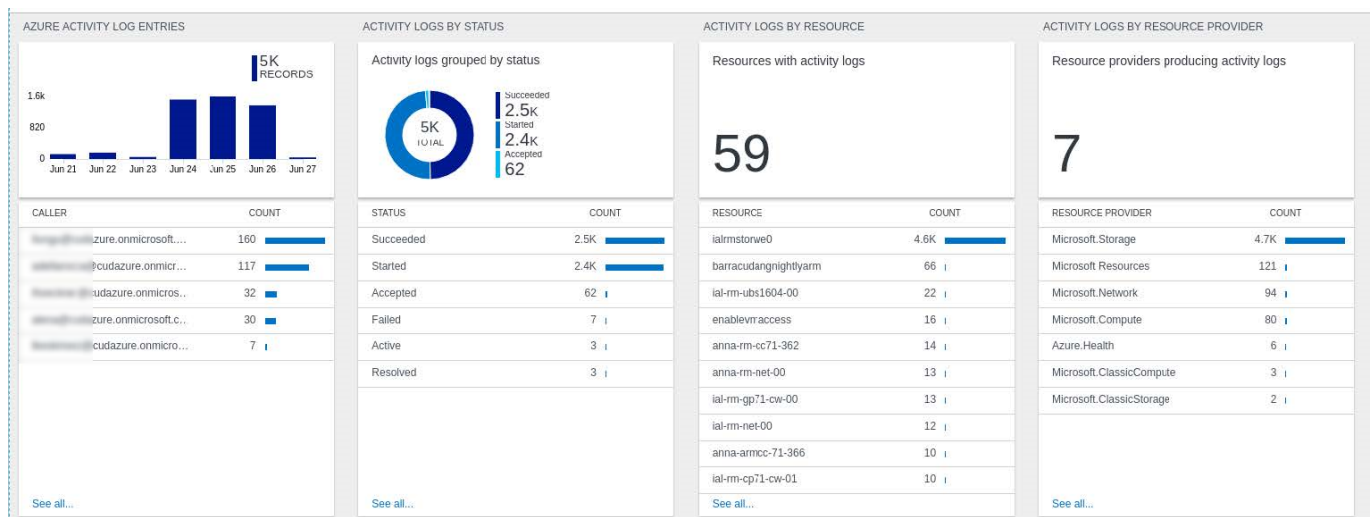


How to Configure Log Streaming to Microsoft Azure Log Analytics

<https://campus.barracuda.com/doc/98210729/>

To stream log data and custom metrics from your firewall to a Log Analytics workspace in Microsoft Azure, you must connect the firewall VM to your Log Analytics workspace and configure syslog streaming on the firewall to send the syslog stream to Azure Log Analytics. For streaming logs to Log Analytics using the CEF format, you must configure Microsoft OMS Security as the streaming destination. On the Azure side, the virtual machines are connected to the Log Analytics workspace. All selected log files are then streamed to Azure Log Analytics, where they can be stored, analyzed, or processed. CloudGen Firewall boxes that run outside the Azure cloud can also be connected to a Microsoft Azure Log Analytics workspace. For more information, see [How to Connect non-Azure CGFs to a Microsoft Azure Log Analytics Workspace](#).

To stream log data from the same source to multiple destinations, you must assign these multiple destinations to that single log source in the Logdata Stream configuration.



Custom VPN Metrics

- Client-to-site VPN tunnels
- SSL VPN clients
- Site-to-site VPN tunnels up
- Site-to-site VPN tunnels down

