



# **Integration Guide**

## **ManagedMethods Cloud Access Monitor**

# About This Guide

---

## Guide Type

*Documented Integration* — WatchGuard or a Technology Partner has provided documentation demonstrating integration.

## Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

# ManagedMethods Cloud Access Monitor Integration Overview

---

ManagedMethods is a cloud access security provider that enables companies to monitor and control use of cloud applications and reduce cloud risk. ManagedMethods Cloud Access Monitor integrates with WatchGuard Firebox appliances to provide IT security teams with control and visibility into both network and cloud application use.

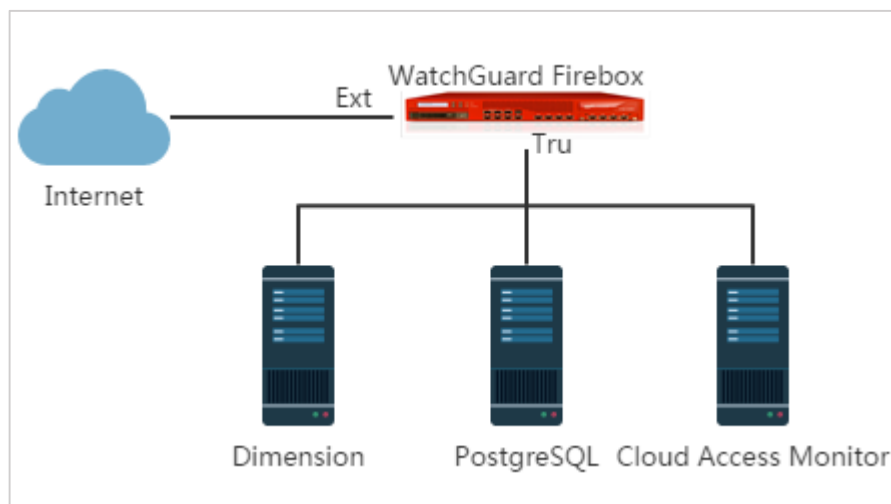
This document describes the steps to integrate Cloud Access Monitor with your WatchGuard Firebox.

## Platform and Software

The hardware and software used to complete the steps outlined in this document include:

- Firebox or WatchGuard XTM device installed with Fireware v11.10.2
- Cloud Access Monitor v7.1
- WatchGuard Dimension v2.1
- PostgreSQL version 9.5.3

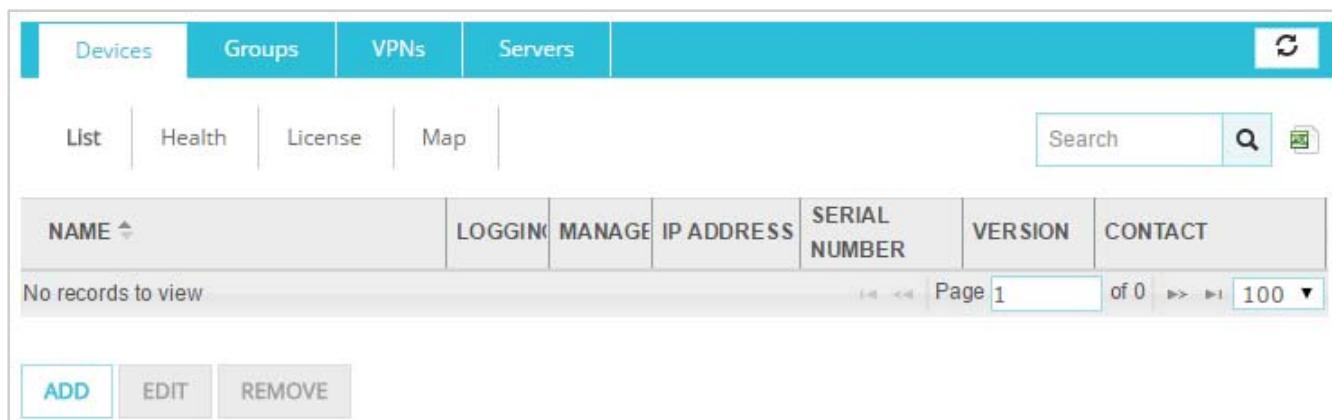
This diagram describes the integration environment:



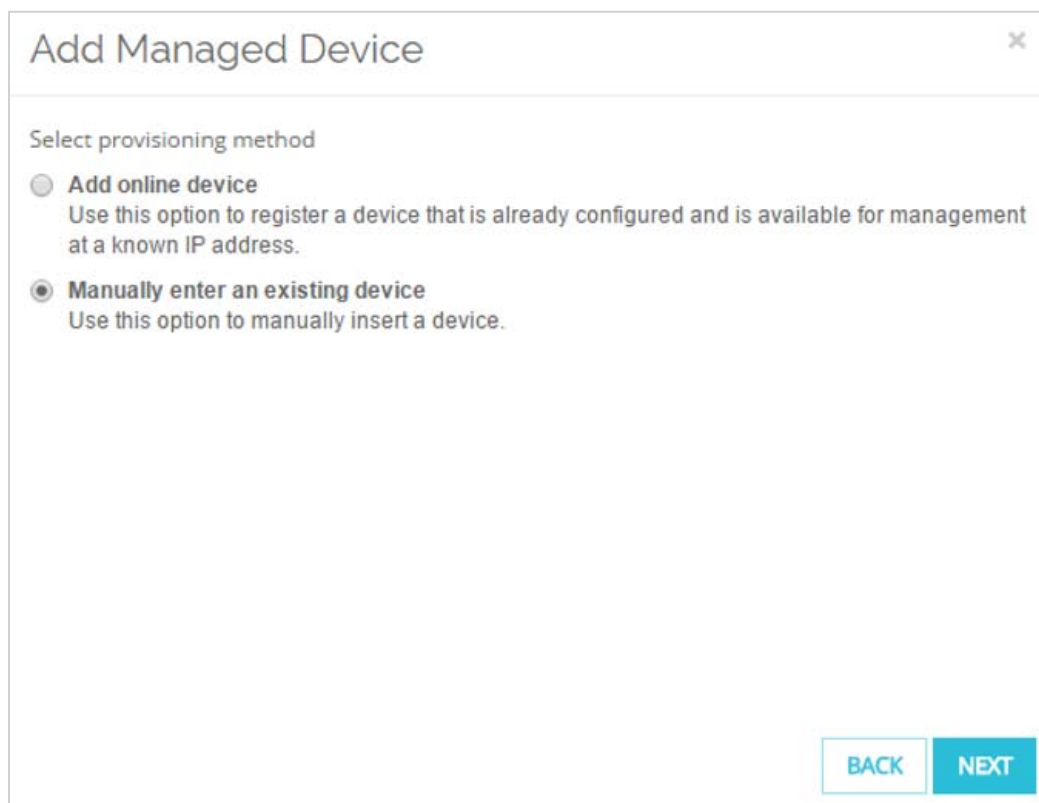
## Add a Firebox to Dimension

---

1. Log in to Dimension Web UI.  
*The Devices page appears with the List tab selected.*
2. Click **Add**.  
*The Add Managed Device wizard appears.*



3. Click **Next**.  
*The Select provisioning method page appears.*
4. Select **Manually enter an existing device**.



5. Click **Next**.
6. From the **Type** drop-down list, select **Single Device**.
7. In the **Device Name** text box, type a friendly name for this Firebox.
8. In the **Serial Number** text box, type the serial number for this Firebox.

## Add Managed Device ✕

Input the information for the single device or FireCluster to add to Dimension.

Type

Device Name  (Required)

Serial Number  (Required)

Enable logging

9. Click **Next**.

*The Firebox is added to Dimension as a managed device and the Download page appears.*

## Add Managed Device ✕

Your Firebox was successfully added to Dimension as a managed device.


To enable your device to connect to Dimension, you must download the management settings file and import it to the Firebox. The management settings file includes the logging and management settings for this Firebox.

10. To download the WGD file for the Firebox, click **Download** and select a location to save the file.  
*To complete the process, you must import the WGD file to the Firebox to manage the device with Dimension. For more information, see Fireware Help.*
11. Click **Finish**.  
*The Firebox appears in the Devices List, but is not yet connected to Dimension for logging or management.*
12. Connect to Fireware Web UI for the Firebox you just added to Dimension.
13. Select **System > Managed Device**.  
*The Managed Device page appears.*
14. Select the **Enable Centralized Management** check box.
15. From the **Manage Device With** drop-down list, select **Dimension Command**.

