Integration Guide

ManagedMethods Cloud Access Monitor

Revised: 22 September 2016

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.

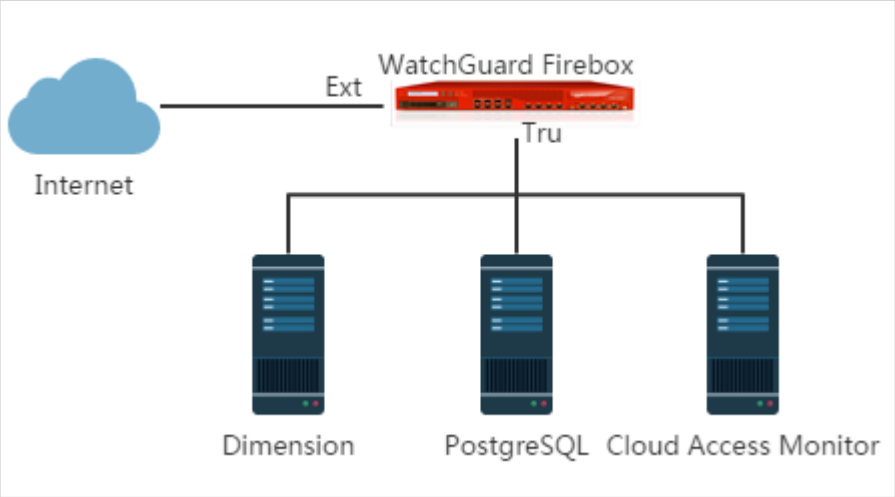
This document describes the steps to integrate Cloud Access Monitor with your WatchGuard Firebox.

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

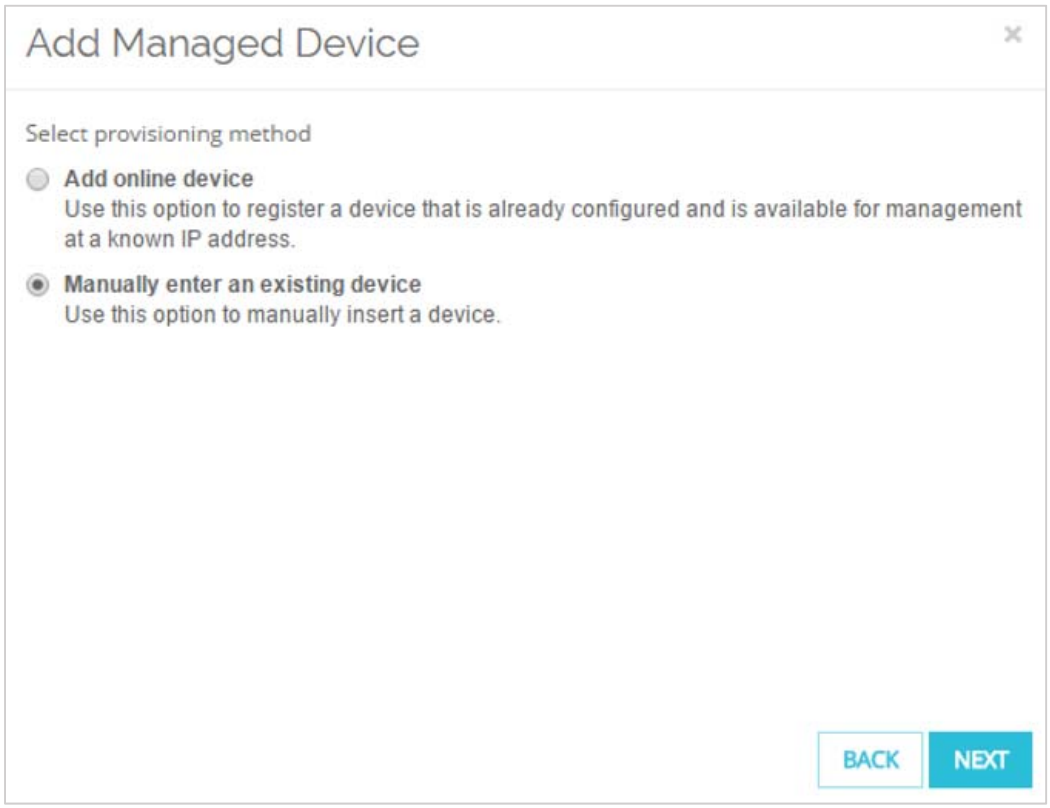
This diagram describes the integration environment:



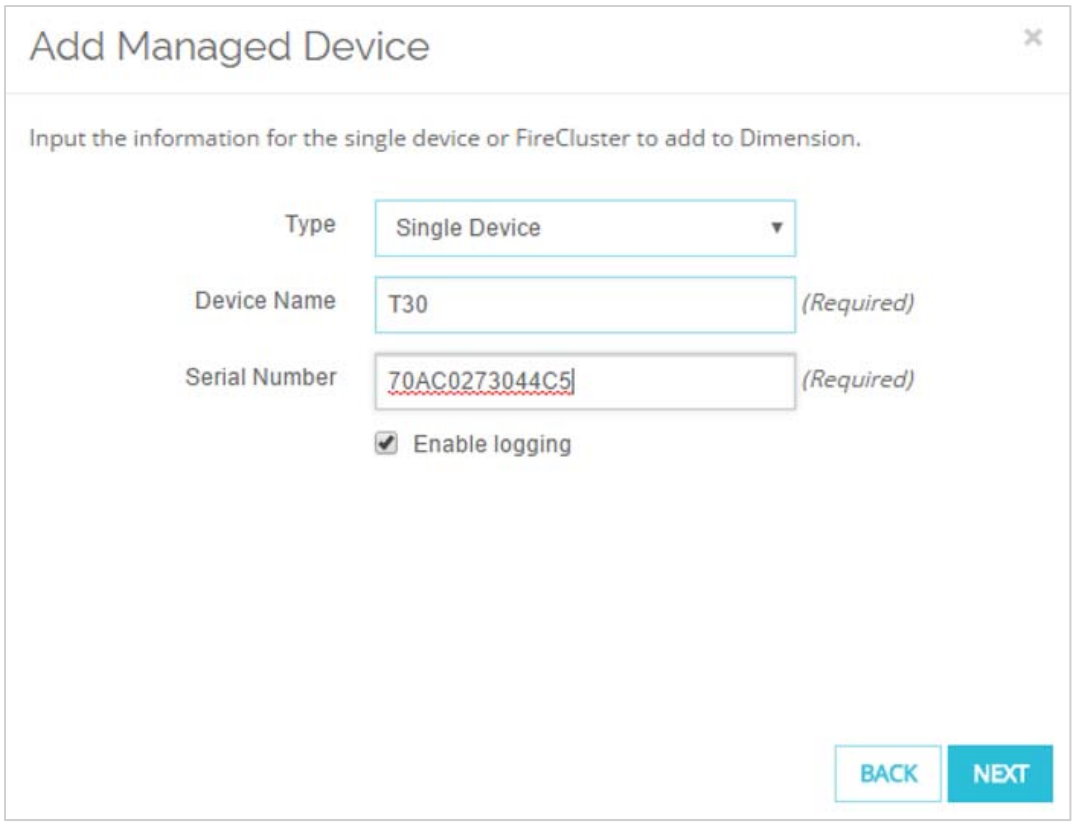
Add a Firebox to Dimension

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**.

