



FORUM SENTRY™ VERSION 9

CLOUD POLICIES GUIDE

Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™ Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Cloud Policies Guide, published May 2024.

D-ASF-SE-01903

Table of Contents

INTRODUCTION TO THE CLOUD POLICIES GUIDE	1
Conventions Used	1
Cloud Policies Referenced in the Cloud Guide	1
CLOUD POLICIES OVERVIEW.....	2
CLOUD IAAS PROVIDER: Amazon EC2	2
Cloud Policies	2
Retrieve Access Credentials from Amazon EC2	3
Insert Access Credentials in Forum Sentry	3
Configure Amazon EC2 Management from Sentry	4
Term Details: Amazon EC2 Management from Sentry	4
Configure Network Policies for Cloud Management.....	5
CLOUD IAAS PROVIDER: GoGrid.....	7
Cloud Policies	7
Retrieve Access Credentials from GoGrid.....	7
Configure GoGrid Management from Sentry.....	8
Term Details: GoGrid Management from Sentry.....	9
Configure Network Policies for Cloud Management.....	10

INTRODUCTION TO THE CLOUD POLICIES GUIDE

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: *********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section. For using the Cloud Policies Guide, you should have the Cloud Policies appear under the SUPPORTED FEATURES.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

Cloud Policies Referenced in the Cloud Guide

The Cloud Policies screen displays policies and settings for a variety of IaaS provider that are directly managed by Forum Sentry via calling IaaS APIs natively integrated in the Sentry product. You may create, edit, delete, enable and disable Cloud Policies.

CLOUD POLICIES OVERVIEW

The Cloud policies screen manages Cloud policies, their settings and status in the system. It enables users to set the parameters required for interacting with various IaaS providers such as Amazon EC2, GoGrid. Other providers with WSDL APIs can rapidly be added when required. The function of cloud policies is to instantiate pre-packaged images as the traffic requirements increase. As shown in Figure 1 below, Cloud Policies also enable setting up images of multiple cloud providers simultaneously for failover and load-balancing capabilities.

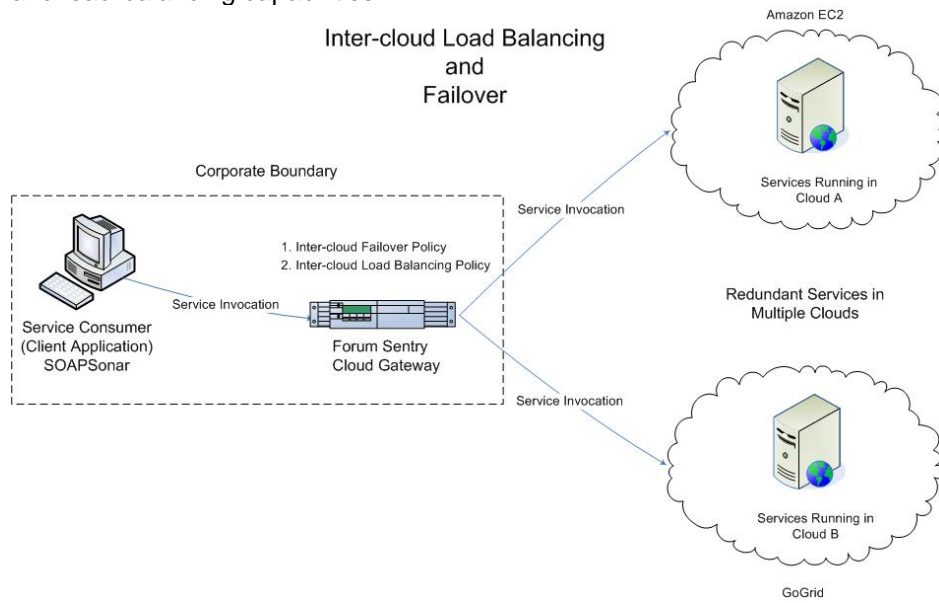


Figure 1: Inter-cloud load balancing and failover.

CLOUD IAAS PROVIDER: Amazon EC2

In this section, we will set up Forum Sentry's interaction with Amazon Elastic Cloud Computing (Amazon EC2) infrastructure.

Cloud Policies

Cloud policies can easily be setup by instantiating images on IaaS providers. The sequence for creating a cloud policy is as follows:

From the Gateway Policies, select Cloud Policies and click on New to start creating a new policy as shown in the screen below.