The screenshot displays the 'Managed Device' configuration page in the Fireware Web UI. On the left, a dark sidebar contains a navigation menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, SYSTEM, Information, Feature Key, NTP, SNMP, Managed Device (highlighted), Logging, Diagnostic Log, Global Settings, Certificates, Proxy Auto-Configuration, and Upgrade OS. The main content area is titled 'Managed Device' and includes the following elements:



- A heading: 'Managed Device'
- Instructional text: 'Configure these settings to make this device a Managed Device. You can specify an instance of Dimension Command or a Management Server.'
- A checked checkbox: 'Enable Centralized Management'
- A dropdown menu: 'Manage Device With' with 'Dimension Command' selected.
- Text: 'Import the Managed Device Settings for this device from a .wgd archive.'
- File selection area: 'Select a .wgd file' with a 'Choose File' button, 'No file chosen' text, and an 'IMPORT' button.
- Section: 'Dimension Command Address(es)' with an unchecked 'IP ADDRESS' radio button and an empty input field.
- Buttons: 'ADD' and 'REMOVE' buttons.
- Section: 'Dimension Command Port' with an input field containing '443'.
- Section: 'Dimension Command CA Certificate' with the text 'Select the Dimension Command CA certificate to import.'
- File selection area: 'Choose File' button, 'No file chosen' text, and an 'IMPORT' button.

16. Click **Choose File** and select the WGD file you downloaded for this Firebox from Dimension.
17. Click **Import**.  
*The management settings from the WGD file are imported to the Firebox, and the Logging and Managed status on the Device List page change to Yes.*


Devices			Groups	VPNs	Servers
List	Health	License	Map		
NAME	LOGGING	MANAGED			
 T30	Yes	Yes			
View 1 - 1 of 1					
<a href="#">ADD</a>	<a href="#">EDIT</a>	<a href="#">REMOVE</a>			

## Set Up the Dimension Database Location

---

1. Log in to Dimension with a user account that has Administrator credentials.
2. Select  > **Database**.  
*The Database page appears.*
3. Click **Configuration**.
4. To unlock the configuration so you can make changes, click .
5. Select **External PostgreSQL database**.
6. In the **Database Name** text box, type your database name.
7. In the **Host** text box, type IP address of the PostgreSQL database server.
8. In the **Port** text box, type the port used by the PostgreSQL database.
9. In the **Database User** text box, type the PostgreSQL Database user name.
10. In the **Passphrase** text box, type the PostgreSQL Database passphrase.
11. Click **Test Connection**. The message “Connection to database was successful” appears if the test is successful.

[Home](#) / [Database](#) [Status](#) | [Configuration](#) | [Diagnostics](#)

 *Click the lock to prevent further changes*

## Database Location

If you change the location of the Log Server database, the Log Server restarts.

Built-in database    External PostgreSQL database

Database Name:

Host:

Port:

Encryption:  ▼

Database User:

Passphrase:

Connection to database was successful.

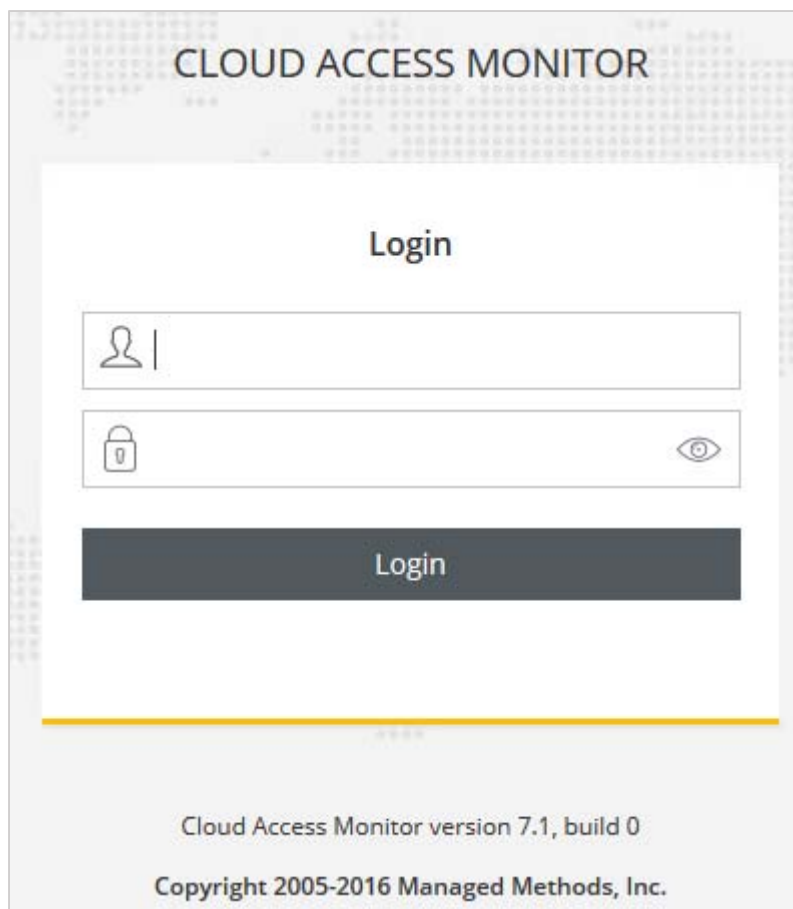
12. Click **Save**.