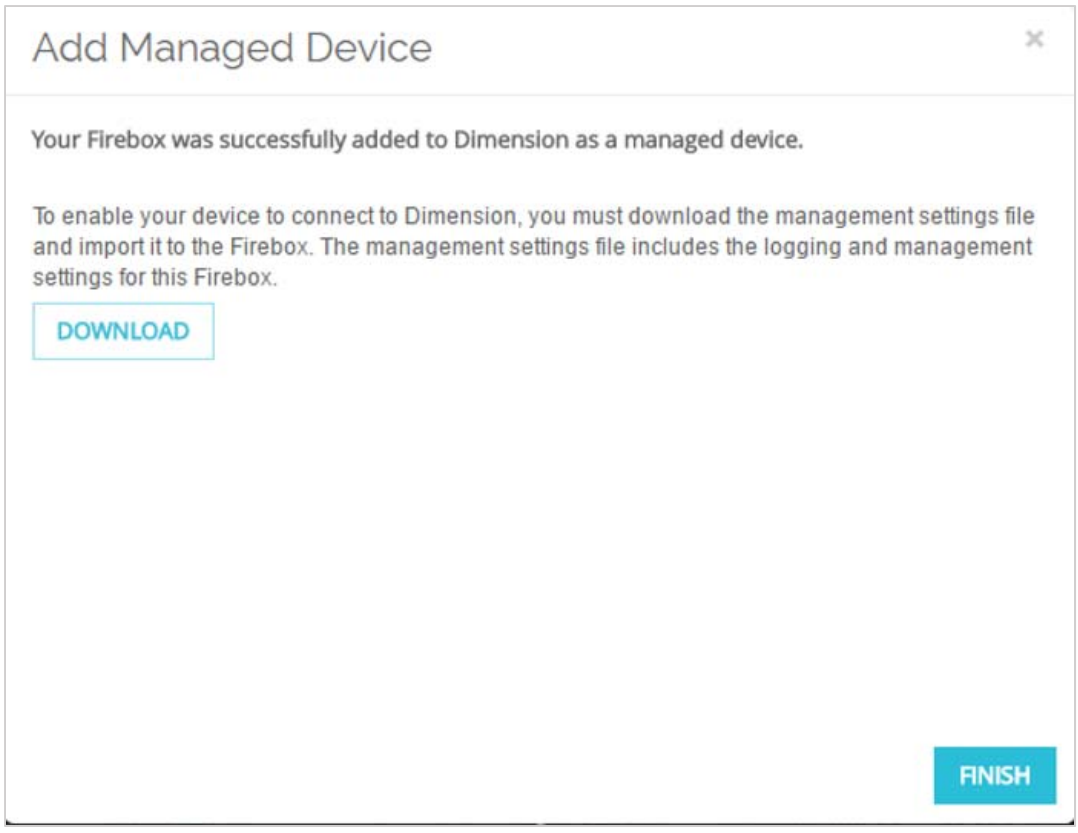


5. Click **Next**.
6. From the **Type** drop-down list, select **Single Device**.
7. In the **Device Name** text box, type a friendly name for this Firebox.
8. In the **Serial Number** text box, type the serial number for this Firebox.



9. Click **Next**.

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

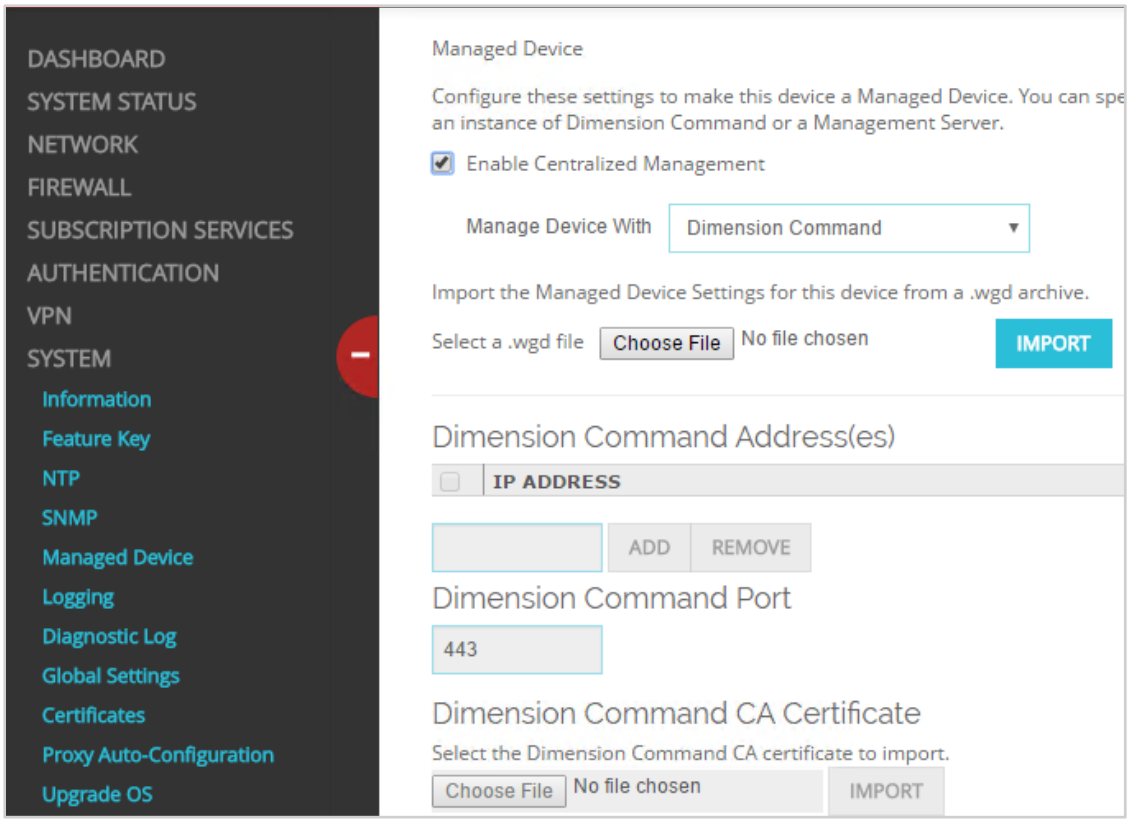


10. To download the WGD file for the Firebox, click **Download** and select a location to save the file.

    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**.

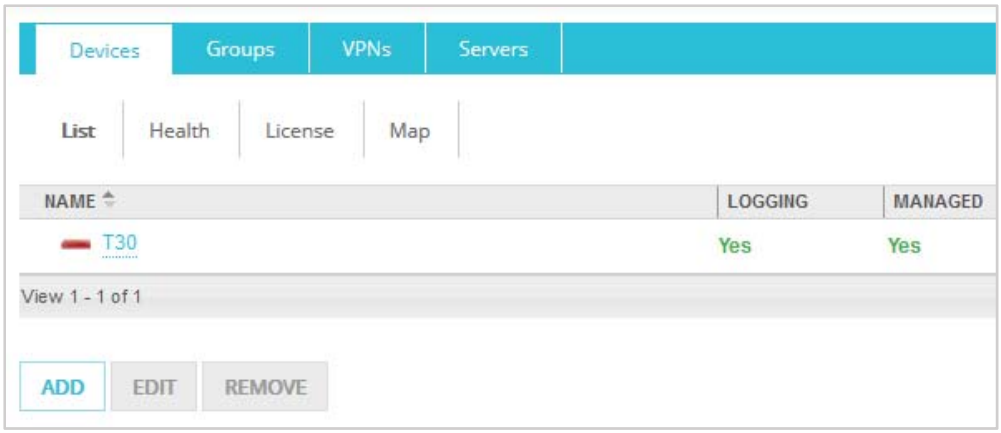
    The Firebox appears in the Devices List, but is not yet connected to Dimension for logging or management.
12. Connect to Fireware Web UI for the Firebox you just added to Dimension.
13. Select **System > Managed Device**.

    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**.



