



Active Scan

User Manual

Build 2.2.0.1

2017-04-14

This is the official user manual on using and configuring SAMLite Active Scan.

Table of Contents

SAMLite 5 Active Scan Guide	3
Quick Setup Steps	3
Scan Types.....	4
Active Scan Page	5
Configuration	6
Configure Active Probe	6
New Active Probe.....	6
Edit an Existing Active Probe.....	7
Remove Active Probe.....	7
Configure Credentials.....	8
Add a Windows Credential	8
Add an SSH Credential	9
Credential Details.....	10
Remove Credentials	10
Active Collection	11
Active Scan Now.....	11
Monitoring scan progress	14
Schedule Scan	15
Create a new schedule.....	15
Update an existing Schedule.....	19
Remove a Schedule.....	20
Event Log.....	21
Active Scan Event Log	21
Schedule History	22
Appendix	23
Putty.....	23
Creating an SSH Key	23
Converting an existing OpenSSH key to Putty format	28
Installing an SSH Public Key on Linux/Unix	31
Enabling SSH access on OS X.....	32

SAMLite 5 Active Scan Guide

The SAMLite Active Scan is a network based scanning method. With this method the SAMLite Active Probes make network connections to machines to try to scan them. Scans can be started manually or based on a schedule.

By default an Active Probe is installed by the SAMLite installer on the same machine as the rest of the SAMLite modules. You can install Active Probes on other machines to increase coverage or work within network/firewall restrictions. The default URL for Active Probes is *http://<Probe Address>/SAMLiteActiveProbe/activeprobe.asmx*

The default local active probe can be accessed with Probe Address = localhost or 127.0.0.1.

If probes are installed on other machines they can be access using a similar URL but with the Probe Address set to the machine's IP or address.

Quick Setup Steps

- 1) Login to the SAMLite Web Dashboard
- 2) Click on Active Scan
- 3) Click on Configure Active Probe
- 4) Configure and add a local Active Probe (127.0.0.1)
- 5) Go to Active Scan, Configure Credential
- 6) Add credentials for the Active Probe to use for scanning
- 7) Go to Active Scan and create a schedule for scanning.

Scan Types

- IP Address/Hostname

This runs WMI scans on hostnames, IP addresses or IP ranges.

- Windows Network Neighbourhood

This runs WMI scans on machines discovered in the Network Neighborhood.

- SMS/SCCM Collection

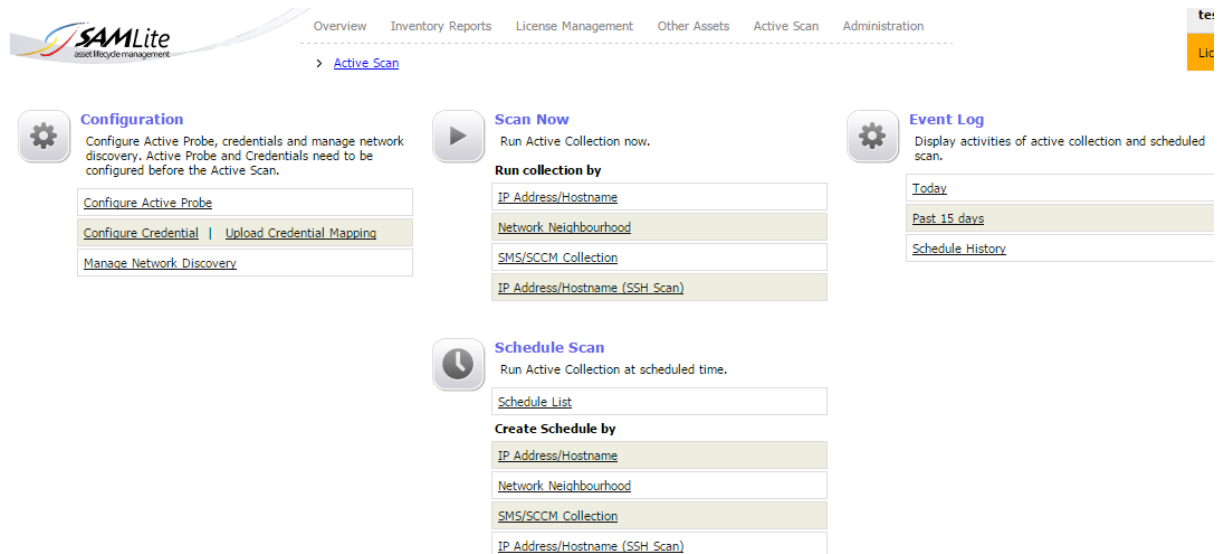
This gets scan information by querying a specified SCCM database.

- IP Address/Hostname (SSH Scan)

This runs SSH scans on hostnames, IP addresses or IP ranges.

Active Scan Page

To access the Active Scan configuration page, users must have Active Collection Moderator rights.



The screenshot shows the SAMLite web interface. The top navigation bar includes links for Overview, Inventory Reports, License Management, Other Assets, Active Scan, and Administration. The 'Active Scan' link is highlighted. Below the navigation bar, there are three main sections: Configuration, Scan Now, and Event Log. The Configuration section includes links for Configure Active Probe, Configure Credential, Upload Credential Mapping, and Manage Network Discovery. The Scan Now section includes a 'Run collection by' dropdown menu with options: IP Address/Hostname, Network Neighbourhood, SMS/SCCM Collection, and IP Address/Hostname (SSH Scan). The Event Log section includes a 'Today' dropdown menu with options: Today, Past 15 days, and Schedule History. Below the Scan Now section, there is a 'Schedule Scan' section with a 'Schedule List' dropdown menu and a 'Create Schedule by' dropdown menu with the same options as the Scan Now section.

Name	Description
Configure Active Probe	Configure/Add Active Probes to be used for scanning
Configure Credential	Configure Credentials that will be used to connect to client machines
Scan Now	Perform scans immediate after the configuration. Click one from sub menus to select the scan type.
Schedule Scan	Perform scans at a scheduled time. Click one from sub menus to select the scan type.
Event Log	View scan related logs.
Schedule History	Display schedule history such as start times of scheduled scans.

Configuration

Configure Active Probe

Configure Active Probe

Complete the form to add an active probe. Select an existing active probe from the list to modify its details. Click + to add new active probe.

2 records ✓ ✕ ✕ +

<input type="checkbox"/>	Server Name	IP Address	Port	Enabled
<input type="checkbox"/>	Remote Server 1	10.55.1.2	80	✓
<input type="checkbox"/>	local	127.0.0.1	80	✓

Add new Active Probe

Server Name

Location/port

Description

Enabled

☒

A list of configured active probes will be displayed at the left panel while the new or selected active probe configuration will be on the right panel.

To disable active probes select them on the left panel and click the green X ✕ button. To enable selected the active probes click on the green tick ✓ button. To delete, click on the red X ✕ button.

To add an active probe click on the + button:

New Active Probe

Field name	Description
Server Name	Name of the Server
IP Address	IP address in ipv4 (4 segments), together with the port number. The port number is used if the SAMLite Active Probe is not installed in default website (port 80)
Description (Optional)	Description of active probe
Enable	Check to enable the active probe on creation

How to configure new active probe:

- 1) Complete the form at the right panel. (Or click + and complete the form)
- 2) Click **Test Connection** to test on Active Probe
- 3) Click **Add** if the test succeeds and you see a green Valid below Location/port.

Edit an Existing Active Probe

Configure Active Probe

Complete the form to add an active probe. Select an existing active probe from the list to modify its details. Click [+](#) to add new active probe.


<input type="checkbox"/>	Server Name	IP Address	Port	Enabled
<input type="checkbox"/>	Remote Server 1	10.55.1.2	80	<input checked="" type="checkbox"/>
<input type="checkbox"/>	local	127.0.0.1	80	<input checked="" type="checkbox"/>

Active Probe Detail

Server Name	<input type="text" value="Remote Server 1"/>
Location/port	<input type="text" value="10.55.1.2"/> <input style="width: 50px;" type="text" value="80"/>
<input type="button" value="Test Connection"/>	
Description	<div style="border: 1px solid #ccc; height: 30px;"></div>
Enabled	<input checked="" type="checkbox"/>
<input type="button" value="Get Local Location"/> <input type="button" value="Update"/>	

- 1) Select an active probe at left panel.
- 2) Details of the selected probe will be displayed at right panel.
- 3) Click **Update** to save the changes.


