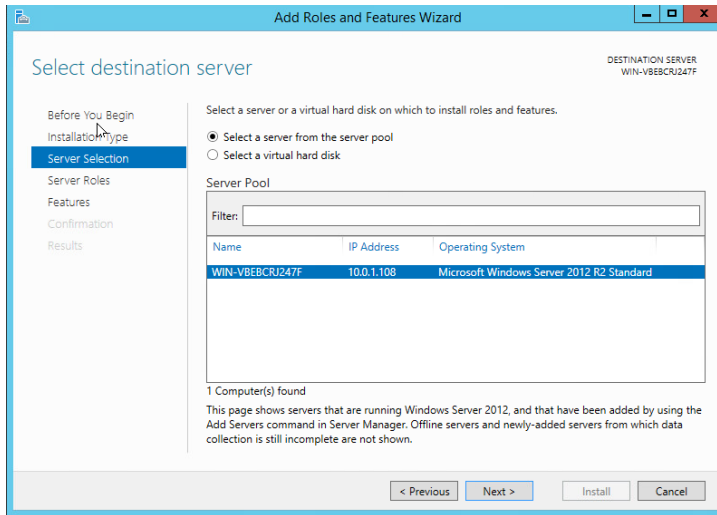
2. Click **Next** on the before you begin page.



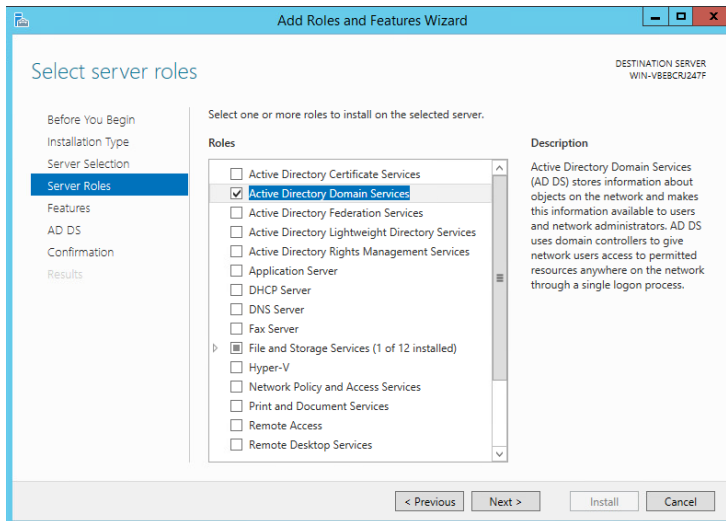
3. Click **Next** on the select installation type page.



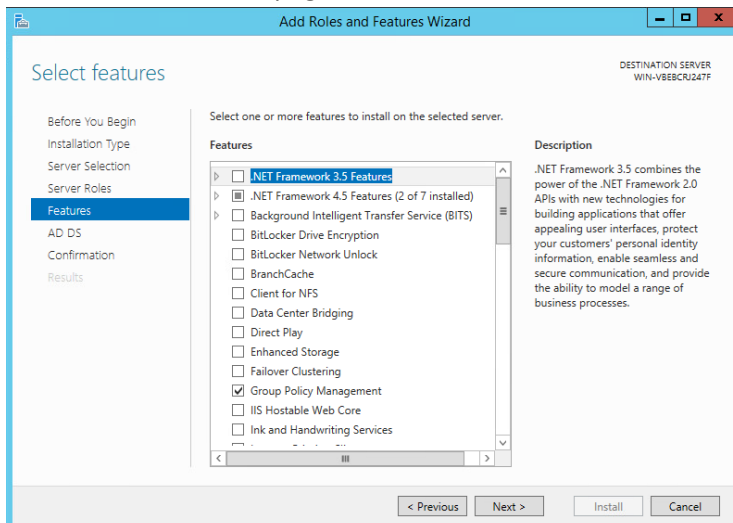
4. Click **Next** on the select destination server page.