## Set Up Cloud Access Monitor

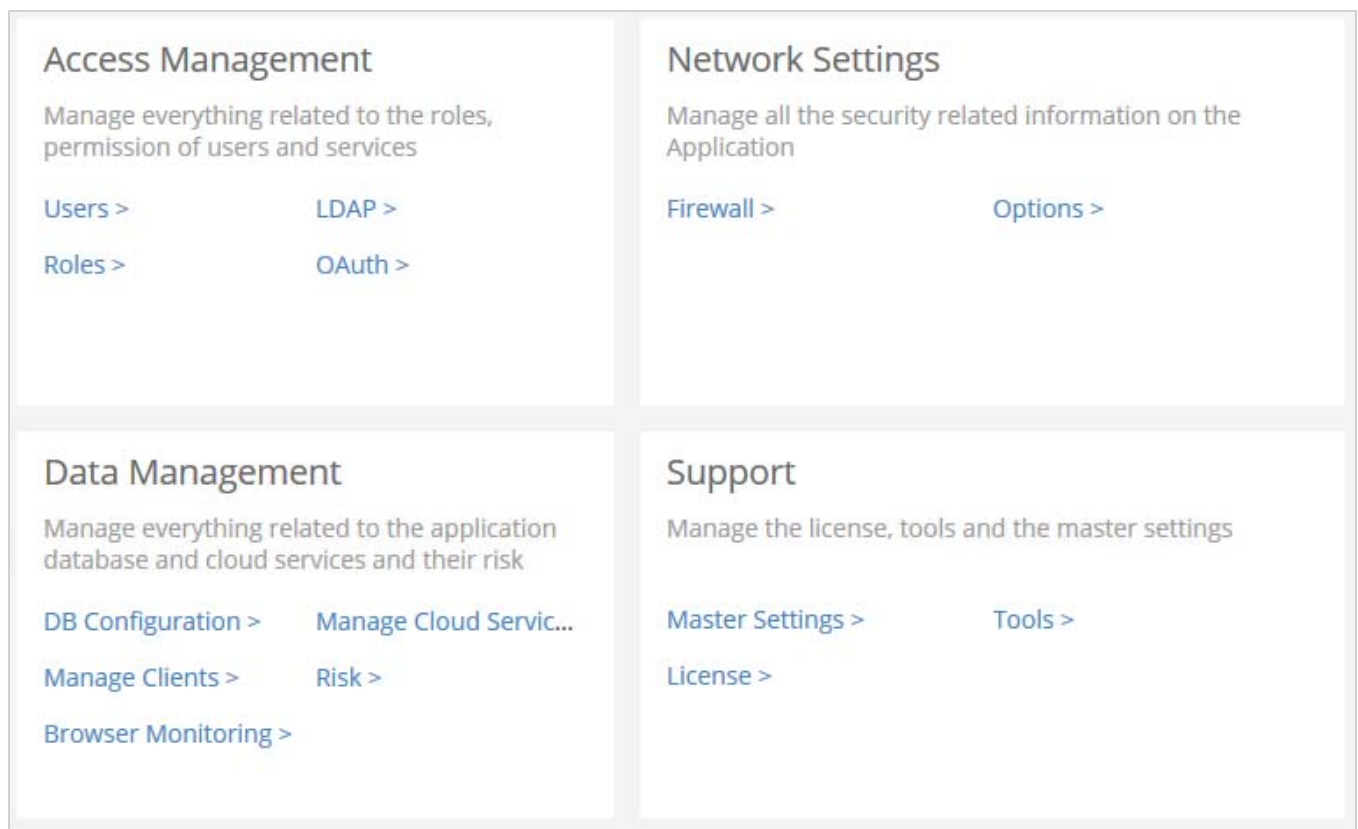
---

1. On the computer where Cloud Access Monitor is installed, go to <http://localhost:9090/Hubble/servlet/LoginServlet>.
2. Log in with user name and password.  
*The Overview page appears.*