Remove Active Probe











- 1) Select the active probe to delete on left panel.
- 2) Click 

Note: All schedules using removed active probe will be disabled

Configure Credentials


Configure Credential

Complete the form to add a new credential. Select an existing credential from the list to modify its details. Click  to add new credential.

6 records    					Add New Credential	
<input type="checkbox"/>	Type	Username	Description	Enabled	Credential Type	
<input type="checkbox"/>	SSH	<u>root</u>	test		Userid	<input type="text"/>
<input type="checkbox"/>	SSH	<u>root</u>	privkey.ppk		Password	<input type="text"/>
<input type="checkbox"/>	SSH	<u>root</u>			Confirm Password	<input type="text"/>
<input type="checkbox"/>	SSH	<u>test2</u>			Description	<input type="text"/>
<input type="checkbox"/>	Windows	<u>isat\samlite</u>			Enabled	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Windows	<u>localhost\administrator</u>			<input type="button" value="Add"/>	


Credentials store a list of username and password that will be used to connect to client machines. Passwords are encrypted during the process. Username/Userid refers to the logon ID used for logging on and not the user's display name.

Add a Windows Credential

- 1) Click  if the "Add New Credential" form is not visible.
- 2) Select Windows for Credential Type
- 3) Fill in the credential details.
- 4) Click **Add** to add the credential

Add an SSH Credential

Add New Credential	
Credential Type	SSH ▼
Userid	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
SSH Key (.ppk)	<input type="button" value="Choose file"/> No file chosen
Description	<input type="text"/>
Enabled	<input checked="" type="checkbox"/>
<input type="button" value="Add"/>	

- 1) Click  if the “Add New Credential” form is not visible.
- 2) Select SSH for Credential Type
- 3) Fill in the credential details.
- 4) Optionally upload a “Putty” format SSH public key (.ppk file extension). If an SSH key is used the specified Password will be used to decrypt it. Refer to the Appendix on creating or importing SSH keys.
- 5) Click **Add** to add the credential

Credential Details

Configure Credential

Complete the form to add a new credential. Select an existing credential from the list to modify its details. Click [+](#) to add new credential.

6 records ✓ ✕ ✕ ✕ +				
<input type="checkbox"/>	Type	Username	Description	Enabled
<input type="checkbox"/>	SSH	root	test	✓
<input type="checkbox"/>	SSH	root	privkey.ppk	✓
<input type="checkbox"/>	SSH	root		✕
<input type="checkbox"/>	SSH	test2		✓
<input type="checkbox"/>	Windows	isat\samlite		✓
<input type="checkbox"/>	Windows	localhost\administrator		✓

Credential Detail

Credential Type	SSH ▼
Userid	<input type="text" value="test2"/>
Password	(Not displayed) Edit
SSH Key	1482 bytes <input type="checkbox"/> Delete key
New SSH Key (.ppk)	<input type="button" value="Choose file"/> No file chosen
Description	<div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div>
Enabled	<input checked="" type="checkbox"/> Enable this to use this credential for active collection

- 1) Select a username from credential list
- 2) Details of selected username will be displayed at right panel.
- 3) You may change the details. Check the Delete key checkbox if you wish the SSH key to be deleted when changes are saved.
- 4) Click **Save** to save the changes.

Remove Credentials

- 1) Select a username at left panel
- 2) Click **Delete** to remove the credential

Active Collection

Active Scan Now

Configure Active Probe
Configure Credential

Complete the configuration to begin the active collection

Collect Now

General Setting

Active ProbeRemote Server 1 (IP: 10.55.1.2:80)
Collection TypeIP Address/Hostname

Collection Type Configuration

Insert the hostname/ip address and click add

Hostname/IPAddress
Add >

IP Address Range

From10243
To10243
Add >

Please Add hostname, IP Address or range before begin the scan

There are 3 steps for configuring an Active Scan:

- 1) Select active probe
- 2) Select a collection type
- 3) Specify collection details/settings

Active ProbeRemote Server 1 (IP: 10.55.1.2:80)
Collection TypeIP Address/Hostname

First select the active probe that will be used for active collection. Next select a collection type. This is to choose the scanning method e.g. IP Address/Hostname (Windows Scan), Network Neighborhood (Windows Scan), SMS/SCCM Collection (connect to SCCM database) or SSH Scan.

IP Address/Hostname, SSH Scan

Collection Type Configuration

Insert the hostname/ip address and click add

IP Address Range

From	10	.	243	.	<input style="width: 100%;" type="text"/>	.
	<input style="width: 100%;" type="text"/>					
To	10	.	243	.	<input style="width: 100%;" type="text"/>	.
	<input style="width: 100%;" type="text"/>					

Import list of computers to scan (csv file)

No file chosen

✖

Please Add hostname, IP Address or range before begin the scan

For the IP Address/Hostname or SSH Scan collection types, specify the hostnames, IP addresses or IP ranges to be scanned. Then click on “Collect Now”

You can also import a list of machines to be scanned:

1) Import list of machines to be scanned

- a. You must have the CSV file that contains the list of machine to scan.
- b. The file will contain either the IP address or hostnames of machines that you wish to scan.
- c. Each IP address or hostname is separated by a breakline. E.g. :

192.168.1.1
 192.168.1.4
 192.168.1.96
 .
 .
 .
 192.168.1.234
- d. To import the list, click “Choose File” button and select the file.
- e. Click “Import” button to add them into your scanning list.

Page **12** of 33

Network Neighbourhood

Complete the configuration to begin the active collection	
Collect Now	
General Setting	
Active Probe	Remote Server 1 (IP: 10.55.1.2:80) ▼
Collection Type	Windows Network Neighbourhood ▼
Collection Type Configuration	
Method	<input checked="" type="radio"/> Discover and scan computers <input type="radio"/> Choose computers
Collect Now	

To scan discovered computers pick the “Discover and scan computers” option then click on Collect Now.

To choose computers you want to scan pick the “Choose computers option”:

Collection Type Configuration	
Method	<input type="radio"/> Discover and scan computers <input checked="" type="radio"/> Choose computers
Active Probe	local (IP: 127.0.0.1:80) ▼ SAMLite is now discovering networks. It takes a few minutes to complete depending on the size of network.
Discover Network Now	
Select discovered computers from the list below: (Refresh list) <input checked="" type="checkbox"/> hide Operating System	
<input type="checkbox"/> Select All <input type="checkbox"/> adtest2.here <input type="checkbox"/> SAMLITE-PC <input type="checkbox"/> WINXP PROJSE <input type="checkbox"/> ADTEST2 <input type="checkbox"/> SAMLITEWIN81	

Then select the machines to be scanned and click on Collect Now.

SCCM/SMS Collection

Collection Type Configuration	
Please provide SCCM/SMS Database connection settings	
SCCM/SMS Database Instance	192.168.1.5
Authentication	SQL Server Authentication ▼ Login ID: samlite Password: Connect
Collect Now	

Enter the address of the SCCM database, and the appropriate credentials to access it. Then click on connect.

Collection Type Configuration	
Please provide SCCM/SMS Database connection settings	
SCCM/SMS Database Instance	192.168.1.5
Authentication	SQL Server Authentication ▼ Login ID: samlite Password: <input type="password"/> <input type="button" value="Connect"/>
Select Database	-- Select Database -- ▼
Validity	CM_ISA
Computers	master msdb tempdb

If the connection was successful you can select the SCCM database you wish to collect data from.

Collection Type Configuration	
Please provide SCCM/SMS Database connection settings	
SCCM/SMS Database Instance	192.168.1.5
Authentication	SQL Server Authentication ▼ Login ID: samlite Password: <input type="password"/> <input type="button" value="Connect"/>
Select Database	CM_ISA ▼
Validity	Valid SMS/SCCM database
Computers	4

If the selected database is valid and compatible you will see the message “Valid SMS/SCCM database”. You can then click on “Collect Now” to run the scan.

Monitoring scan progress

You can monitor the progress of the scan by viewing the Event Logs. See the Event Logs section for details.