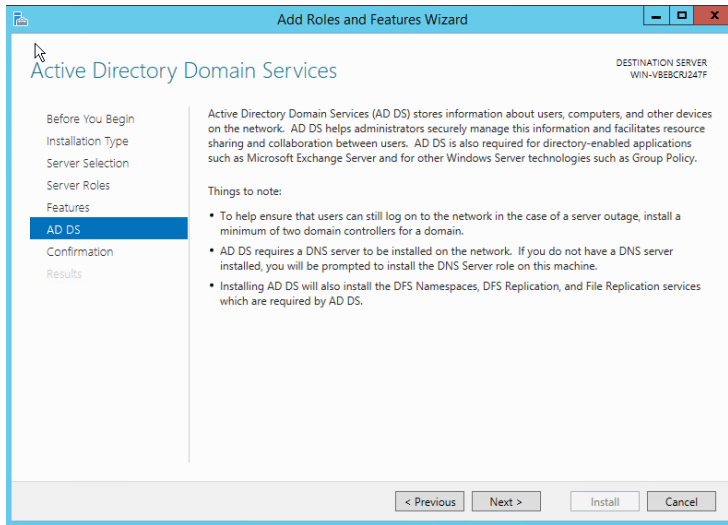
5. On the select server roles page, check the box next to **Active Directory Domain Services**. Click **Next**.



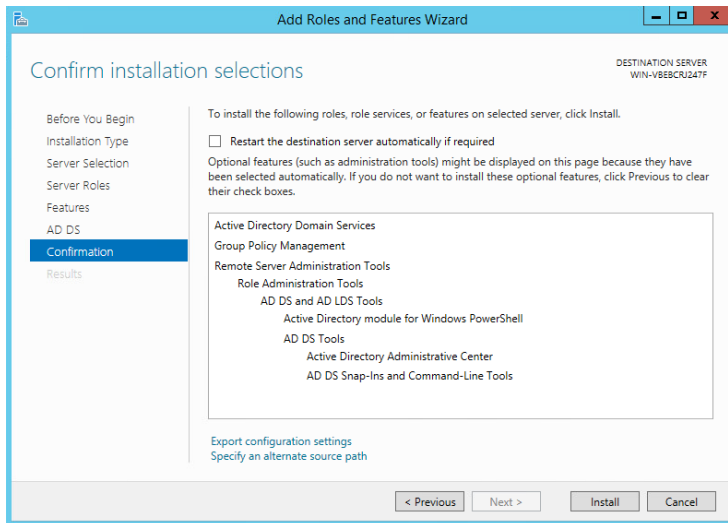
6. On the select features page, click **Next**.



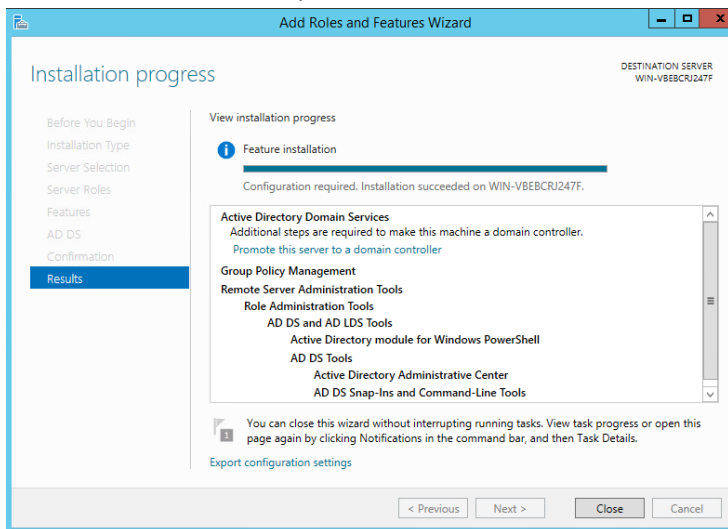
7. Click **Next** on the AD DS Page.



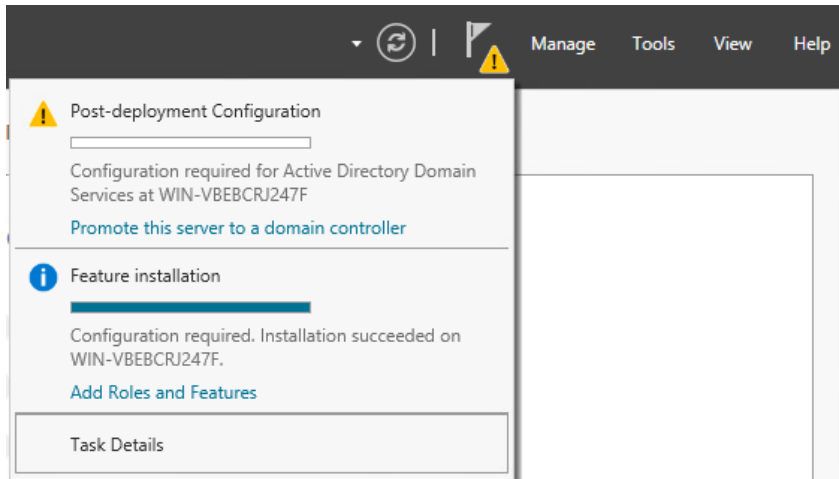
8. Review the confirmation page and click **Install**.