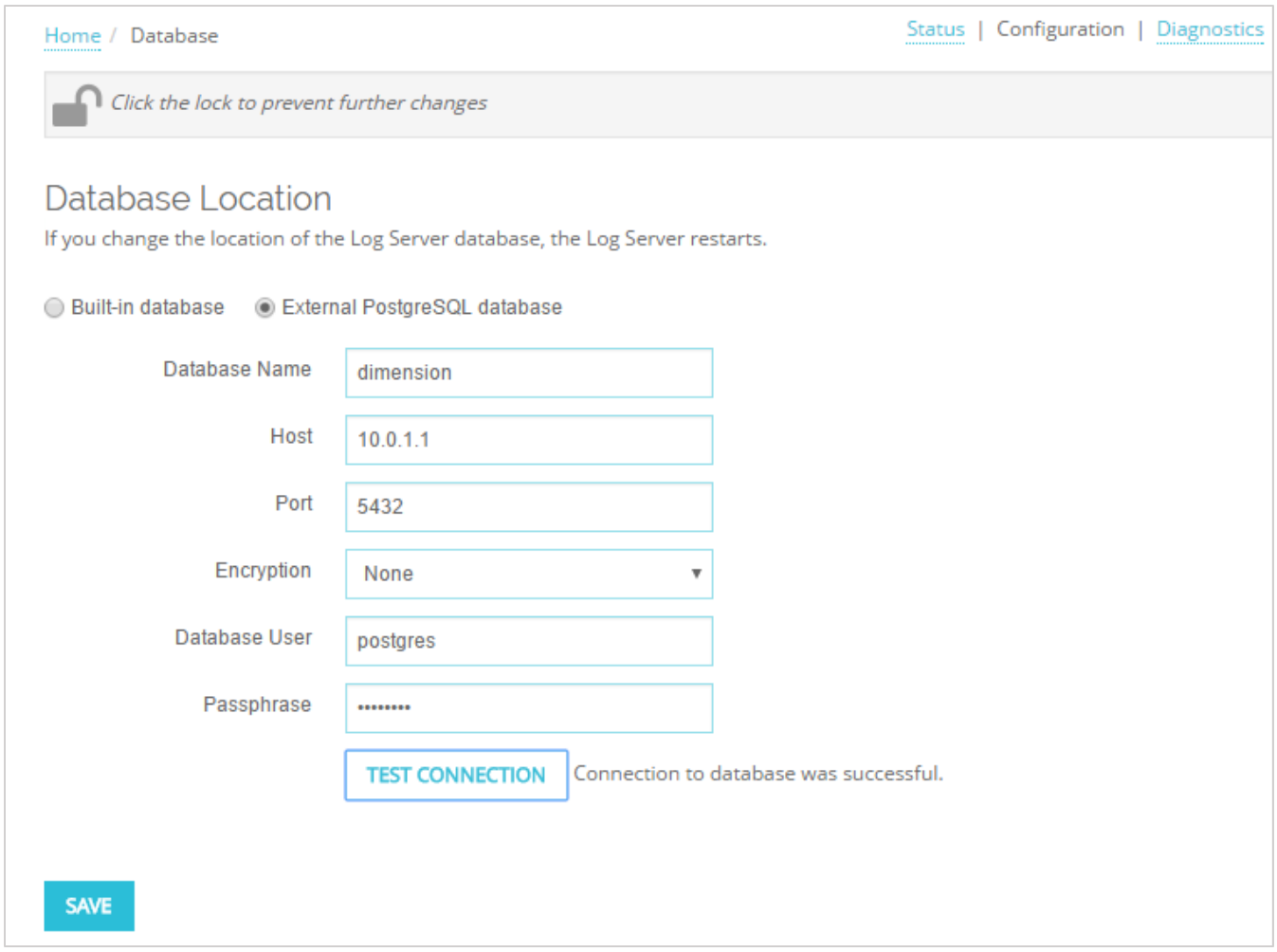
16. Click **Choose File** and select the WGD file you downloaded for this Firebox from Dimension.
17. Click **Import**.

    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.



Set Up the Dimension Database Location

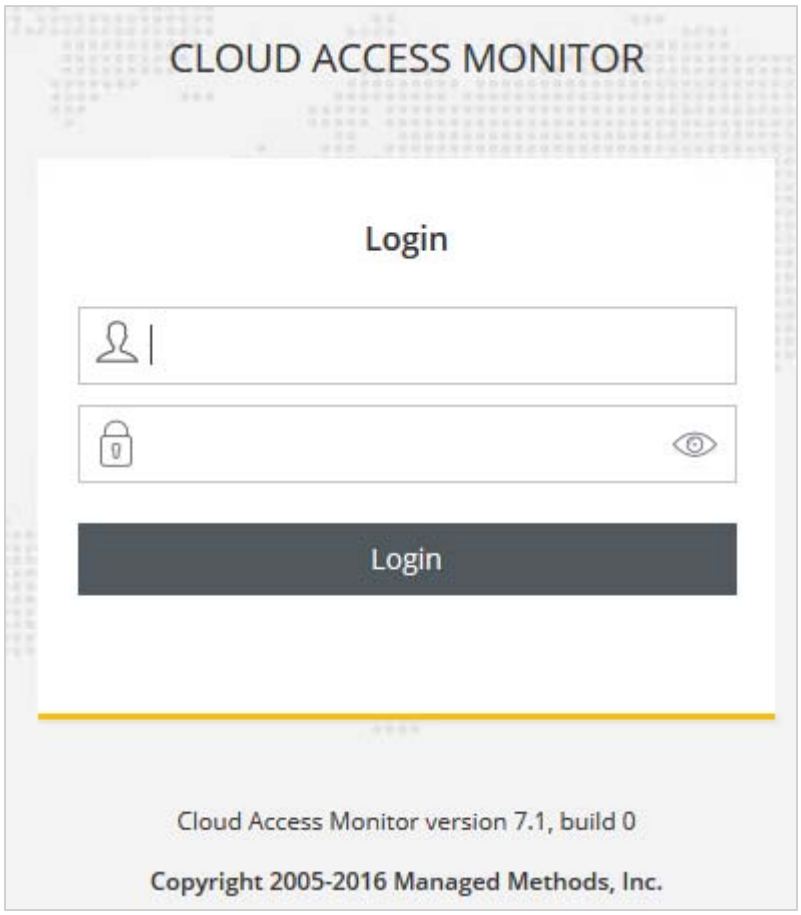
1. Log in to Dimension with a user account that has Administrator credentials.
2. Select ⚙ > **Database.**
   The Database page appears.
3. Click **Configuration**.
4. To unlock the configuration so you can make changes, click 🔒.
5. Select **External PostgreSQL database**.
6. In the **Database Name** 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.