Schedule Scan

Schedule scans are scans done on a schedule (e.g. daily, weekly).

Create a new schedule



Schedule Scan

Run Active Collection at scheduled time.

[Schedule List](#)

Create Schedule by

[IP Address/Hostname](#)

[Network Neighbourhood](#)

[SMS/SCCM Collection](#)

[IP Address/Hostname \(SSH Scan\)](#)

Select the scan/collection type.

General Setting	
Schedule Name	<input type="text"/>
Active Probe	Remote Server 1 (IP: 10.55.1.2:80) ▼
Start Time	<input checked="" type="radio"/> This time <input type="radio"/> At Specific time with Date: <input type="text" value="12/04/2017"/> Time: <input type="text" value="18:43"/> (24 hour format)
Interval	<input type="radio"/> Everyday <input checked="" type="radio"/> Once a week <input type="radio"/> First <input type="text" value="Sunday"/> of every month <input type="radio"/> Every day of week on <input type="text" value="Sunday"/> <input type="radio"/> Every <input type="text" value="0"/> day <input type="text" value="0"/> hour <input type="text" value="0"/> minute
Repeat	<input type="checkbox"/> Repeat <input type="text" value="0"/> times (Uncheck to repeat the scan continuously)
Collection Type	IP Address/Hostname ▼

Fill in the Schedule Details. You can still change the Collection Type at this point.

IP Address/Hostname, SSH Scan

Collection Type Configuration	
<div> <div>Insert the hostname/ip address and click add</div> <div> <div>Hostname/IPAddress</div> <div></div> <div>Add ></div> </div> </div>	
<div> <div>IP Address Range</div> <div> <div>From</div> <div> <div>10</div> <div>243</div> <div></div> </div> </div> <div>To</div> <div> <div>10</div> <div>243</div> <div></div> </div> </div> <div>Add ></div>	
<div> <div>Import list of computers to scan (csv file)</div> <div> <div>Choose file</div> <div>No file chosen</div> </div> <div>Import ></div> </div>	

✖

Please Add hostname, IP Address or range before begin the scan

Specify the hostnames, IP addresses or IP ranges to be scanned.

Network Neighbourhood

Collection Type Configuration	
Method	<input type="radio"/> Discover and scan computers <input type="radio"/> Choose computers
<div>Create</div>	

To scan discovered computers pick the “Discover and scan computers” option then click on Create.

To choose computers you want to scan pick the “Choose computers option”:

Collection Type Configuration	
Method	<input type="radio"/> Discover and scan computers <input checked="" type="radio"/> Choose computers
Active Probe	<div>local (IP: 127.0.0.1:80)</div> <div>SAMLite is now discovering networks. It takes a few minutes to complete depending on the size of network.</div> <div>Discover Network Now</div>
<div>Select discovered computers from the list below: (Refresh list) <input checked="" type="checkbox"/> hide Operating System</div> <div> <input type="checkbox"/> Select All <div> <input type="checkbox"/> adtest2.here <div> <input type="checkbox"/> SAMLITE-PC <input type="checkbox"/> WINXP PROJ51 </div> </div> <div> <input type="checkbox"/> ADTEST2 <div> <input type="checkbox"/> SAMLITEWIN81 </div> </div> </div>	

Then select the machines to be scanned and click on Create.

SCCM/SMS Collection

Collection Type Configuration	
Please provide SCCM/SMS Database connection settings	
SCCM/SMS Database Instance	<input type="text" value="192.168.1.5"/>
Authentication	<div>SQL Server Authentication ▼</div> <div> Login ID: <input type="text" value="samllite"/> Password: <input type="password" value="*****"/> <input type="button" value="Connect"/> </div>
<input type="button" value="Create"/>	

Enter the address of the SCCM database, and the appropriate credentials to access it. Then click on connect.

Collection Type Configuration	
Please provide SCCM/SMS Database connection settings	
SCCM/SMS Database Instance	<input type="text" value="192.168.1.5"/>
Authentication	<div>SQL Server Authentication ▼</div> <div> Login ID: <input type="text" value="samllite"/> Password: <input type="password"/> <input type="button" value="Connect"/> </div>
Select Database	<div>-- Select Database -- ▼</div> <div>-- Select Database --</div>
Validity	CM_ISA
Computers	master msdb tempdb

If the connection was successful you can select the SCCM database you wish to collect data from.

Collection Type Configuration	
Please provide SCCM/SMS Database connection settings	
SCCM/SMS Database Instance	<input type="text" value="192.168.1.5"/>
Authentication	<div>SQL Server Authentication ▼</div> <div> Login ID: <input type="text" value="samllite"/> Password: <input type="password"/> </div> <div>Connect</div>
Select Database	CM_ISA ▼
Validity	Valid SMS/SCCM database
Computers	4

If the selected database is valid and compatible you will see the message “Valid SMS/SCCM database”.

Saving changes

Once the settings are as desired, click on to create the schedule.

Update an existing Schedule

Select Schedule List to get a list of existing schedules.

> [Active Scan](#) > [Schedule List](#)

Innovation

+ Create New Schedule

4 records ✓ ✗ ✗

	Schedule Name	Active Probe	Created Date	Last Scheduled time	Next Scheduled Time	Enabled	Repeat Scan Remaining
<input type="checkbox"/>	isa_sccm_test	local	24/03/2016 5:01:24 PM	12/04/2017 4:49:24 PM	13/04/2017 4:49:22 PM	✓	-
<input type="checkbox"/>	test	Remote Server 1	4/06/2013 2:23:26 AM	27/05/2016 12:33:03 PM	28/05/2016 12:33:00 PM	✗	-
<input type="checkbox"/>	test_winn	local	12/04/2017 6:51:12 PM	12/04/2017 6:51:12 PM	19/04/2017 6:51:11 PM	✓	-
<input type="checkbox"/>	testssh	local	17/03/2017 4:49:37 PM	12/04/2017 4:48:49 PM	13/04/2017 4:48:50 PM	✓	-

- 1) Click the schedule's name from the list.

Schedule Detail

[Update](#)

General Setting

Schedule Name

Active Probe

Start Time
☒ This time
☐ At Specific time with Date: Time: (24 hour format)

Interval
☒ Everyday
☐ Once a week
☐ First of every month
☐ Every day of week on
☐ Every day hour minute

Repeat
☐ Repeat times
 (Uncheck to repeat the scan continuously)

Enabled ☒

Collection Type

Collection Type Configuration

Insert the hostname/ip address and click add

Hostname/IPAddress

[Add >](#)

Type	Value
<input type="checkbox"/> Range	192.168.1.1 - 192.168.1.254
<input type="checkbox"/> Range	10.243.0.1 - 10.243.4.254

- 2) The details of the schedule are displayed on this page. You may change the values and click **Update** to update the settings.

Remove a Schedule

+ Create New Schedule							
4 records ✓ ✗ ✗							
	Schedule Name	Active Probe	Created Date	Last Scheduled time	Next Scheduled Time	Enabled	Repeat Scan Remaining
<input type="checkbox"/>	isa sccm test	local	24/03/2016 5:01:24 PM	12/04/2017 4:49:24 PM	13/04/2017 4:49:22 PM	✓	-
<input type="checkbox"/>	test	Remote Server 1	4/06/2013 2:23:26 AM	27/05/2016 12:33:03 PM	28/05/2016 12:33:00 PM	✗	-
<input checked="" type="checkbox"/>	test wnn	local	12/04/2017 6:51:12 PM	12/04/2017 6:51:12 PM	19/04/2017 6:51:11 PM	✓	-
<input type="checkbox"/>	testssh	local	17/03/2017 4:49:37 PM	12/04/2017 4:48:49 PM	13/04/2017 4:48:50 PM	✓	-

- 1) Select a schedule from the list
- 2) Click ✗ to delete the selected schedule.

Event Log







Active Scan Event Log

Active Scan Event Log

Last updated




<

Select the dates on the left to restrict the records on the right to selected dates.


Control	Description
	Filter records by type
	Filter records by status
Refresh rate	Set the rate the page is to be refreshed automatically.
	Click to refresh the records
	Delete selected records
	Export to Excel readable format
	Search for records

Schedule History

Schedule History displays the start time and end time of the scheduled scans.