Custom System Metrics

- Load
- Used memory
- Protected IPs

Custom Firewall Metrics

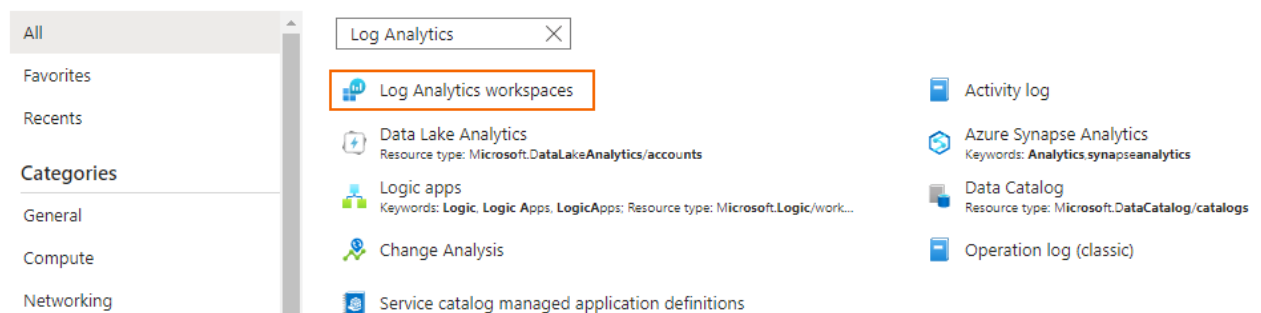
- Bytes in
- Bytes out
- Bytes total
- Packets in
- Packets out
- Packets total
- Connections dropped
- IPS Hits
- Forwarding Connections new
- Forwarding Connections total
- Connections new
- Connections total
- Connections blocked
- Connections failed

Configure log streaming to Azure Log Analytics before managing your firewall via the Control Center.

Step 1. Create a Log Analytics Workspace

1. Log into the Azure portal: <https://portal.azure.com>
2. Go to **All services** and search for **Log Analytics**.
3. Select **Log Analytics workspaces**.

All services



4. In the **Log Analytics workspaces** blade, click **Create**.

Log Analytics workspaces

Barracuda Networks, Inc. (barracuda.com)

[+ Create](#) [Open recycle bin](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#) [Assign tags](#)

Filter for any field... [Subscription equals all](#) [Resource group equals all](#) [Location equals all](#) [Add filter](#)

Showing 1 to 9 of 9 records.

<input type="checkbox"/> Name ↑↓	Resource group ↑↓
<input type="checkbox"/>  alena-ms	alena-rg-001

5. In the **Log Analytics workspaces** blade, enter the following information:

- **Subscription** – Select your subscription.
- **Resource Group** – Select an existing resource group, or create a new, dedicated resource group for your workspace.
- **Name** – Enter a name for the Log Analytics workspace.
- **Region** – Select the geographical location where the data for your workspace will be stored.

[Home](#) > [Log Analytics workspaces](#) >

Create Log Analytics workspace

[Basics](#) [Pricing tier](#) [Tags](#) [Review + Create](#)

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) ×

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ	<input type="text" value="SDWaaS-dev"/>
Resource group * ⓘ	<input type="text" value="(New) Campus-OMS"/>
	Create new

Instance details

Name * ⓘ	<input type="text" value="Campus-OMS-workspace"/>
Region * ⓘ	<input type="text" value="West Europe"/>

[Review + Create](#)[« Previous](#)[Next : Pricing tier >](#)

6. (If applicable) Click **Next : Pricing tier**.

7. The **Pricing tier** blade opens. Specify values for the following:

- **Pricing tier** – Select the pricing tier.

[Home](#) > [Log Analytics workspaces](#) >

Create Log Analytics workspace

Basics

Pricing tier

Tags

Review + Create

The cost of your workspace depends on the pricing tier and what solutions you use.
To learn more about Log Analytics pricing [click here](#)

Pricing tier

You can change to a Capacity Reservation tier after your workspace is created. [Learn more](#)
To learn more about access to legacy pricing tiers [click here](#)

Pricing tier *

Pay-as-you-go (Per GB 2018)



Review + Create


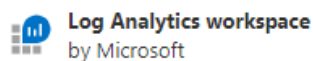
« Previous

Next : Tags >

8. Click **Next : Tags**.
9. Specify values for your tags.
10. Click **Review + Create**.

[Home](#) > [Log Analytics workspaces](#) >

Create Log Analytics workspace

 Validation passed[Basics](#) [Pricing tier](#) [Tags](#) [Review + Create](#)**Log Analytics workspace**
by Microsoft

Basics

Subscription	SDWaaS-dev
Resource group	Campus-LA
Name	Campus-LA-workspace
Region	West Europe

Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)
--------------	-----------------------------

Tags

(none)

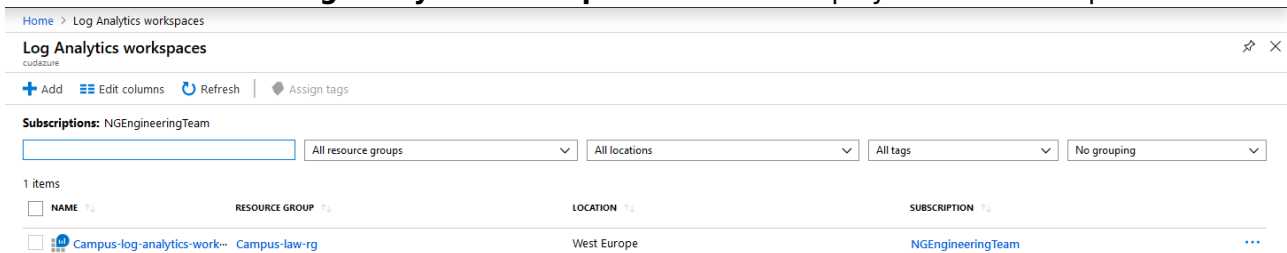
Create

« Previous

[Download a template for automation](#)

11. Verify your settings and click **Create**.

12. Click **Refresh** in the **Log Analytics workspaces** blade to display the new workspace.



Step 2. Install the Log Analytics Template

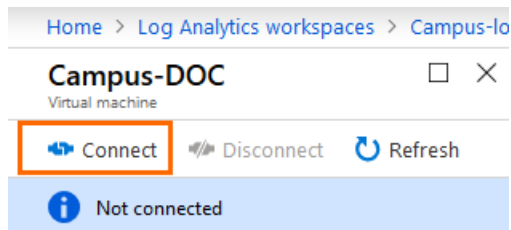
Install the Barracuda CloudGen Firewall Log Analytics ARM template to get the default dashboards, searches, and functions.

- The CloudGen Firewall ARM template to create a log analytics workspace is available on [GitHub](#).

This template installs and configures all dashboards provided by the Barracuda CloudGen Firewall in the Log Analytics workspace. The Log Analytics workspace can be associated with a resource group created in any region.

Step 3. Connect Virtual Machines to the Log Analytics Workspace

1. In the Azure portal, go to the workspace created in Step 1.
2. In the **Connect a data source** section, click **Azure Virtual machine (VMs)**.
3. Search for the name of the CloudGen Firewall virtual machine that you want to connect to the workspace.
4. Click the entry of your virtual machine.
5. Click **Connect**.



Status

Not connected

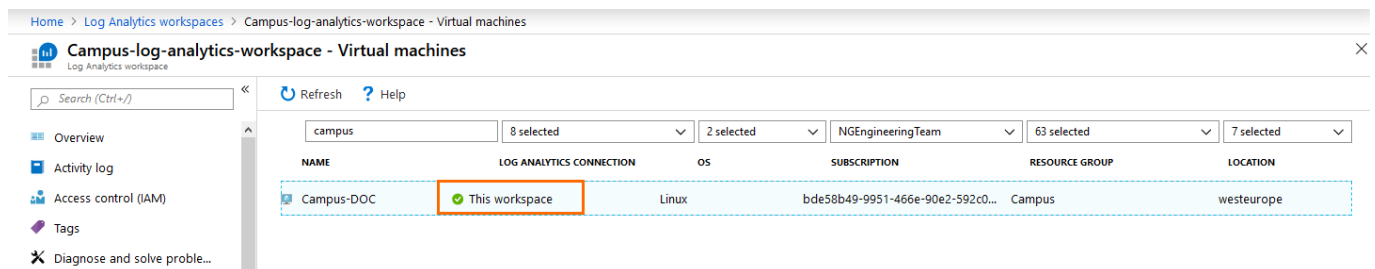
Workspace Name

None

Message

VM is not connected to Log Analytics.