CLOUD POLICIES					
<input type="checkbox"/>	POLICY NAME	STATUS	TYPE	IMAGE ID	SERVERS
<input type="checkbox"/>	Cloud_Policy	●	Amazon EC2	ami-d08f6ab9 (auto-spawn-agent-v4/image.manifest.xml)	0/1
<div>DeleteEnableDisableNew</div>					

Retrieve Access Credentials from Amazon EC2

The next step requires acquiring credentials from your IaaS provider so that Forum Sentry can interact with the IaaS management API. For Amazon EC2, the credentials are available once an account has been set up. After registering with Amazon EC2, select your account name on at the top of the screen and on the drop-down go to My Security Credentials. Next expand the section labeled Access keys. Once here you can create a new Access Key for use with Forum Sentry. Be sure to record both the Access Key ID and the Secret Access Key. This information will be used in the Cloud Policy setup in Sentry to enable interaction between Sentry and Amazon EC2 management API.

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

+	Password
+	Multi-factor authentication (MFA)
-	Access keys (access key ID and secret access key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
---------	---------	---------------	-----------	------------------	-------------------	--------	---------

Insert Access Credentials in Forum Sentry

Insert **Access ID** in the API Key Field and **Secret Access Key** in the API Secret Field for the new Cloud Policy screen as shown below. Click Next.

CLOUD POLICIES > CLOUD POLICY CONFIGURATION

CLOUD POLICY

Policy Name*:

Type: ☒ Amazon EC2 ☐ GoGrid ☐ RackSpace ☐ OpSource ☐ Azure

API Key*:

API Secret*:

[Next](#)

Configure Amazon EC2 Management from Sentry

On successful authentication to Amazon EC2, the following Configuration screen is presented. Click Test to ensure that the connection between Sentry and Amazon EC2 functions as expected.

CLOUD POLICIES > CLOUD POLICY CONFIGURATION

CLOUD POLICY

Policy Name*:

Type: Amazon EC2

API Key*:

API Secret*:

Image Id*:

Min Servers*:

Max Servers*:

Region:

Server Key Name:

Security Group:

Availability Zone:

Instance Type:

Kernel Id:

RAM Disk Id:

User Data:

Term Details: Amazon EC2 Management from Sentry

The following table describes each term and definition for the categories displayed above.

TERM	DEFINITION
Policy Name	The identifier for this Cloud Policy.
Type	Type of the IaaS cloud provider. The product ships with Amazon EC2 and GoGrid management adapters additional IaaS providers can delivered upon request including: <ul style="list-style-type: none">• Rackspace• Opsource• Azure• VMware
API Key	API Key obtained from IaaS provider. Amazon EC2 provides this under <i>Account</i> → <i>Security Credentials</i> → <i>Access Credentials</i>

API Secret	API Secret obtained from IaaS provider. Amazon EC2 provides this under <i>Account</i> → <i>Security Credentials</i> → <i>Access Credentials</i>
Image Id	The pre-package Images available for instantiation. These images have to be built and available prior to use from the Sentry Console. You can build and register images from the cloud provider management console.
Min Servers	The minimum number of server instance to be instantiated. This field is a placeholder for future dynamic scaling capabilities that enable auto scaling based on traffic and latency based metrics.
Max Servers	The max number of server instance to be instantiated.
Region	The demographic region where the instances are to be instantiated. Typically, this is used to address latency issues based on the desired regions to be served by the cloud instances.
Server Key Name	Public AMI instances have no password, and you need a public/private key pair to log in to them. The public key half of this pair is embedded in your instance, allowing you to use the private key to log in securely without a password. After you create your own AMIs, you can choose other mechanisms to securely log in to your new instances. See How to have AWS Create a Key Pair for You .
Security Group	This enables you to set firewall rules such as allowable protocols and ports. This has to be set in the Amazon EC2 Management console for use within Sentry. For more details see Using Security Groups .
Availability Zone	Optional. Amazon EC2 provides the ability to place instances in multiple locations. Amazon EC2 locations are composed of Availability Zones and Regions. Regions are dispersed and located in separate geographic areas (US, EU, etc.). Availability Zones are distinct locations within a Region that are engineered to be isolated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same Region. For Details, see Regions and Availability Zone Concepts .
Instance Type	The type of instance requested based on memory and CPU type. This impacts performance and cost per instance. Amazon EC2 instance types .
Kernel Id	Optional. The operating system Kernel ID associated with the Image. For further details see Enabling User Provided Kernel in Amazon EC2 .
RAM Disk Id	Optional. The RAM Disk associated with the Image. For further details see the Amazon EC2 Developer Documentation.
User Data	Optional. When you launch an instance, you can specify <i>user data</i> , which is available for all instances in the reservation to retrieve. You can also add (or modify) user data to Amazon EBS-backed instances when they're stopped. Requests for the user data returns the data as-is (content type application/x-octetstream). For samples, see Using Instance Metadata .