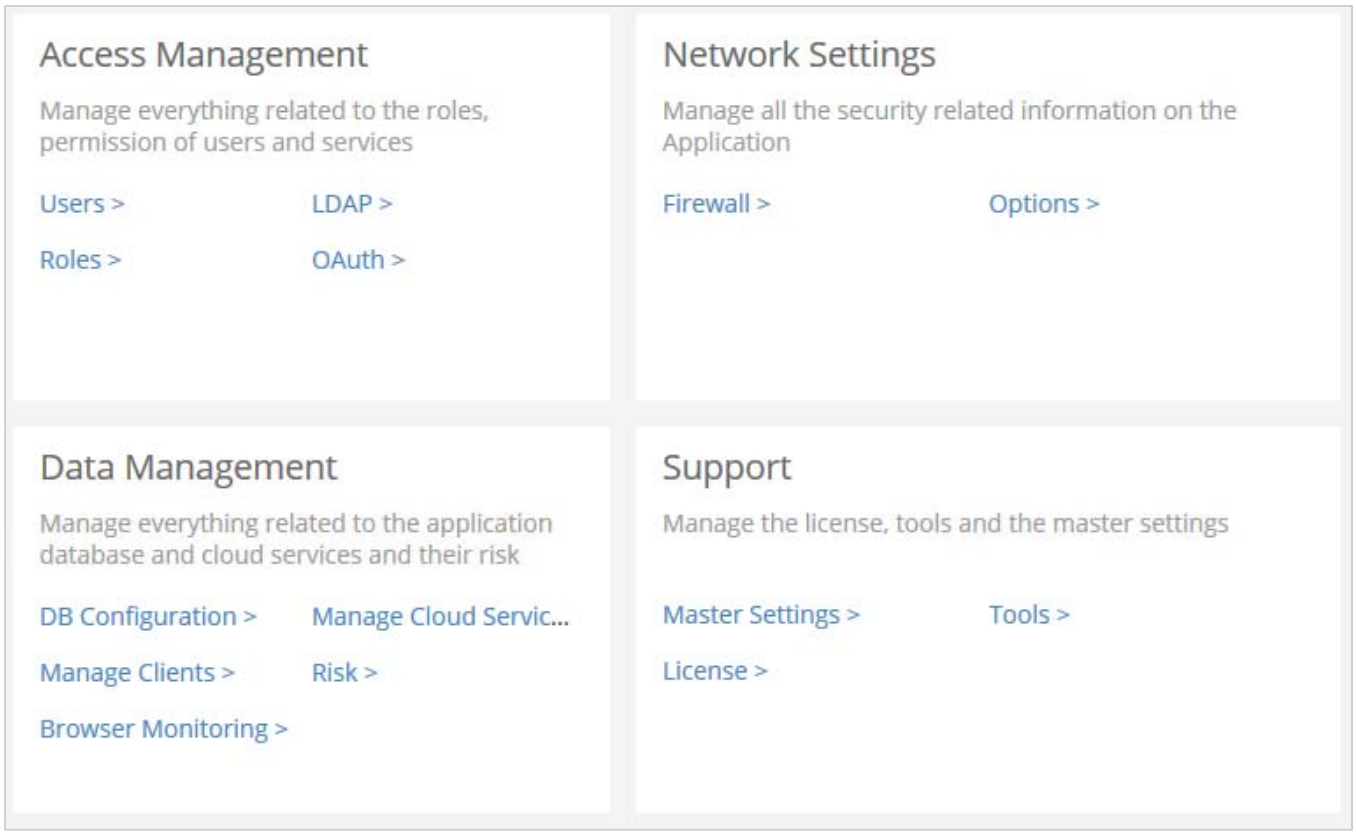
12. Click **Save.**

Set Up Cloud Access Monitor

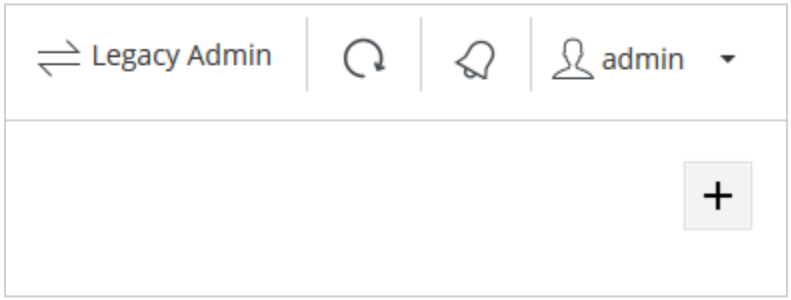
1. On the computer where Cloud Access Monitor is installed, go to http://localhost:9090/Hubble/servlet/LoginServlet.
2. Log in with user name and password.
   The Overview page appears.



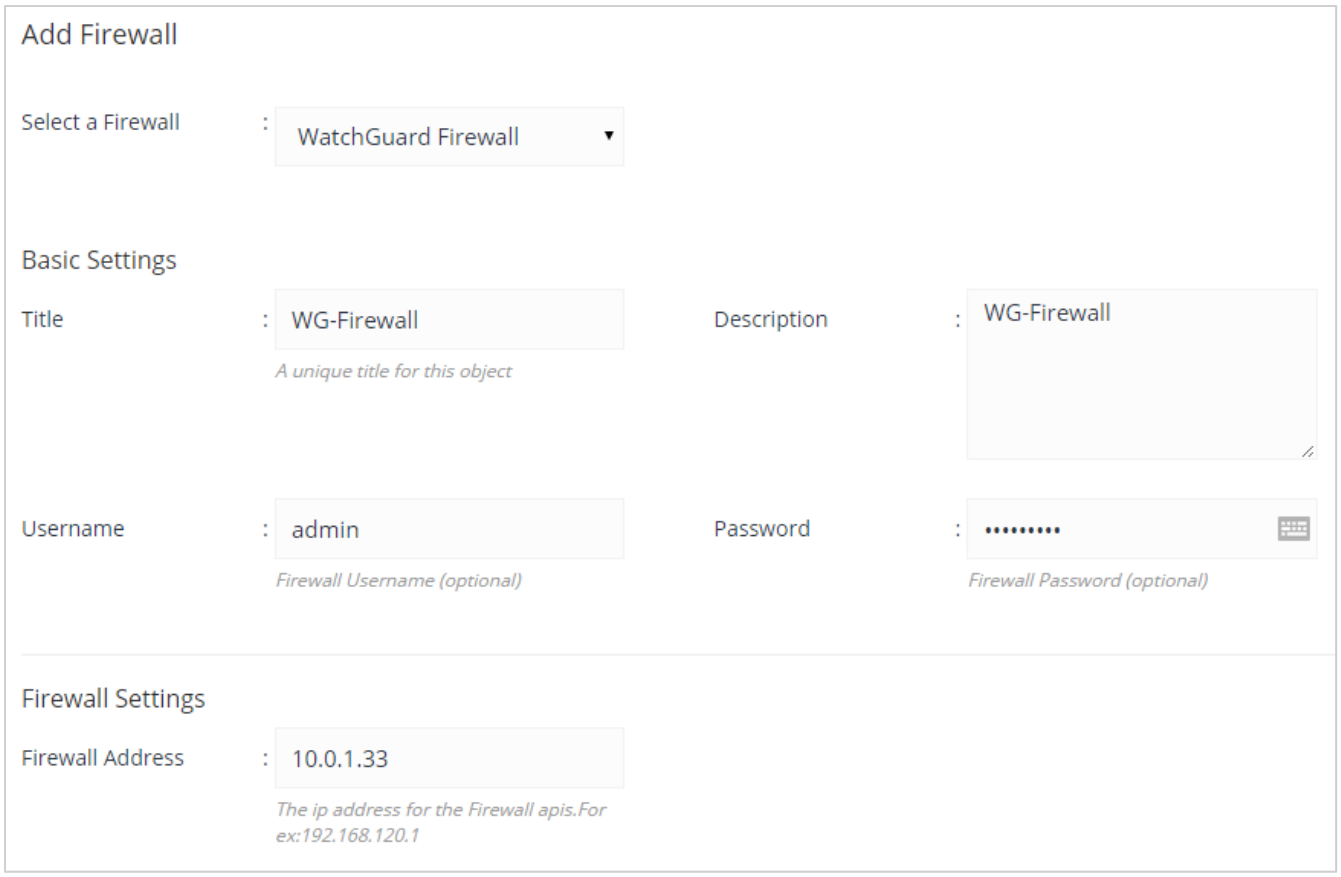
3. From the left navigation menu, select **Admin**.
   The Admin page appears.
4. Select **Firewall** in **Network Settings** window.



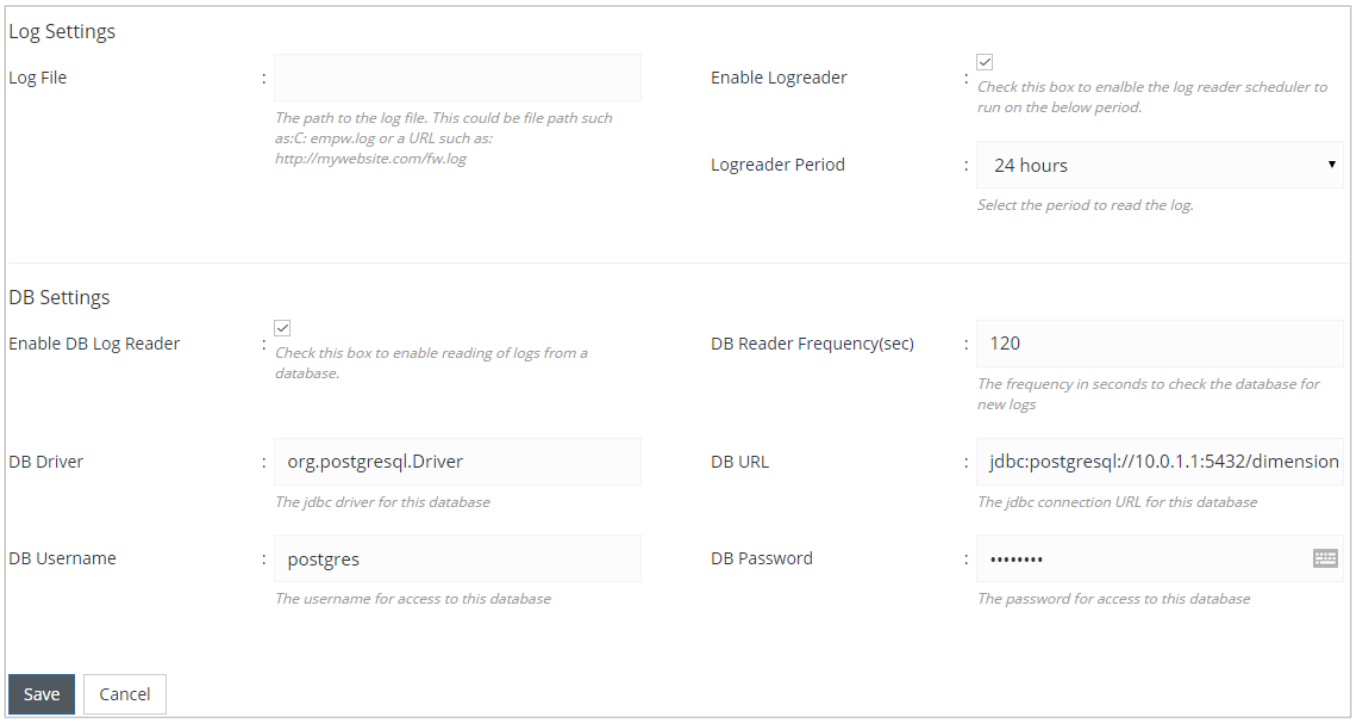
5. Select **+** at the top right to create a new firewall connection.