366 records    Display date before

<input type="checkbox"/>	Start Time	Next Start Time	Schedule Name
<input type="checkbox"/>	10/04/2017 4:49:22 PM	10/04/2017 4:49:22 PM	isa sccm test
<input type="checkbox"/>	10/04/2017 4:48:50 PM	10/04/2017 4:48:52 PM	testssh
<input type="checkbox"/>	9/04/2017 4:49:22 PM	9/04/2017 4:49:21 PM	isa sccm test
<input type="checkbox"/>	9/04/2017 4:48:50 PM	9/04/2017 4:48:51 PM	testssh
<input type="checkbox"/>	8/04/2017 4:49:22 PM	8/04/2017 4:49:23 PM	isa sccm test
<input type="checkbox"/>	8/04/2017 4:48:50 PM	8/04/2017 4:48:52 PM	testssh
<input type="checkbox"/>	7/04/2017 4:49:22 PM	7/04/2017 4:49:22 PM	isa sccm test
<input type="checkbox"/>	7/04/2017 4:48:50 PM	7/04/2017 4:48:52 PM	testssh
<input type="checkbox"/>	6/04/2017 7:42:46 PM	6/04/2017 7:42:48 PM	isa sccm test

Schedule history is to display the activities of scheduled scan. It shows start time and end time of the scheduled scan. Click  to delete the selected records.

Appendix

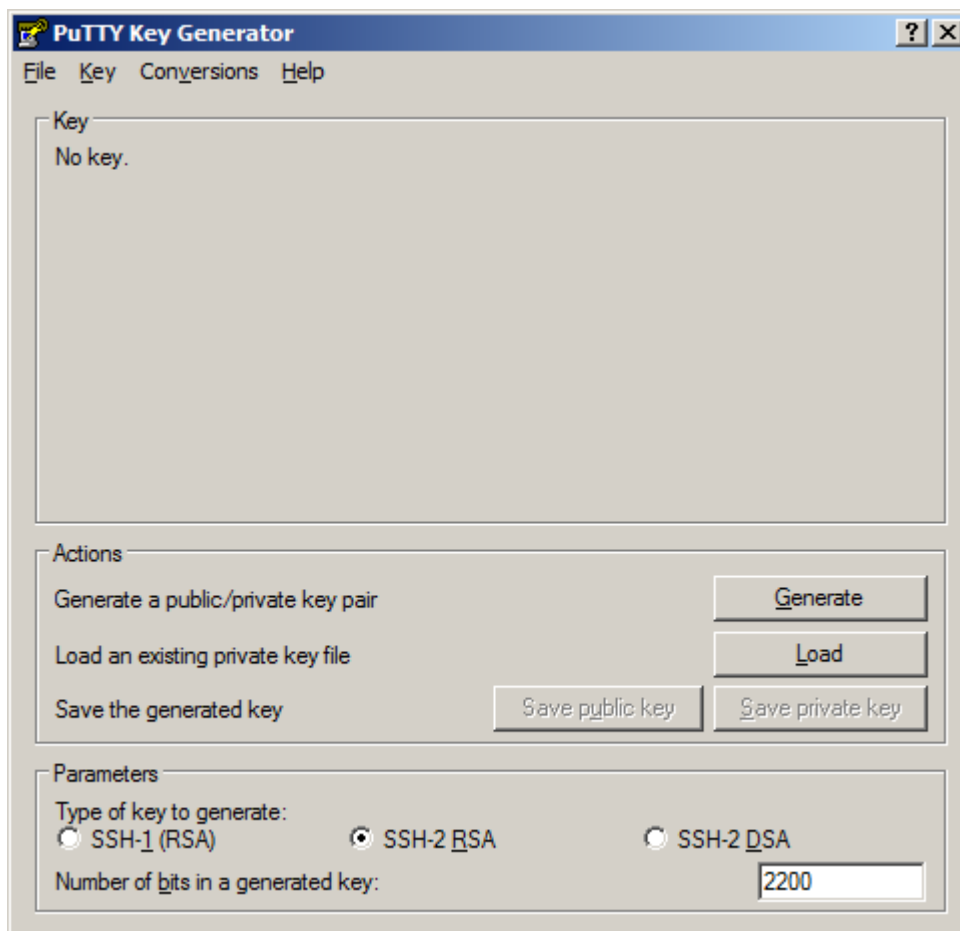
Putty

To manage or create SSH keys on Windows you can use Putty (SSH software for Windows).

You can download Putty from here: <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