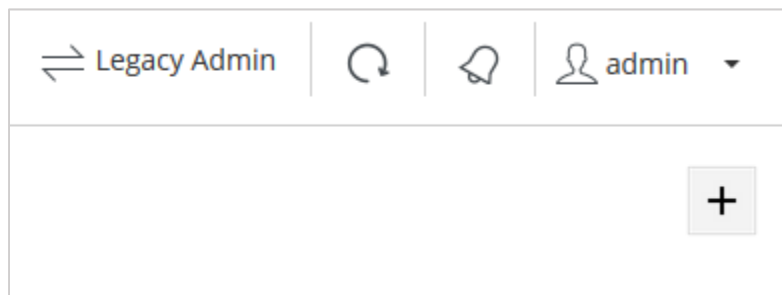




3. From the left navigation menu, select **Admin**.  
*The Admin page appears.*
4. Select **Firewall** in **Network Settings** window.



5. Select **+** at the top right to create a new firewall connection.



6. From the **Select a Firewall** drop-down list, select **WatchGuard Firewall**.
7. In the **Title** text box, type the Firebox name.
8. In the **Description** text box, type the Firebox description.
9. In the **Username** text box, type the Firebox user name.
10. In the **Password** text box, type the Firebox password.
11. In the **Firewall Address** text box, type the Firebox IP address.

### Add Firewall

Select a Firewall : WatchGuard Firewall ▼

**Basic Settings**

Title : WG-Firewall  
*A unique title for this object*

Description : WG-Firewall

Username : admin  
*Firewall Username (optional)*

Password : .....  
*Firewall Password (optional)*

---

**Firewall Settings**

Firewall Address : 10.0.1.33  
*The ip address for the Firewall apis.For ex:192.168.120.1*

12. Select the **Enable Log Reader** check box.
13. Select the **Enable DB Log Reader** check box.
14. In the **DB Driver** text box, type `org.postgresql.Driver`
15. In the **DB URL** text box, type `jdbc:postgresql://IP address:port/DBname`  
*The DB name is dimension if you configured PostgreSQL as the Dimension external database.*
16. In the **DB Username** text box, type the Database user name.
17. In the **DB Password** text box, type the Database password.

### Log Settings

<p>Log File : <input style="width: 90%;" type="text"/></p> <p><small>The path to the log file. This could be file path such as: empw.log or a URL such as: http://mywebsite.com/fw.log</small></p>	<p>Enable Logreader : <input checked="" type="checkbox"/></p> <p><small>Check this box to enable the log reader scheduler to run on the below period.</small></p> <p>Logreader Period : <span style="border: 1px solid #ccc; padding: 2px 5px;">24 hours</span></p> <p><small>Select the period to read the log.</small></p>
--	--

### DB Settings

<p>Enable DB Log Reader : <input checked="" type="checkbox"/></p> <p><small>Check this box to enable reading of logs from a database.</small></p> <p>DB Driver : <span style="border: 1px solid #ccc; padding: 2px 5px;">org.postgresql.Driver</span></p> <p><small>The jdbc driver for this database</small></p> <p>DB Username : <span style="border: 1px solid #ccc; padding: 2px 5px;">postgres</span></p> <p><small>The username for access to this database</small></p>	<p>DB Reader Frequency(sec) : <span style="border: 1px solid #ccc; padding: 2px 5px;">120</span></p> <p><small>The frequency in seconds to check the database for new logs</small></p> <p>DB URL : <span style="border: 1px solid #ccc; padding: 2px 5px;">jdbc:postgresql://10.0.1.1:5432/dimension</span></p> <p><small>The jdbc connection URL for this database</small></p> <p>DB Password : <span style="border: 1px solid #ccc; padding: 2px 5px;">.....</span></p> <p><small>The password for access to this database</small></p>
---	--