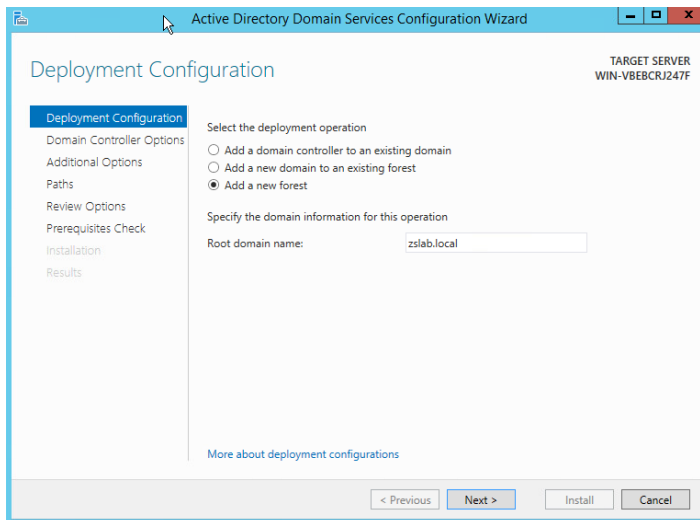
9. When installation is complete, click **Close**.



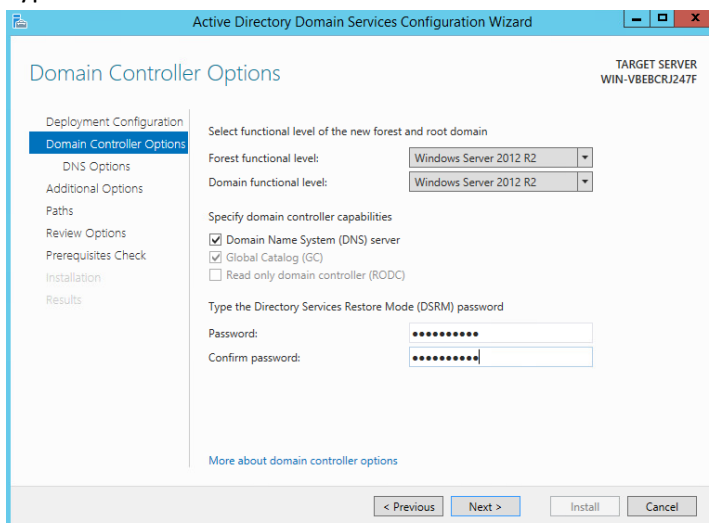
10. In the Server Manager window, click the **Notifications Icon** and the click **Promote this server to a domain controller**.



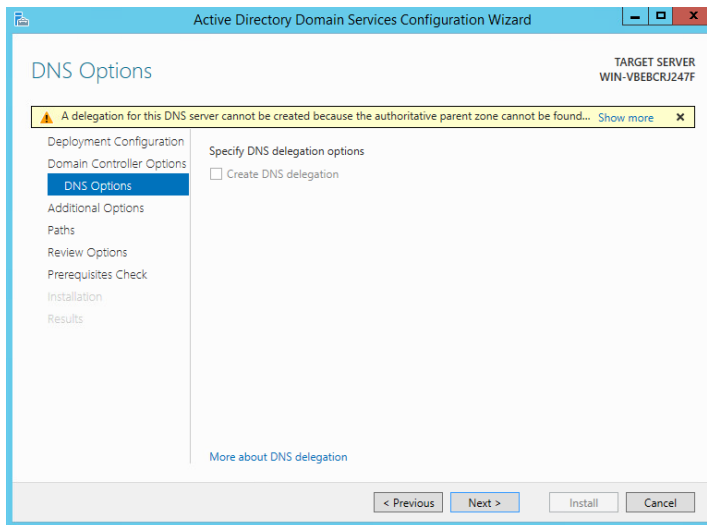
11. On the deployment configuration page, select **Add a new forest** and type in a root domain name and click **Next**.