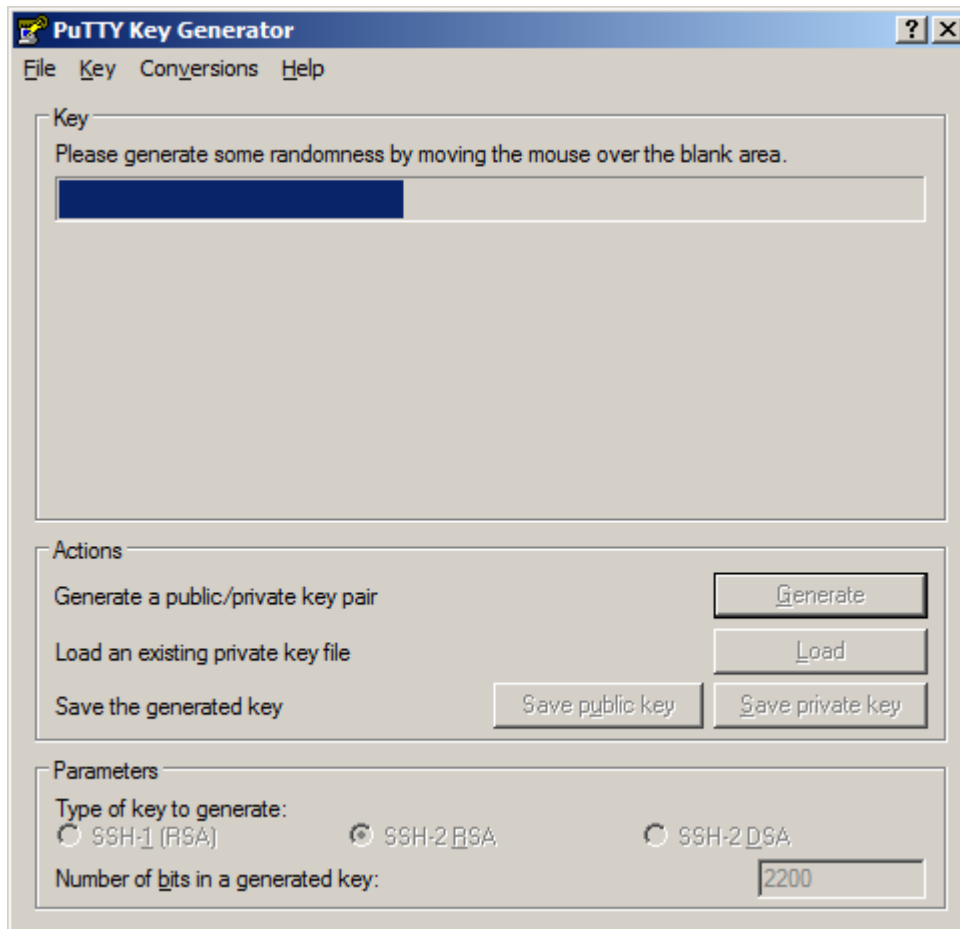
Creating an SSH Key

After installing Putty, run **puttygen**

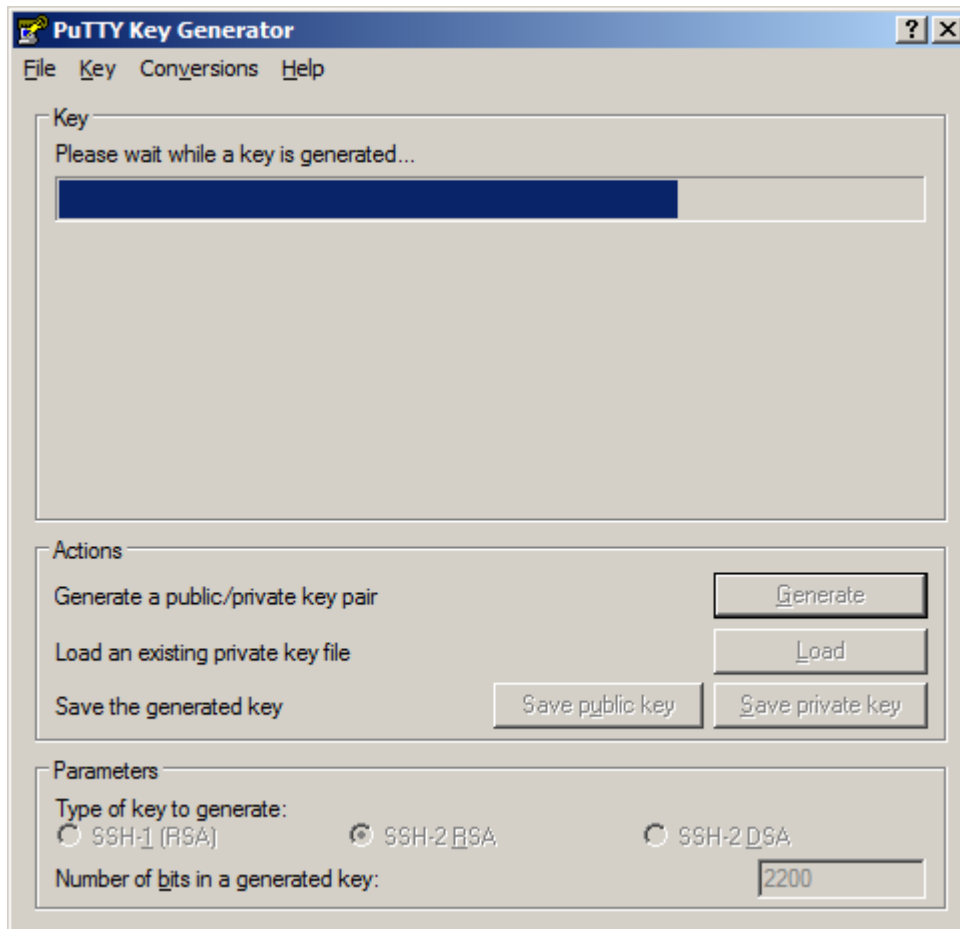


It is recommended to use keys that are larger than 2000 bits. It is also recommended to use SSH-2 RSA keys. SSH-1 and DSA keys are deprecated and not recommended.

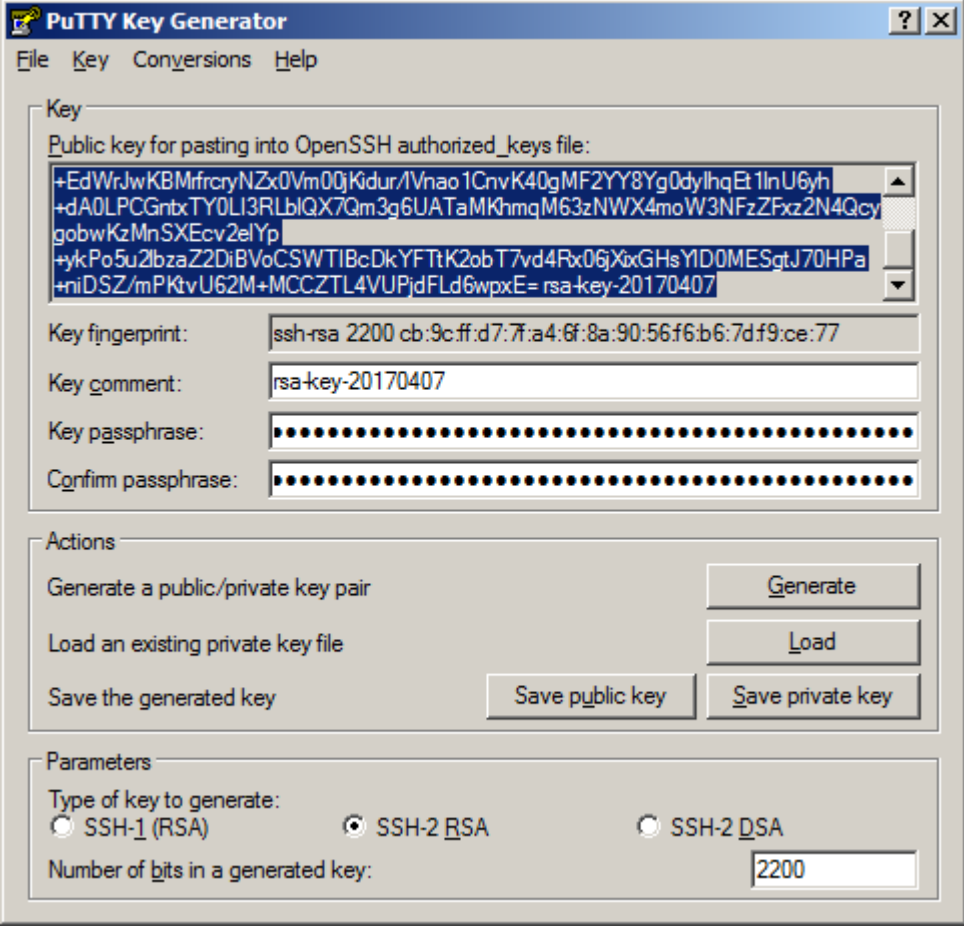
Click on **Generate**.



Move the mouse randomly over the blank area to try to create a key that is difficult to predict.



Wait for the key to be created. If the key is large this may take a while on slow computers.



PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
+EdWrJwKBMrfrcryNZx0Vm00jKidur/1Vnao1CnvK40gMF2YY8Yg0dyIhqEt1lnU6yh
+dA0LPCGntxTY0LI3RLblQX7Qm3g6UATaMKhmQM63zNWX4moW3NFzZFxz2N4Qcy
gobwKzMnSXEcv2elYp
+ykPo5u2lbzaZ2DiBV0CSWTIBcDkYFTtK2obT7vd4Rx06jXixGHsYlD0MESgtJ70HPa
+niDSZ/mPKtvU62M+MCCZTL4VUPjdFLd6wpxE= rsa-key-20170407
```

Key fingerprint: ssh-rsa 2200 cb:9c:ff:d7:7a:4:6f:8a:90:56:f6:b6:7d:f9:ce:77

Key comment: rsa-key-20170407

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:

☐ SSH-1 (RSA) ☒ SSH-2 RSA ☐ SSH-2 DSA

Number of bits in a generated key: 2200

Copy the Public key in OpenSSH format and save it somewhere. For example: sshpubkey.txt

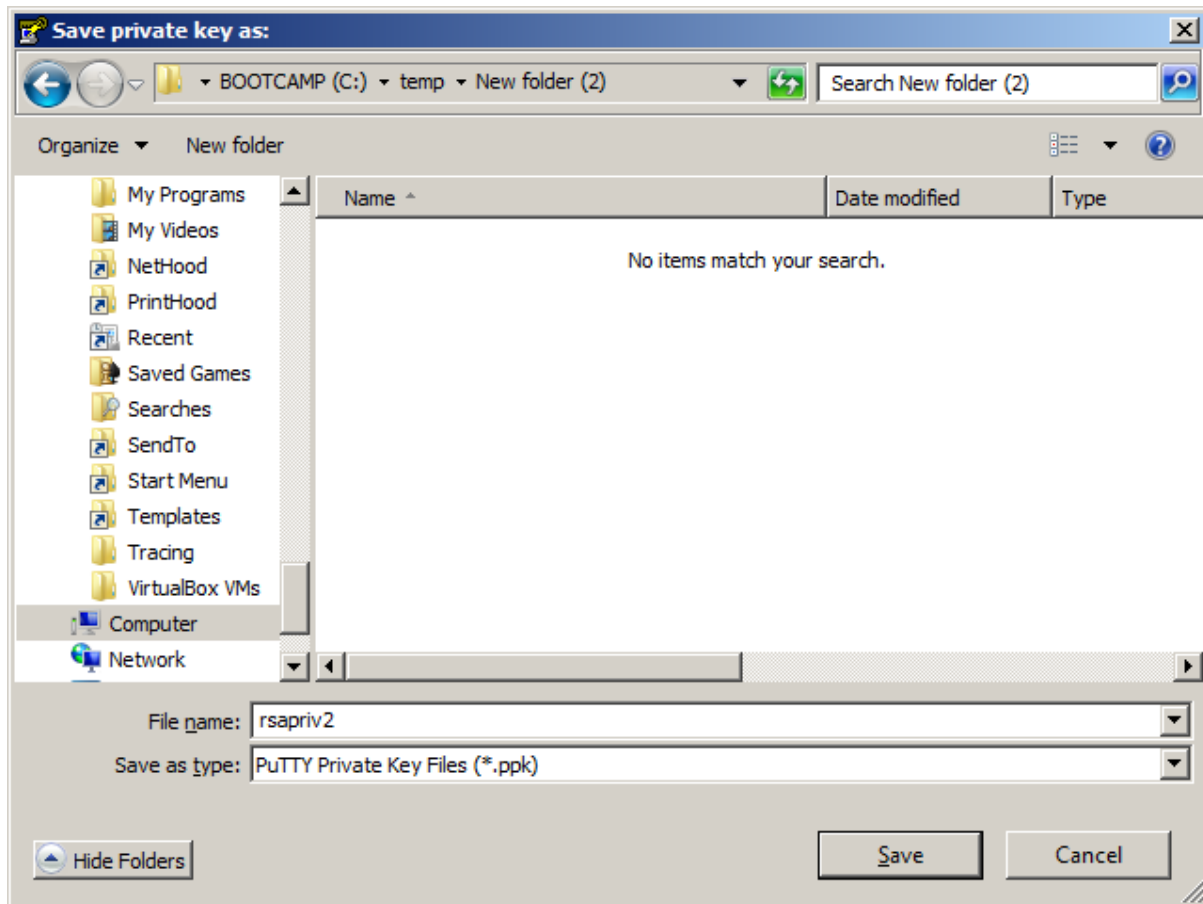
The public key should look similar to this:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAARQA4PaGsN0hEzBqzPcmepZSmL5wfuhJ9ejBstR6WBVmcozzYDPOAHJbsIe
ie5qv/3dlASC6w35J12D1to/dS1jpbqV/uqJ7en+1HCo36YSzze19QbdVKTLp+EdWrJwKBMrfrcryNZx0Vm0
0jKidur/1Vnao1CnvK40gMF2YY8Yg0dyIhqEt1lnU6yh+dA0LPCGntxTY0LI3RLblQX7Qm3g6UATaMKhmQM
63zNWX4moW3NFzZFxz2N4QcygobwKzMnSXEcv2elYp+ykPo5u2lbzaZ2DiBV0CSWTIBcDkYFTtK2obT7vd4
Rx06jXixGHsYlD0MESgtJ70HPa+niDSZ/mPKtvU62M+MCCZTL4VUPjdFLd6wpxE= rsa-key-20170407
```

This text will have to be appended as a single line to the `/root/.ssh/authorized_keys` file onto all the machines to be scanned (see “Appendix: Installing an SSH Public Key” for details).

Enter the Key passphrase and confirmation. Pick a passphrase that is difficult to guess. Do not forget the passphrase.

Click on **Save private key**.



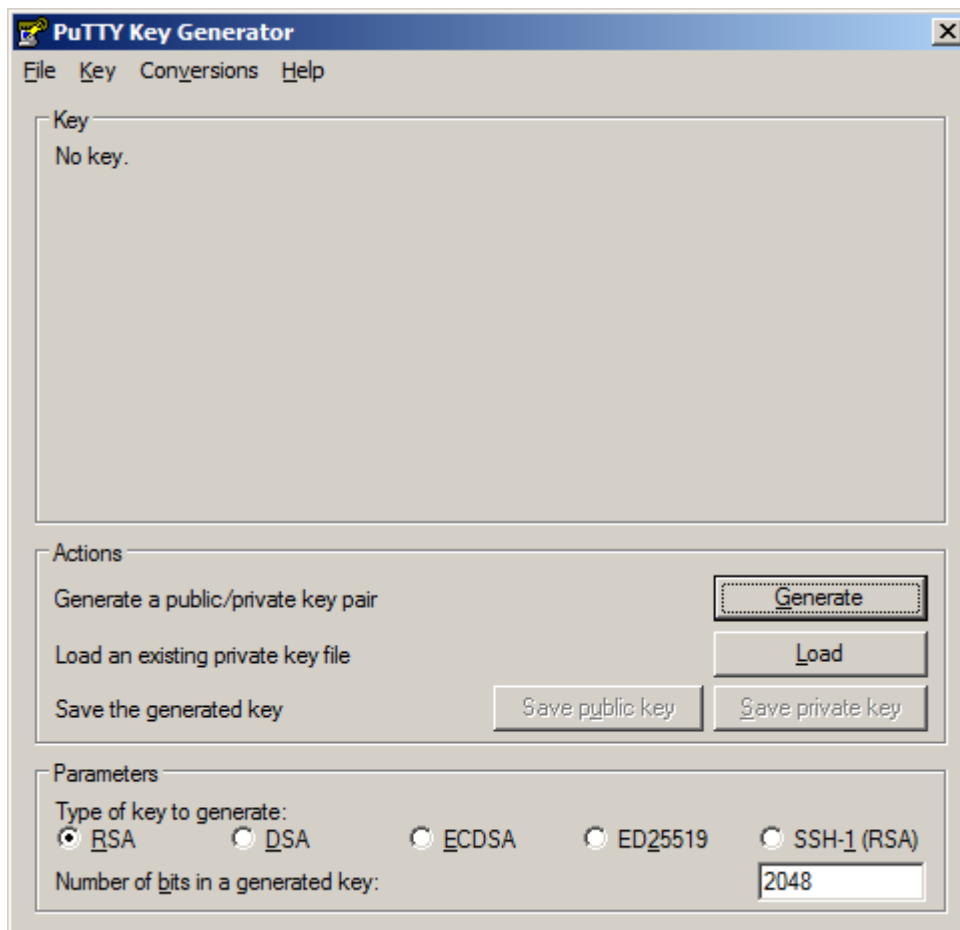
This key and the corresponding passphrase should be used as an SSH Credential.

Converting an existing OpenSSH key to Putty format

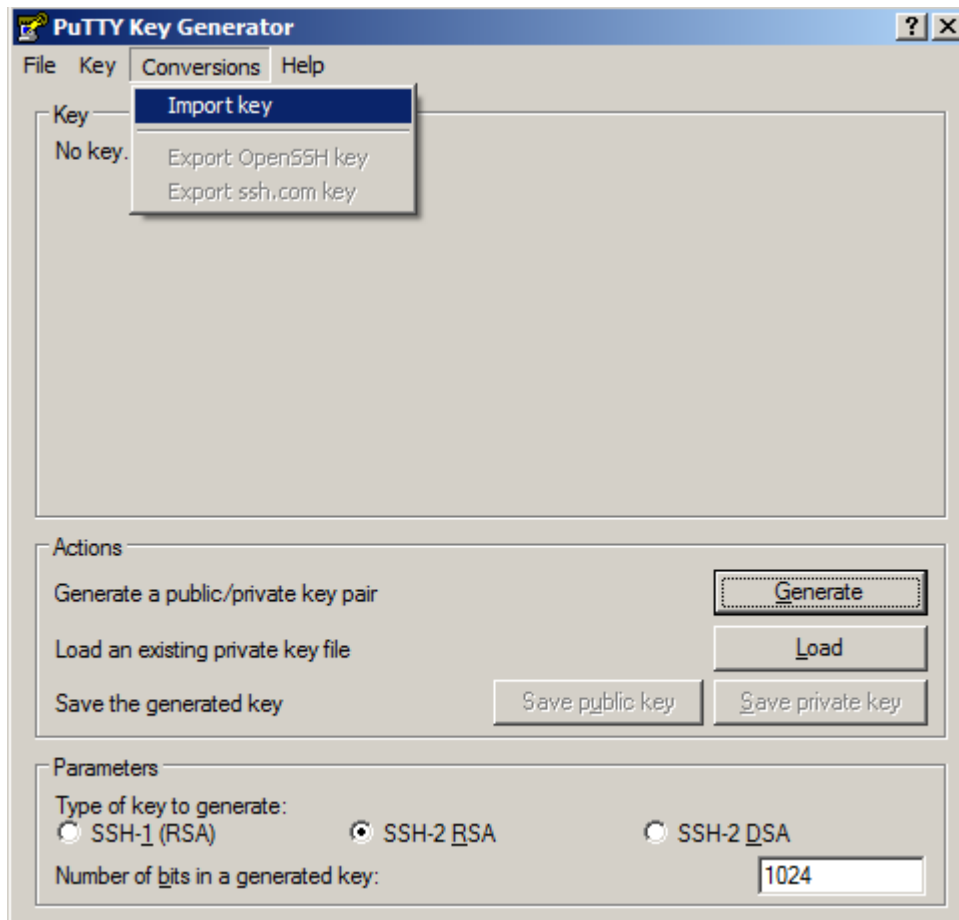
If you have an existing OpenSSH key that you wish to use for scanning (because its already installed on many machines) you need to convert it to the Putty format first.