Save Cancel

18. Click **Save**.

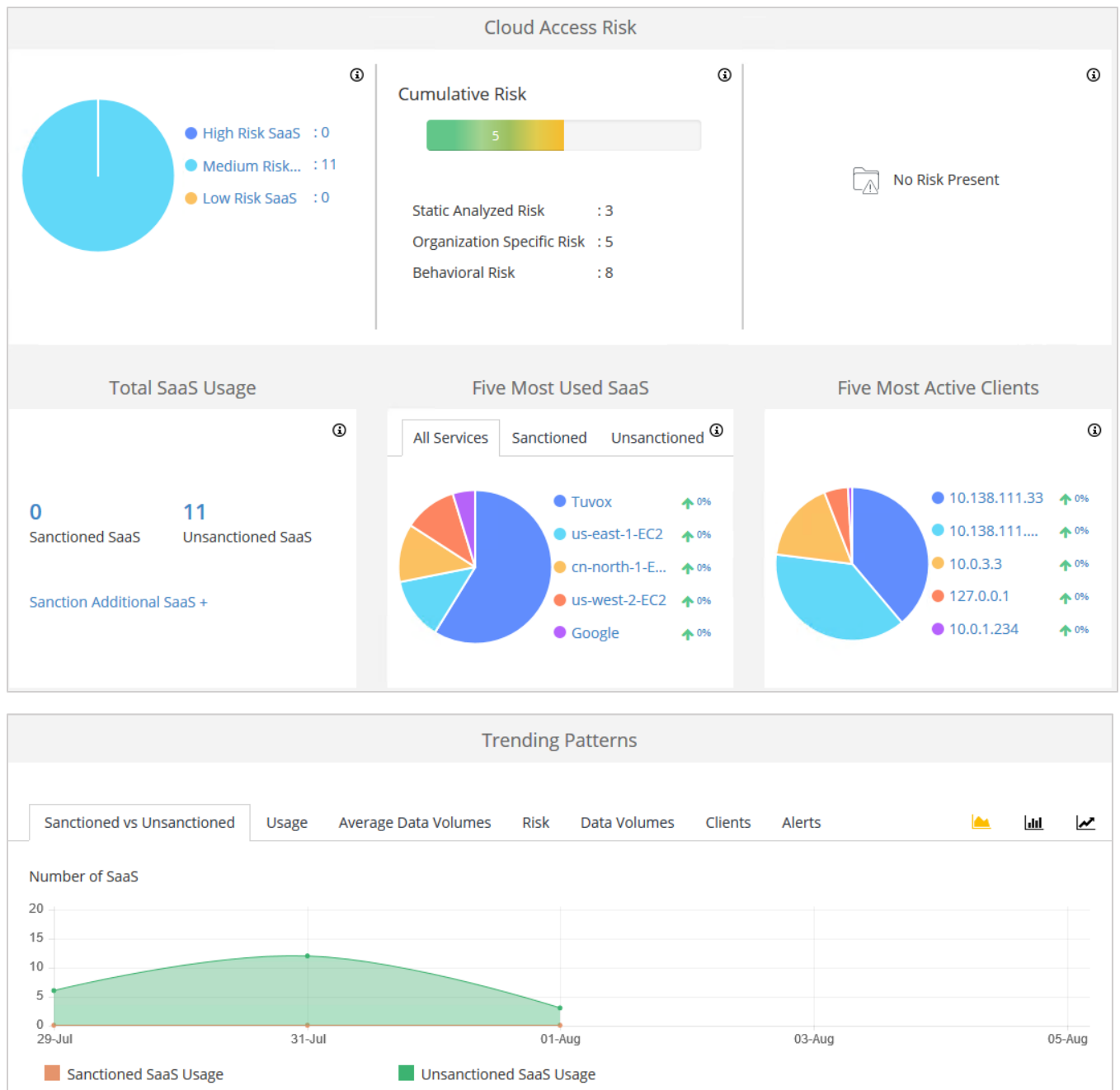
## Test the Integration

---

### Cloud Access Monitor Information Display

While traffic goes through the Firebox, Cloud Access Monitor discovers, records, and displays different types of information.

1. Log in to Cloud Access Monitor.
2. From the left navigation menu, select **Overview**.  
*The overview page appears.*



3. From the left navigation menu, select **Cloud Services**.  
The Cloud page appears.

Summary Alerts Risks

Cloud Services

Sanctioned SaaS Used : 0

Unsanctioned SaaS Used : 11

Total SaaS Discovered : 12

Most Active Clients

Total Active Clients : 8

0 Active 0 b Inbound 0 b Outbound

11 Active 11 Mb Inbound 10 Mb Outbound

O365

Canonical

us-west-2-EC2

[View More](#)

127.0.0.1

10.0.3.3

10.138.111.111

[View More](#)

Search Cloud Services

Filter Sort

Consulting (1)

Tuvox 1 x

Collaboration (2)

Google 2 x

O365 1 x

Cloud Infrastructure (6)

cn-north-1-EC2 2 x







us-west-2-EC2 4 x



us-east-1-EC2 2 x



Watchguard 3 x

- From the left navigation menu, select **Clients**.  
The Client page appears.