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.



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.



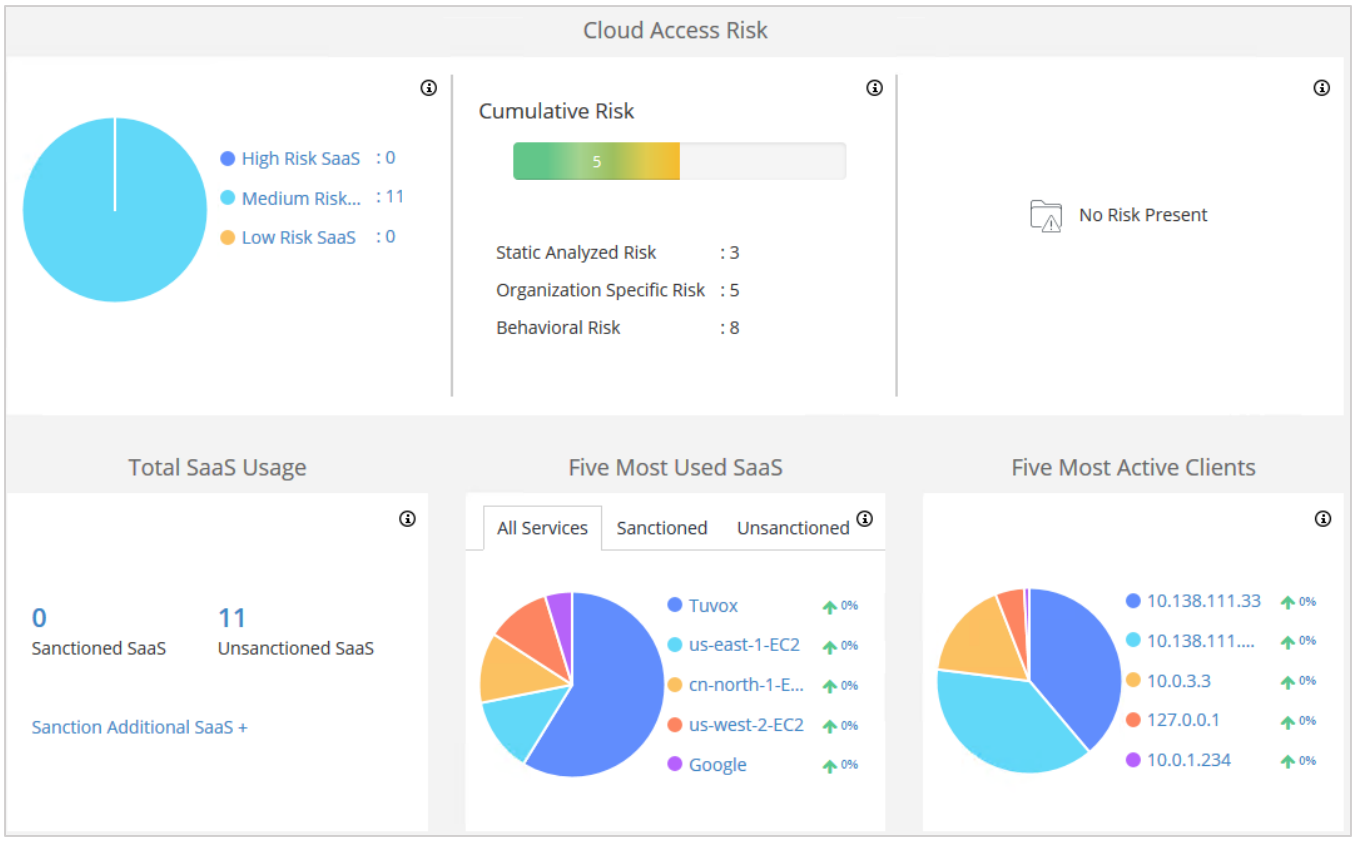
18. Click **Save.**

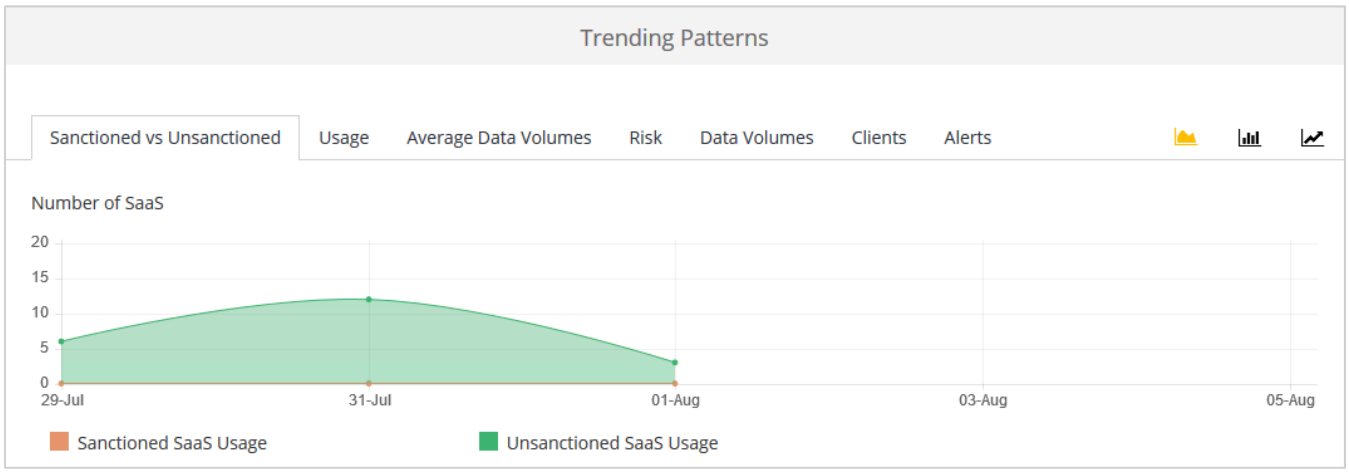
Test the Integration

Cloud Access Monitor Information Display

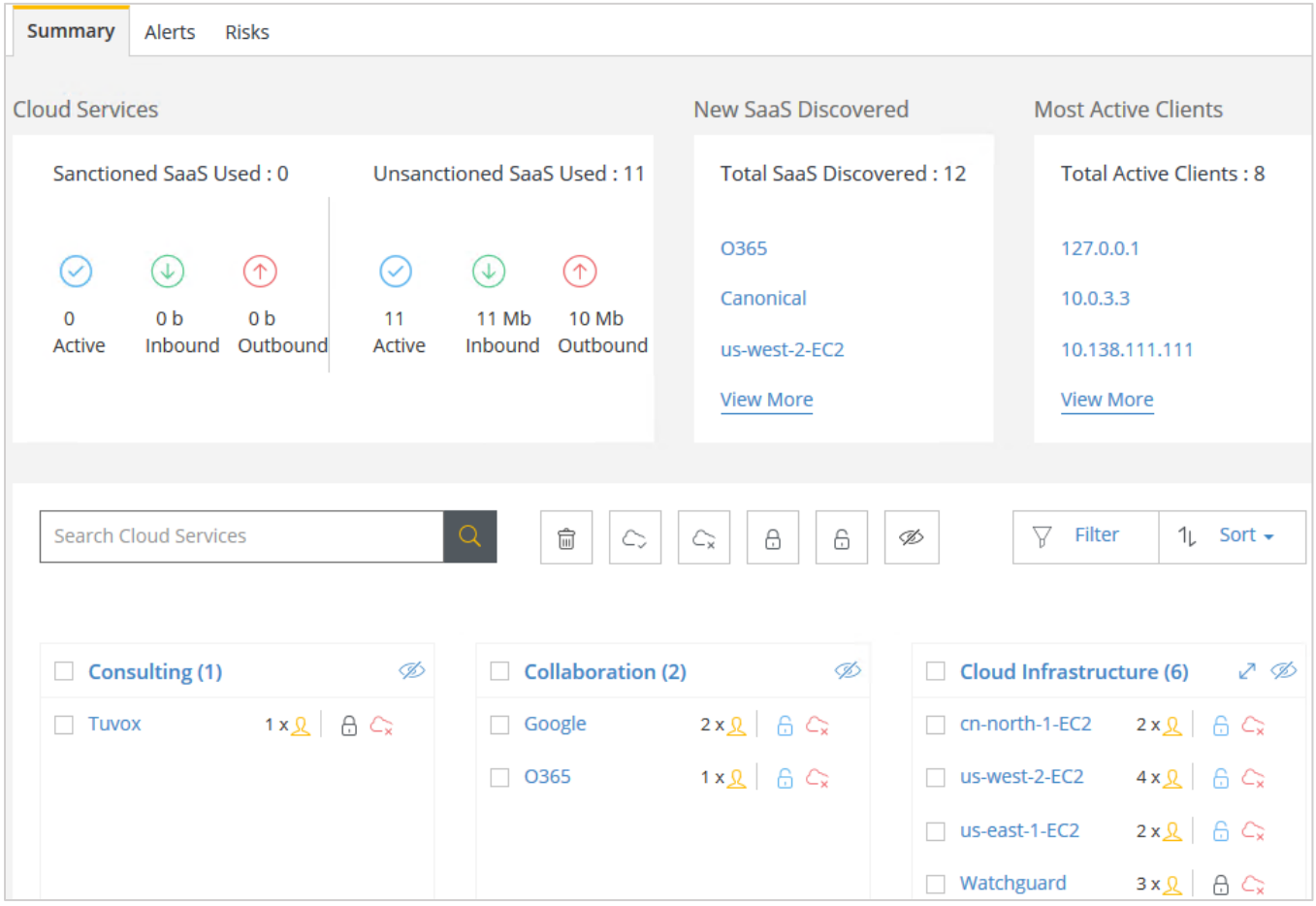
While traffic goes through the Firebox, Cloud Access Monitor discovers, records, and displays different types of information.