You need the **private** key not the public key, and also the passphrase for that key if one exists.

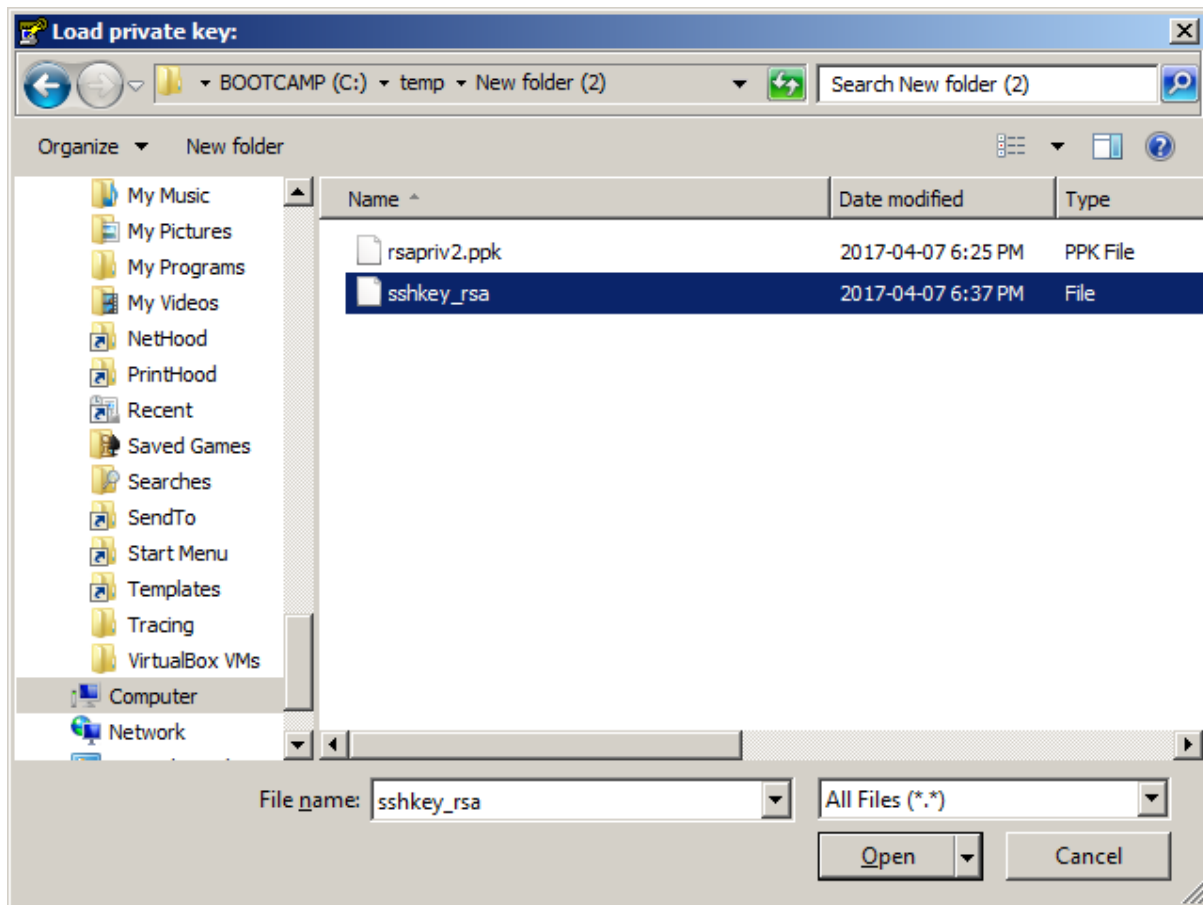
Run PuttyGen



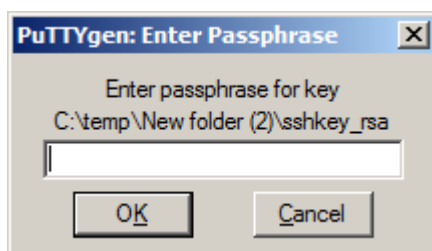
Select Conversions, Import key:



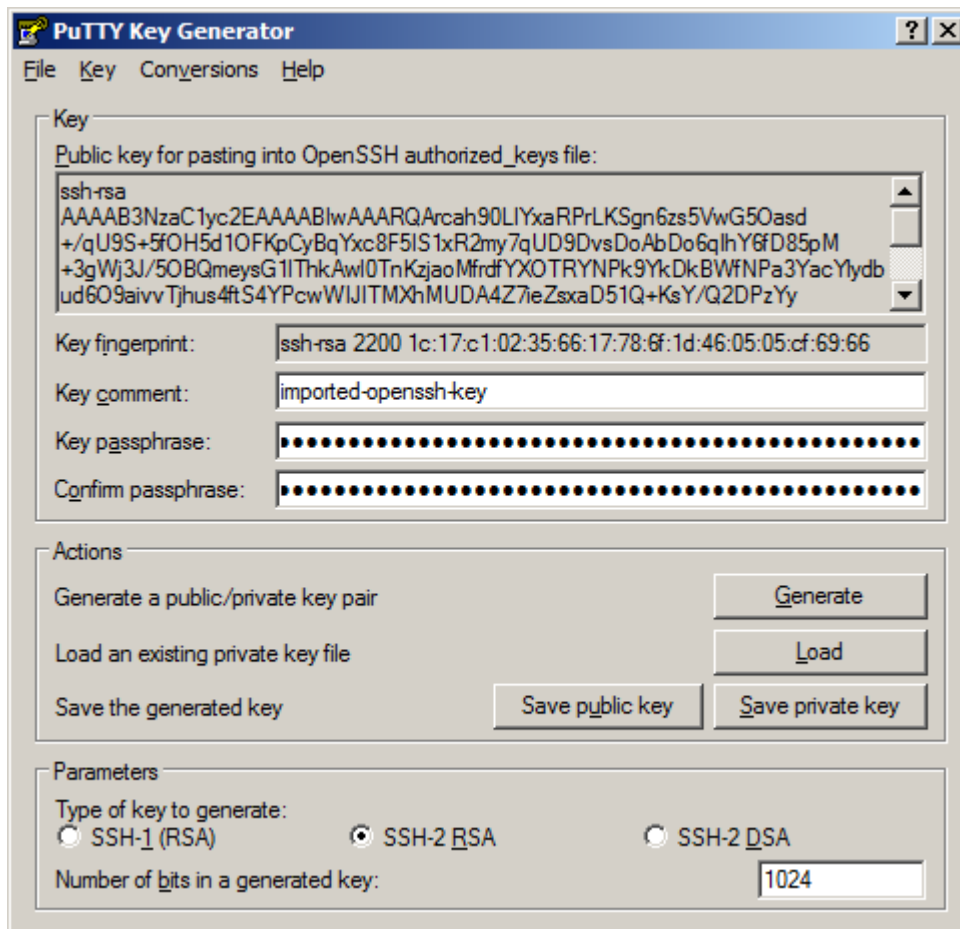
Open the key:



Enter the passphrase:



You should now see something similar to this:



Enter a new passphrase and confirmation if you do not wish to keep the same passphrase.