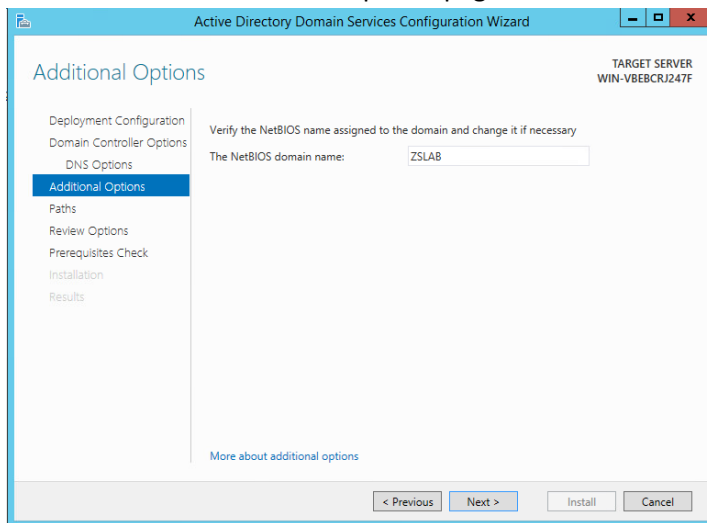
12. Type in a DSRM Password and click **Next**.



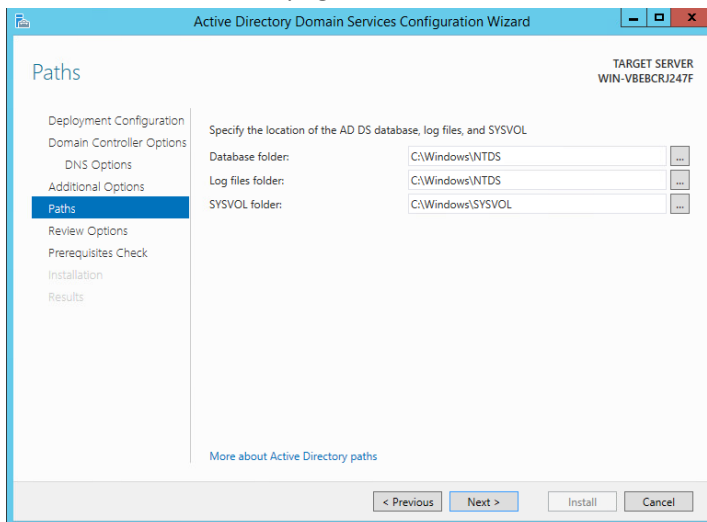
13. Click **Next** on the DNS Options page.



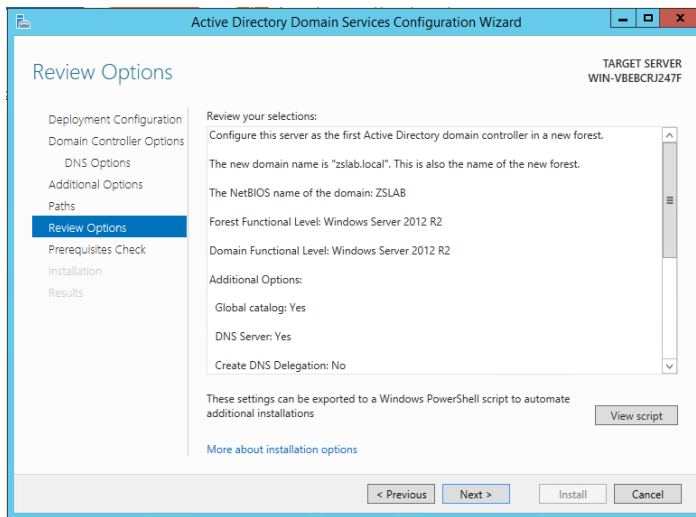
14. Click **Next** on the Additional Options page.



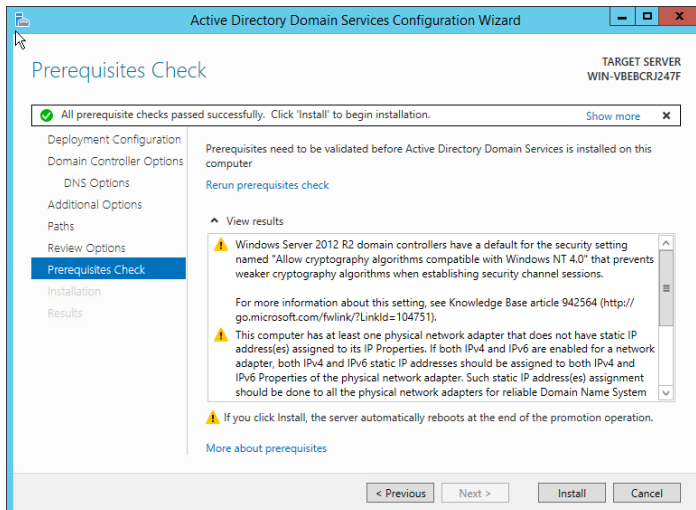
15. Click **Next** on the Paths page.