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

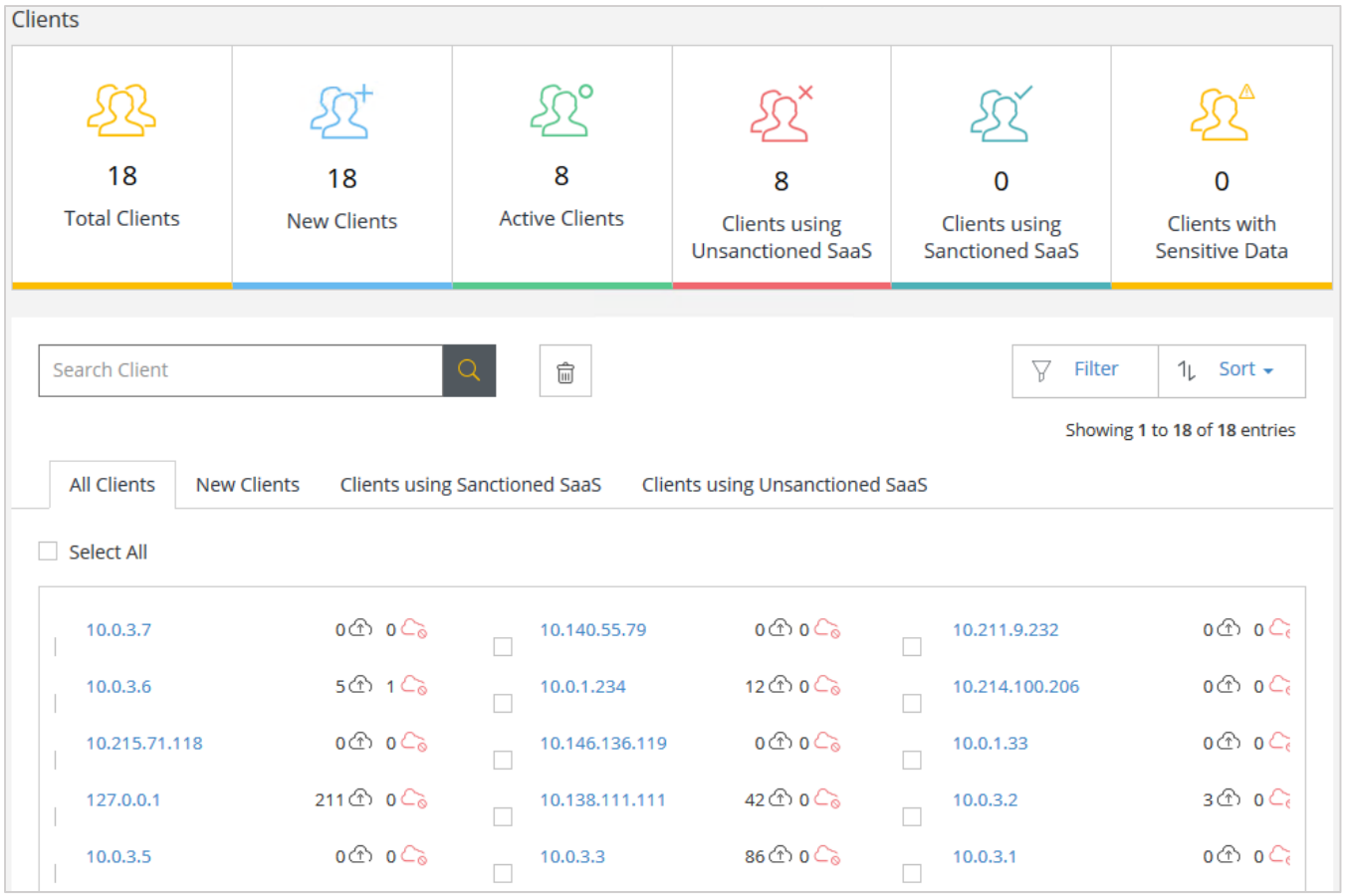




3. From the left navigation menu, select **Cloud Services.**
   The Cloud page appears.



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

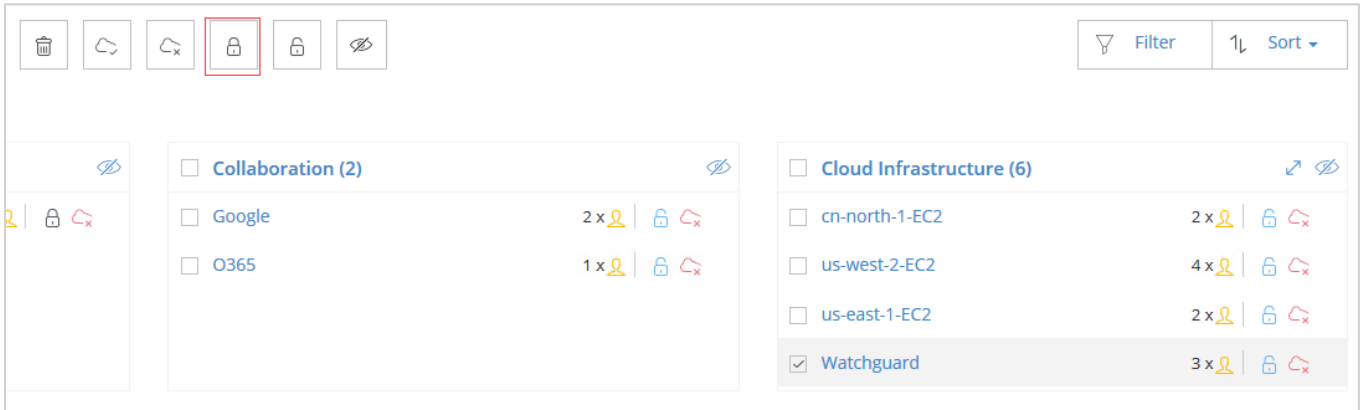


For more information, see the Cloud Access Monitor demo.