**Clients**

 <b>18</b> Total Clients	 <b>18</b> New Clients	 <b>8</b> Active Clients	 <b>8</b> Clients using Unsanctioned SaaS	 <b>0</b> Clients using Sanctioned SaaS	 <b>0</b> Clients with Sensitive Data
---	---	---	--	---	---































Search Client   

 Filter  Sort

Showing 1 to 18 of 18 entries

Select All


**All Clients** | New Clients | Clients using Sanctioned SaaS | Clients using Unsanctioned SaaS







10.0.3.7	0  0 	<input type="checkbox"/>	10.140.55.79	0  0 	<input type="checkbox"/>	10.211.9.232	0  0 
10.0.3.6	5  1 	<input type="checkbox"/>	10.0.1.234	12  0 	<input type="checkbox"/>	10.214.100.206	0  0 
10.215.71.118	0  0 	<input type="checkbox"/>	10.146.136.119	0  0 	<input type="checkbox"/>	10.0.1.33	0  0 
127.0.0.1	211  0 	<input type="checkbox"/>	10.138.111.111	42  0 	<input type="checkbox"/>	10.0.3.2	3  0 
10.0.3.5	0  0 	<input type="checkbox"/>	10.0.3.3	86  0 	<input type="checkbox"/>	10.0.3.1	0  0 



For more information, see the Cloud Access Monitor demo.


## Cloud Access Monitor Cloud Services and Clients Block







Cloud Services and Clients can be managed by Cloud Access Monitor.


1. From the left navigation menu, select **Cloud Services**.
2. On the **Summary** page, select a Cloud Service. In our example, we select WatchGuard.
3. Click the **Block CS**  button.













     

 Filter  Sort

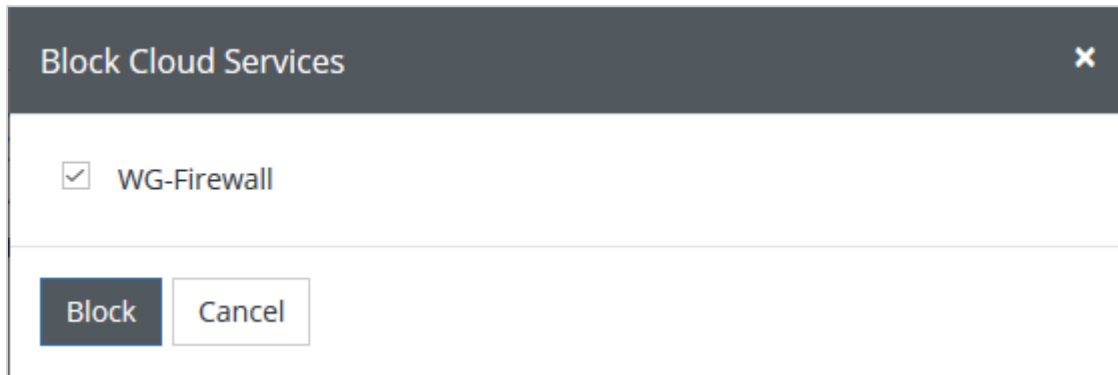
**Collaboration (2)** 

- Google 2 x   
- O365 1 x   

**Cloud Infrastructure (6)** 

- cn-north-1-EC2 2 x   
- us-west-2-EC2 4 x   
- us-east-1-EC2 2 x   
- Watchguard 3 x   