16. Review your selections and click **Next**.

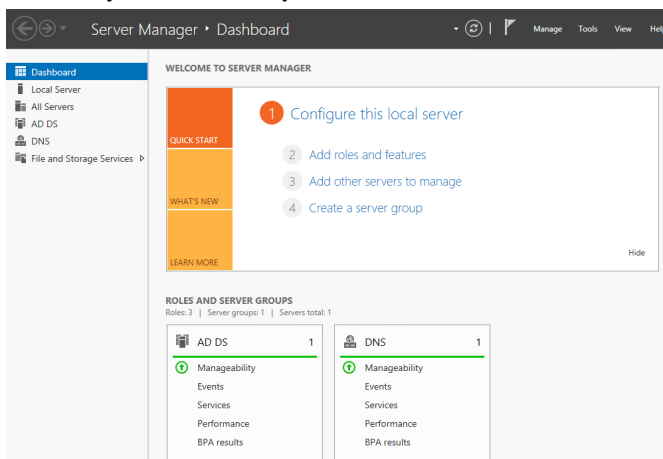


17. Wait for the Prerequisite Check to complete and click **Install**.



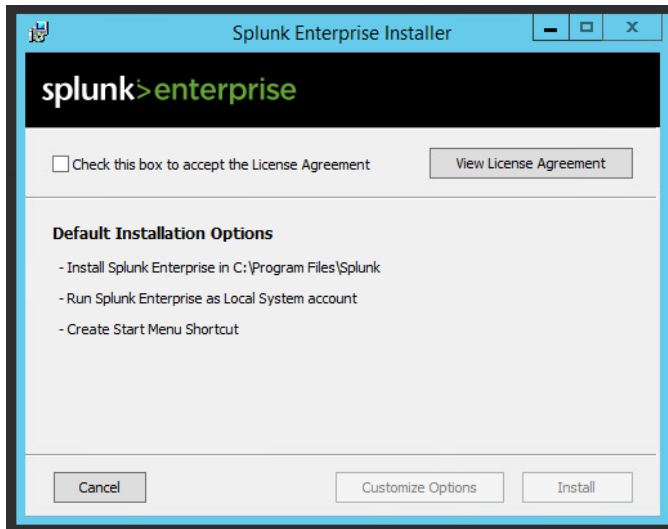
18. The VM will automatically restart. Select **Actions > Guest OS > Send Keys > Ctrl-Alt-Del**. Enter the administrator password to login.

19. You have successfully installed AD DS and promoted your VM to domain controller. Select **Active Directory Users & Computers** from the Tools menu to create test users and groups.

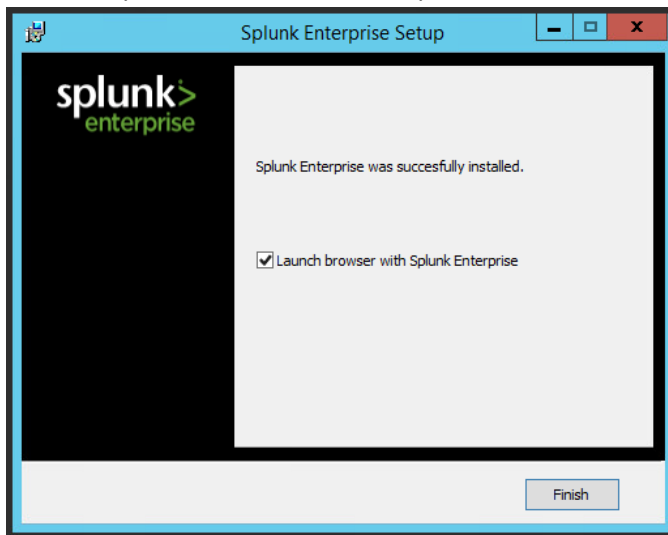


Installing Splunk Enterprise

1. Download the Splunk Enterprise installer, see Appendix II for more information.
2. From your desired virtual machine, launch the Splunk Installer, read and respond to the license agreement and click **Install**.



3. Wait for Splunk installation to complete and click **Finish**.



4. Splunk is now installed and will launch in the browser. Login and select the free license option. Splunk is now ready to use.