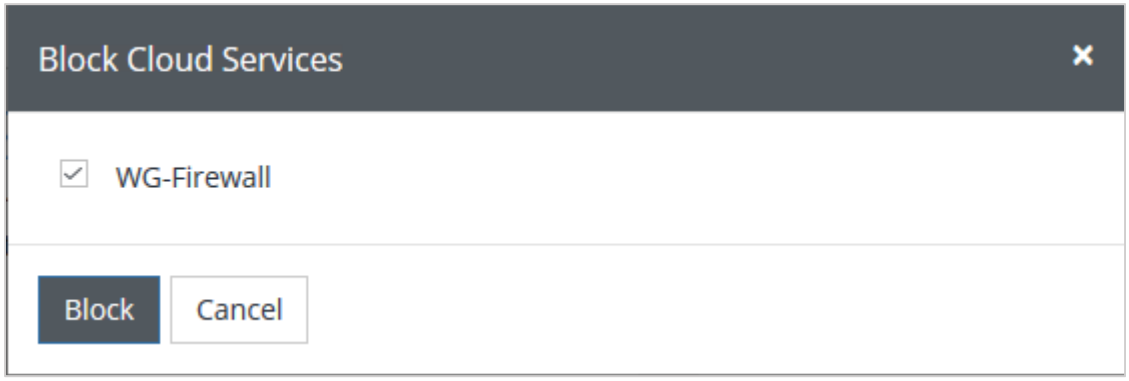
Cloud Access Monitor Cloud Services and Clients Block

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.