4. Select the Firebox you want to block.
5. Click **Block**.

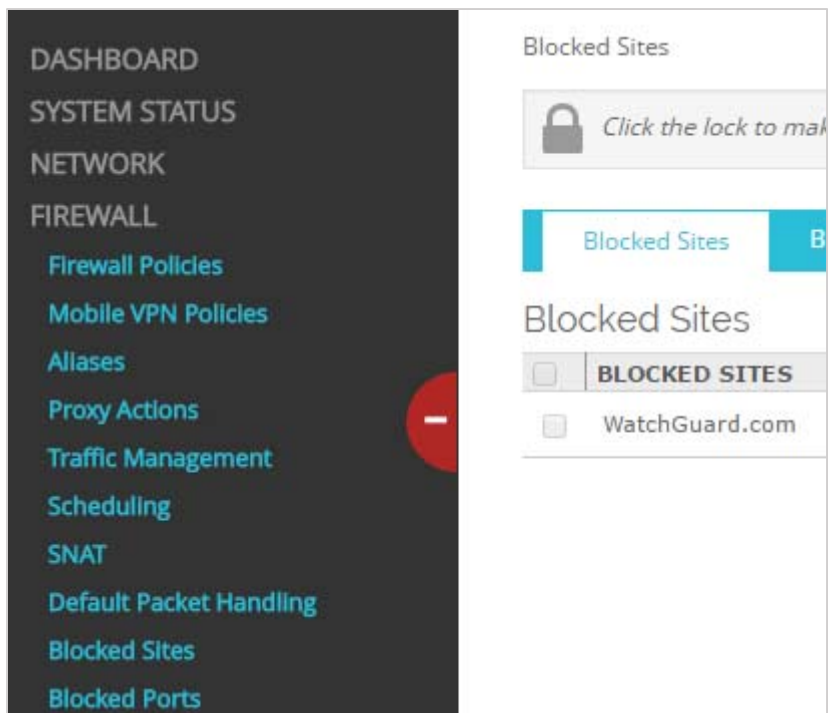


6. After the Block action completes, all WatchGuard traffic is blocked by the Firebox.



7. To see the blocked sites list created by Cloud Access Monitor, select **Firewall > Blocked Sites** in Fireware Web UI.






8. From the left navigation menu in Cloud Access Monitor, select **Clients**.
9. On the **Summary** page, select a client.  
*The information page for that client appears.*


# Clients

Summary Risks

## Clients



**18**  
Total Clients






**18**  
New Clients

🔍
🗑️

Active ✕
Clear All

All Clients
New Clients
Clients using Sanctioned Sa

Select All


<input type="checkbox"/>	10.0.3.6	5 
<input type="checkbox"/>	10.138.111.111	42 
<input type="checkbox"/>	10.138.111.33	8 

10. Click the **Block a client**  button on the client page.

10.0.3.6

Summary Risks

Clients > Internal > 10.0.3.\* > 10.0.3.6

	Client Name	: 10.0.3.6	Machine Name	:
	Email Address	: -	Machine Friendly Name	:
	Contact Name	:	Client IP	: 10.0.3.6
	Collector	: WIN-UU4TEU6JIQJ.yan.com	Device Type	:
	First Discovered	: Aug 3, 2016 2:07:51 PM		
	Last Seen	:		


11. Select the Firebox and Cloud Service to be blocked. In our example, we use WatchGuard.
12. Click **(Un)Block**.

### Block/Unblock Client : 10.0.3.6

**Selected services will be blocked / unblocked across the following selected firewalls:**

WG-Firewall

**Blocked Cloud Services (Deselect the cloud services to unblock)**

 No services are blocked

**Unblocked Cloud Services (Select the cloud services to block)**

<input type="checkbox"/> Canonical	<input type="checkbox"/> cn-north-1-EC2
<input type="checkbox"/> Google	<input type="checkbox"/> O365
<input type="checkbox"/> Tuvox	<input type="checkbox"/> us-east-1-AMAZON
<input type="checkbox"/> us-west-2-EC2	<input checked="" type="checkbox"/> Watchguard

**(Un)Block**

13. After the block command succeeds, all WatchGuard traffic from the selected client is blocked by the Firebox.
14. To see the policy created by Cloud Access Monitor, select **Firewall > Firewall Policies** in Fireware Web UI.

DASHBOARD

SYSTEM STATUS

NETWORK

FIREWALL

Firewall Policies

Mobile VPN Policies

Aliases

Proxy Actions

Policies



Click the lock to make changes

<input type="checkbox"/>	ORDER	ACTION	POLICY NAME	TYPE	FROM	TO	PORT
<input type="checkbox"/>	1	✗	<a href="#">mm_Watchguard_10.0.3.6</a>	Any	10.0.3.6	WatchGuard.com	Any
<input type="checkbox"/>	2	✓	<a href="#">FTP</a>	FTP	Any-Truste	Any-External	tcp:21