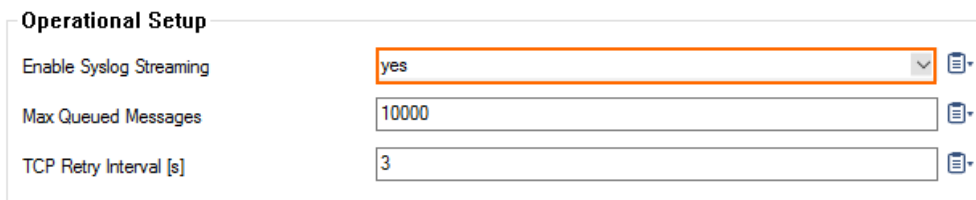
It may take a couple of minutes for the extension to be installed on the firewall.



Step 4. Enable Syslog Streaming on the Firewall VM

Enable syslog streaming on the Barracuda CloudGen Firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. Click **Lock**.
3. Set **Enable Syslog Streaming** to **yes**.

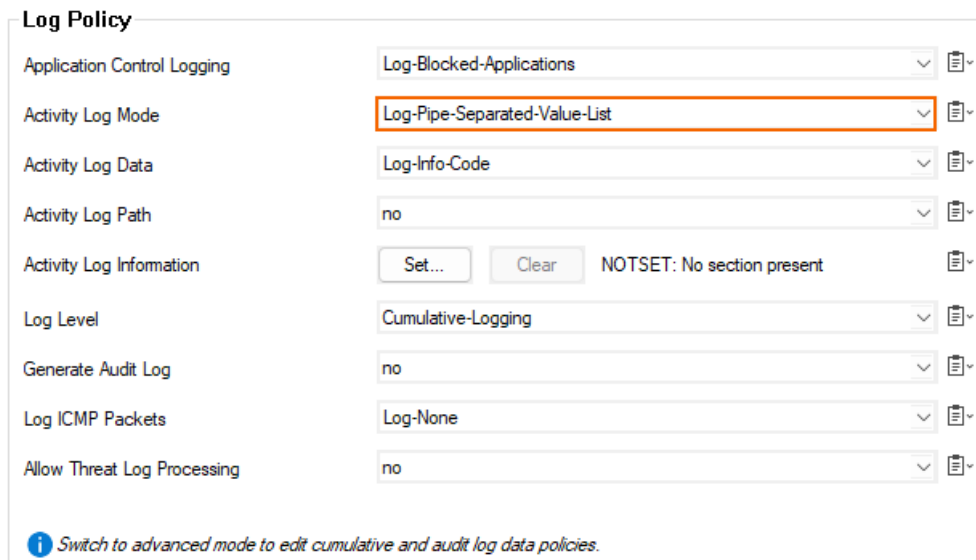


Operational Setup	
Enable Syslog Streaming	yes
Max Queued Messages	10000
TCP Retry Interval [s]	3

4. Click **Send Changes** and **Activate**.

Step 5. Enable Detailed Firewall Reporting

1. Go to **Configuration Tree > Infrastructure Services > General Firewall Configuration**.
2. Click **Lock**.
3. In the left menu, select **Audit and Reporting**.
4. Under **Log Policy**, set the **Activity Log Mode** to **Log-Pipe-Separated-Value-List**.



Log Policy	
Application Control Logging	Log-Blocked-Applications
Activity Log Mode	Log-Pipe-Separated-Value-List
Activity Log Data	Log-Info-Code
Activity Log Path	no
Activity Log Information	Set... Clear NOTSET: No section present
Log Level	Cumulative-Logging
Generate Audit Log	no
Log ICMP Packets	Log-None
Allow Threat Log Processing	no

Switch to advanced mode to edit cumulative and audit log data policies.

5. Click **Send Changes** and **Activate**.

Note: For streaming logs in syslog format, you can also chose **Log-Pipe-Separated-Key-Value-List**.