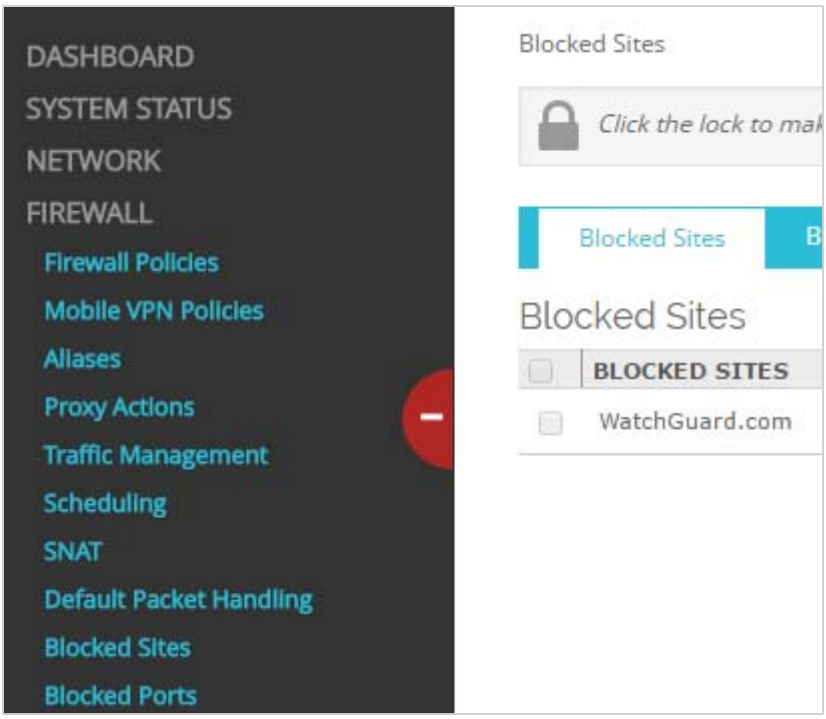


4. Select the Firebox you want to block.
5. Click **Block**.

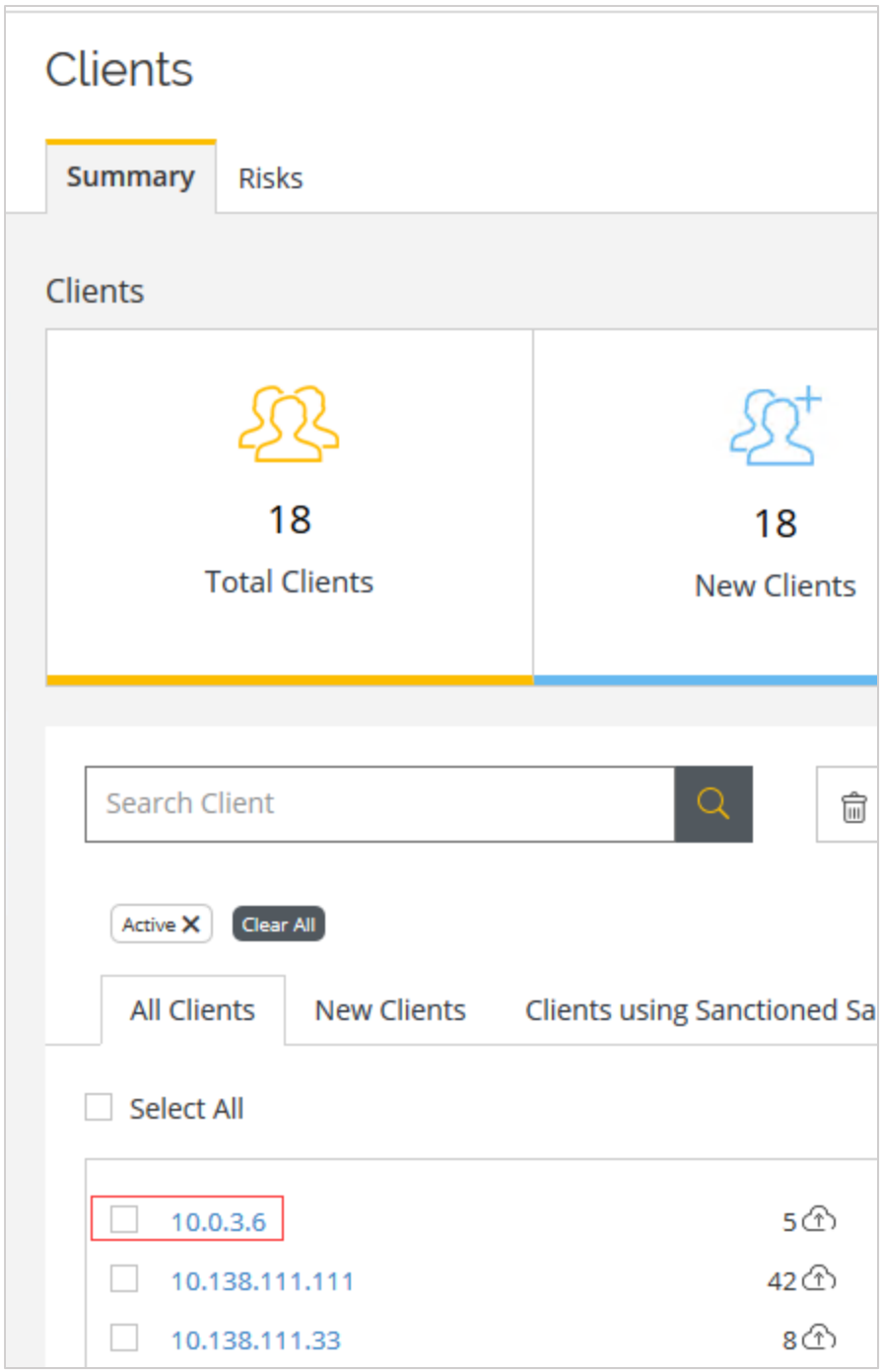


6. After the Block action completes, all WatchGuard traffic is blocked by the Firebox.

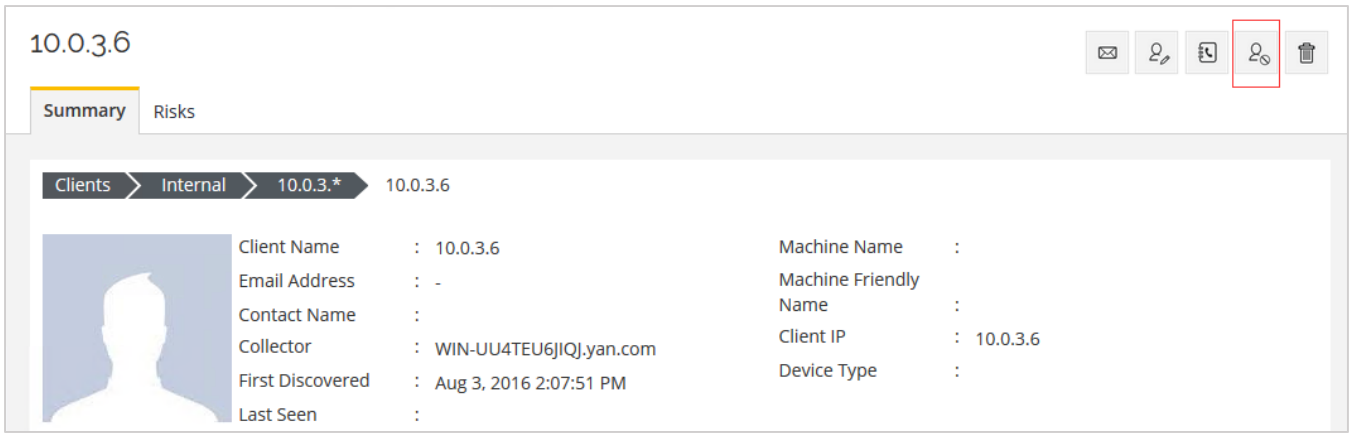
7. To see the blocked sites list created by Cloud Access Monitor, select **Firewall > Blocked Sites** in Fireware Web UI.



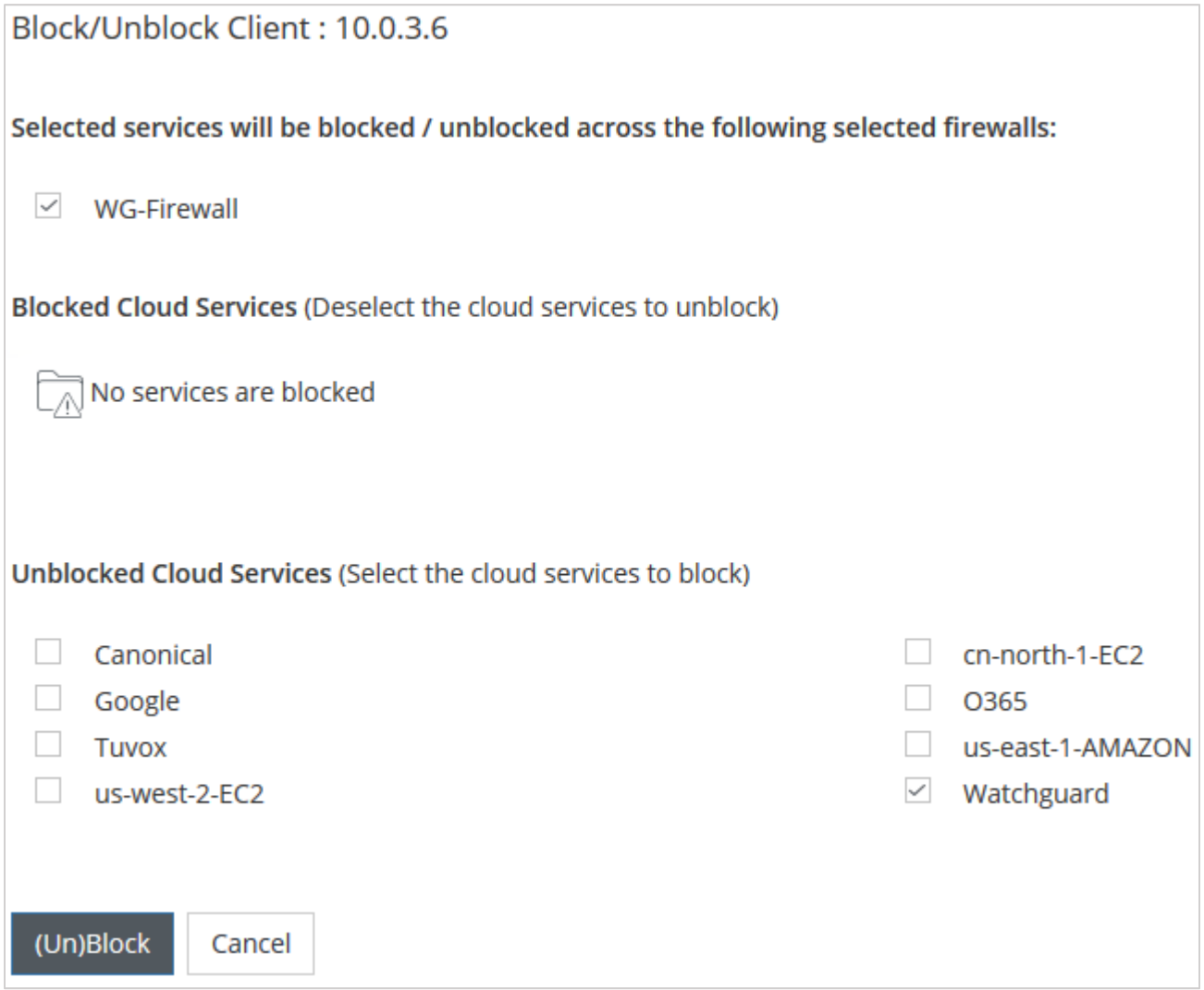
8. From the left navigation menu in Cloud Access Monitor, select **Clients.**
9. On the **Summary** page, select a client.
   The information page for that client appears.



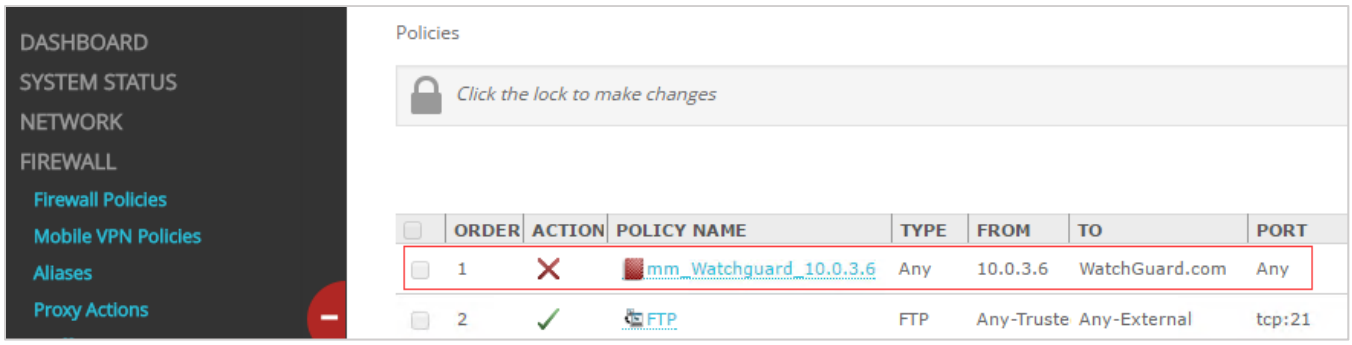
10. Click the **Block a client** button on the client page.



11. Select the Firebox and Cloud Service to be blocked. In our example, we use WatchGuard.
12. Click **(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
ORDER
ACTION
POLICY NAME
TYPE
FROM
TO
PORT
1
mm_Watchguard_10.0.3.6
Any
10.0.3.6
WatchGuard.com
Any
2
FTP
FTP
Any-Truste
Any-External
tcp:21