Then click on **Save private key**.

The new saved private key and corresponding passphrase can be used as a SAMLite Active Probe credential.

Installing an SSH Public Key on Linux/Unix

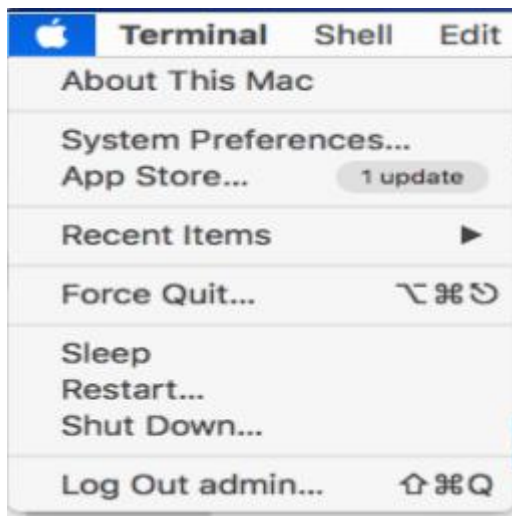
In order to use an SSH private key to log in to a machine, its corresponding SSH Public Key has to be installed. One method is to issue the following command as root on the target machine:

```
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAARQA4PaGsN0hEzBqzPcmepZSmL5wfuhJ9ejBstR6WBVmcozzYDPOAHJbsIe
ie5qv/3dlASC6w35J12D1to/dSljppqV/uqJ7en+1HCo36YSzze19QbdVKTLP+EdWrJwKBMrfrcryNZx0Vm0
0jKidur/1Vnao1CnvK40gMF2YY8Yg0dyIhqEt1lnU6yh+dA0LPCGntxTY0LI3RLblQX7Qm3g6UATaMKhmQM
63zNWX4moW3NFzZFxz2N4QcygobwKzMnSXEcv2e1Yp+ykPo5u2lbzaZ2DiBVoCSWTIBcDkYFTtK2obT7vd4
Rx06jXixGHsY1D0MESgtJ70HPa+niDSZ/mPKtvU62M+MCCZTL4VUPjdFLd6wpxE= rsa-key-20170407"
>> ~/.ssh/authorized_keys
```

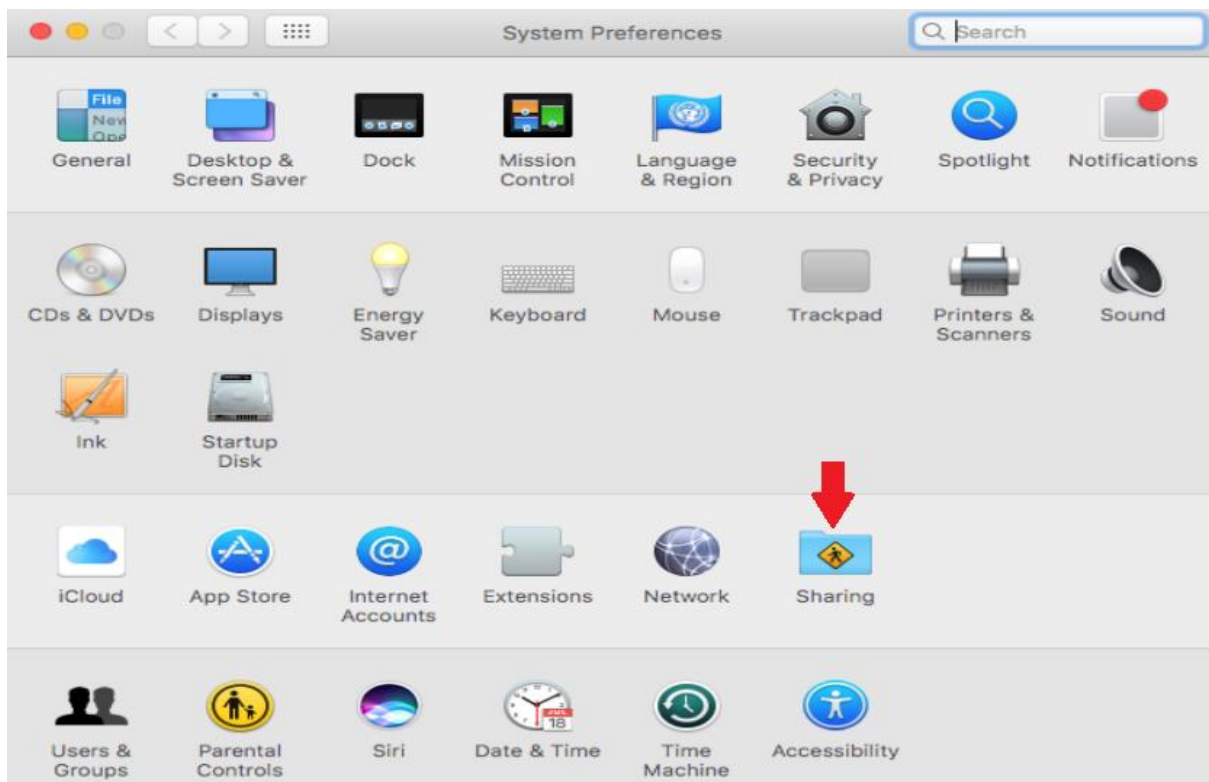
This has to be a single line with no explicit line-breaks. Replace the example key text with the actual public key.

Enabling SSH access on OS X

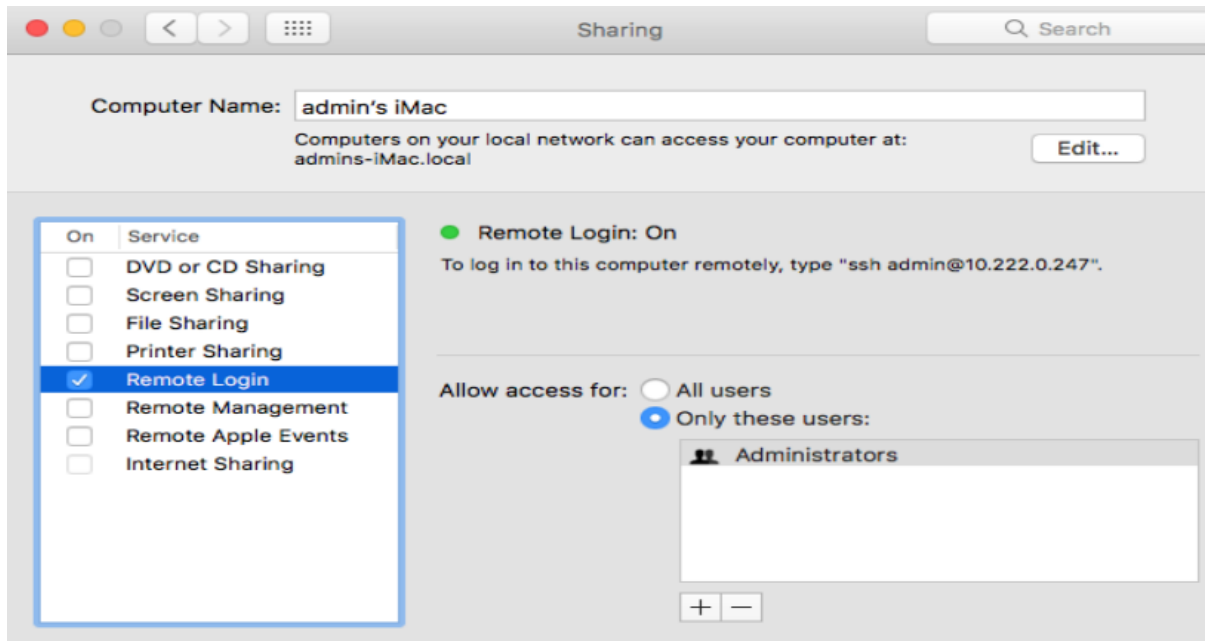
Open the Apple menu.



Select System Preferences.



Click on the “Sharing” preference panel.



Select the checkbox next to “Remote Login”. This will immediately enable SSH access.

You can now close the “Sharing” preference panel.