Example output: 2024 05 07 10:02:51 +00:00 Info Allow:
type=LOUT|proto=TCP|srcIF=dhcp|srcIP=10.0.0.4|srcPort=47542|srcMAC=00:0d:3a:4
6:14:a3|dstIP=168.63.129.16|dstPort=32526|dstService=|dstIF=|rule=PASSALL|inf

```
o=0|srcNAT=10.0.0.4|dstNAT=168.63.129.16|duration=0|count=1|receivedBytes=0|sentBytes=0|receivedPackets=0|sentPackets=0|user=|protocol=|application=|target=|content=|urlcat=
```

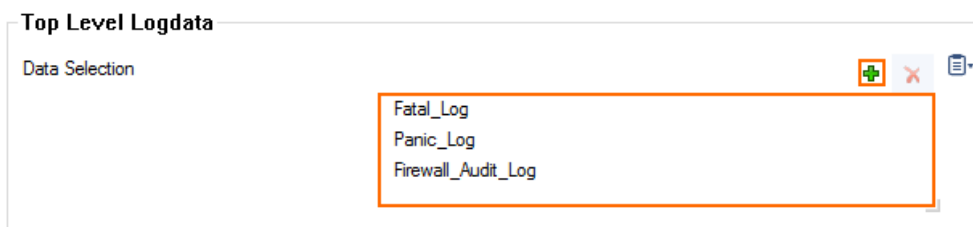
However, for streaming to OMS Security (i.e. logs in Common Event Format), the logs must be simple, pipe-separated values since parsing is done for this format.

```
Example output: 2024 05 07 10:02:57 +00:00 Info      Allow:
LOUT|TCP|dhcp|10.0.0.4|33848|00:0d:3a:46:14:a3|168.63.129.16|80|http||PASSALL
|0|10.0.0.4|168.63.129.16|0|1|0|0|0|0|||
```

Step 6. Configure Logdata Filters

Define profiles specifying the log file types to be transferred / streamed. Log files are classified into top level, box level, and service level log data sources.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Filters**.
3. Click **Lock**.
4. In the **Filters** table, click **+** to add a new filter. The **Filters** window opens.
5. Enter a **Name**.
6. Click **OK**.
7. In the **Data Selection** table, add the **Top Level Logdata** log files to be streamed. You can select:
 - **Fatal_log**
 - **Firewall_Audit_Log** – Data can be streamed as a part of the firewall service logs.
 - **Panic log**



8. Configure the **Affected Box Logdata** filters:
 1. From the **Data Selector** list, select which files for this category are streamed:
 - **All** – All box level logs are streamed.
 - **None** – Box level logs are not streamed.
 - **Selection** – Only box level log files defined in the **Data Selection** list are streamed.

Box Level Logfiles

Data Selector Selection

Data Selection

Name	Log Groups	Log Message Filter
DATA01	Cloud_awsconfigsyncd , ...	All

2. (**Selection** only) Click **+** to add custom filters to the **Data Selection** table.
 1. In the **Log Groups** table, click **+**.
 2. (only for Microsoft Azure Log Analytics and standard syslog streaming) From **Log Groups**, select the box level log files, or select **Other** to enter a **user defined log group pattern** to stream log files matching this pattern.
 3. (optional for logfile streaming using CEF) From **Log Groups**, select **Firewall-Activity-Only** and **Firewall-Threat-Only**.

Affected Box Logdata

Data Selector Selection

Data Selection

Name	Log Groups	Log Message Filter
DATA01	Firewall_Activity , Firewall_threat	All

4. (optional) From the **Log Message Filter** list, select the message types from the log group that is streamed.
5. (**Selection** only) In the **Selected Messages Types** table, click **+** to add message types.
6. Click **OK**.

Data Selection

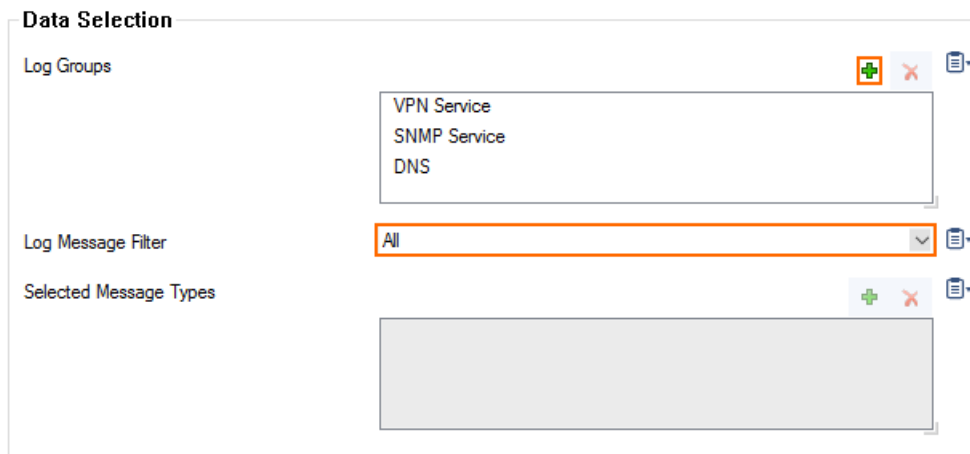
Log Groups

Log Message Filter All

Selected Message Types

9. Configure the **Affected Service Logdata** filters:
 1. From the **Data Selector** list, select which files for this category are streamed:
 - **All** – All service logs are streamed.

- **None** – Service level logs are not streamed.
 - **Selection** – Only service level log files defined in the **Data Selection** list are streamed.
2. (**Selection** only) Click **+** to add custom filters to the **Data Selection** table.
 1. In the **Log Groups** table, click **+**.
 2. Select the box level log files, or select **Other** to enter a **user defined log group pattern** to stream log files matching this pattern.
 3. (optional) From the **Log Message Filter** list, select the message types from the log group that are streamed.
 4. (**Selection** only) In the **Selected Messages Types** table, click **+** to add message types.
 5. Click **OK**.






10. Click **Send Changes** and **Activate**.

Step 7. Configure Azure Log Analytics as the Logstream Destination

Configure the firewall to send the syslog stream to Microsoft Azure Log Analytics.




1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logstream Destinations**.
3. Click **Lock**.
4. In the **Destinations** table, click **+** to add a new filter. The **Destinations** window opens.
5. Enter a **Name**.
6. Click **OK**.
7. (only for **Microsoft Azure Log Analytics** and standard syslog streaming) From the **Logstream Destination** list, select **Microsoft OMS**.

Destination Address

Logstream Destination	Microsoft OMS	
Destination IP Address		
Destination Port	5143	

8. (optional for logfile streaming using CEF) From the **Logstream Destination** list, select **Microsoft OMS Security**.

Destination Address

Logstream Destination	Microsoft OMS Security	
Destination IP Address		
Destination Port	5143	

9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Data sent to Log Analytics will show up under the **Syslog** tag in Azure Log Analytics. Data sent to Microsoft OMS Security can be found under **CommonSecurityLog**, which requires **Security and Audit** to be enabled in the workspace (select **Configure monitoring solutions** and search for the solution).

Step 8. Configure the Logdata Streams to Azure Log Analytics

Combine the logdata filters and logstream destination to a logdata stream.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Streams**.
3. Click **Lock**.
4. In the **Streams** table, click **+** to add a new syslog stream. The **Streams** window opens.
5. Enter a **Name**.
6. Click **OK**.
7. Set **Active Stream** to **yes**.
8. In the **Log Destinations** table, click **+** and select the logstream destination configured in Step 5.
9. In the **Log Filters** table, click **+** and select the logdata filter configured in Step 4. Choose either OMS or OMS Security as your log destination.

Stream Configuration

Active Stream

Log Destinations + - ⌵

OMS

Log Filters + - ⌵

FILT01

10. Click **OK**.
11. Click **Send Changes** and **Activate**.

All logs covered by the logdata filter are now streamed to Microsoft Azure Log Analytics. It might take some time for logs to be displayed in the Azure Log Analytics portal.

Figures

1. oms.png
2. az_log_01.png
3. az_log_02.png
4. oms_basics.png
5. pricing_tier.png
6. review.png
7. display_law.png
8. connect_vm.png
9. law_cgf_status.png
10. oms_08.png
11. log_pipe.png
12. oms_09.png
13. oms_10.png
14. conf_oms_sec.png
15. oms_11.png
16. oms_12.png
17. oms_13.png
18. select_dest_oms_security_via_cef.png
19. oms_14.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.