Configure Network Policies for Cloud Management

In Network Policies, create a new Group Remote Policy and associate the Cloud Policy with the Group Remote Policy as shown in the figure below:

NETWORK POLICIES > GROUP REMOTE POLICY

Contains Remote Policies

<input type="checkbox"/>	NAME	REMOTE ADDRESS	CLOUD POLICY
<input checked="" type="checkbox"/>	Aggregated-Services-Remote	[Cloud_Policy_Amazon_EC2]:8080	Cloud_Policy_Amazon_EC2

Remaining Remote Policies

<input type="checkbox"/>	NAME	REMOTE ADDRESS
<input type="checkbox"/>	Aggregated-Services-Remote-2	localhost:8080

Finish

POLICY SELECTIONS

<u>Policy Name:</u>	GroupRemotePolicy
<u>Strategy:</u>	Round Robin
<u>Protocol:</u>	HTTP
<u>Retry Delay:</u>	30
<u>Server Affinity:</u>	None
<u>Remote Policies:</u>	[Aggregated-Services-Remote]

The Group Remote Policy now includes a set of all the IP addresses retrieved from Amazon EC2. Additional remote policies can be selected from the *Remaining Remote Policies* section and pointed to additional Cloud Policies. This enable failover and load balancing across a pool of cloud instance that can be configured in disparate physical regions for an IaaS provider or across IaaS vendors. Note that the port in the *Remote Address* for the Cloud Policy above is the same since the images are assumed to be identical with services configured on a selected port. The cloud provider will assign unique IP addresses on startup that become the pool of IP address that the Group Remote Policy will cycle through based on the *Strategy*. In the screen show above, the *Strategy* is set to *Round Robin*.

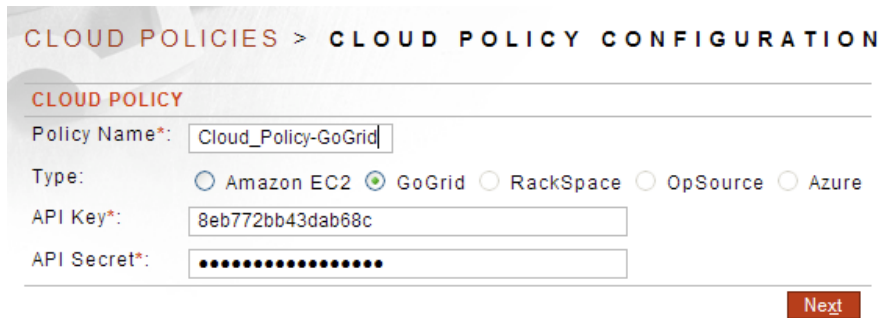
CLOUD IAAS PROVIDER: GoGrid

In this section, we will set up Forum Sentry's interaction with GoGrid, another well know IaaS provider.

Cloud Policies

Cloud policies can easily be setup by instantiating images on IaaS providers. The sequence for creating a cloud policy is as follows:

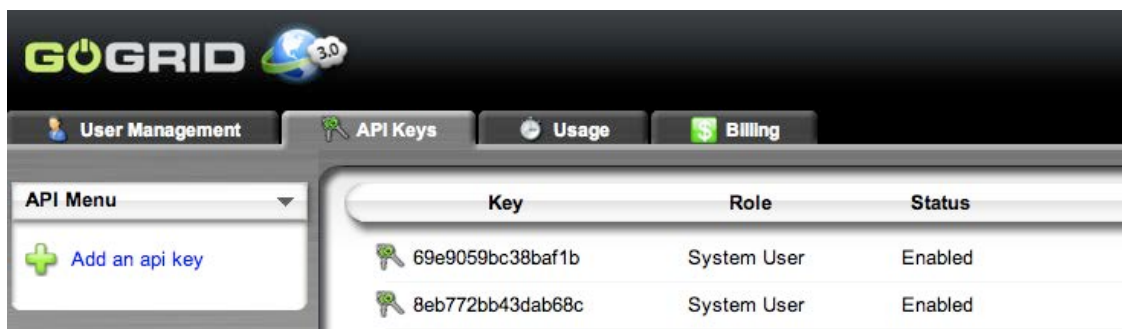
From the Gateway Policies, select Cloud Policies and click on New to start creating a new policy as shown in the screen below.



The screenshot shows the 'CLOUD POLICIES > CLOUD POLICY CONFIGURATION' page. It contains a form for creating a new cloud policy. The 'Policy Name*' field is filled with 'Cloud_Policy-GoGrid'. The 'Type' field has radio buttons for 'Amazon EC2', 'GoGrid' (which is selected), 'RackSpace', 'OpSource', and 'Azure'. The 'API Key*' field is filled with '8eb772bb43dab68c'. The 'API Secret*' field is masked with dots. A 'Next' button is located at the bottom right of the form.

Retrieve Access Credentials from GoGrid

The next step requires acquiring credentials from GoGrid so that Forum Sentry can interact with the IaaS management API. For GoGrid, the credentials are available once an account has been set up. After registering with GoGrid, under *My Account* → *API*, select **Key** and **Shared Secret**. This information is inserted in the Cloud Policy setup in Sentry to enable interaction between Sentry and GoGrid management API.

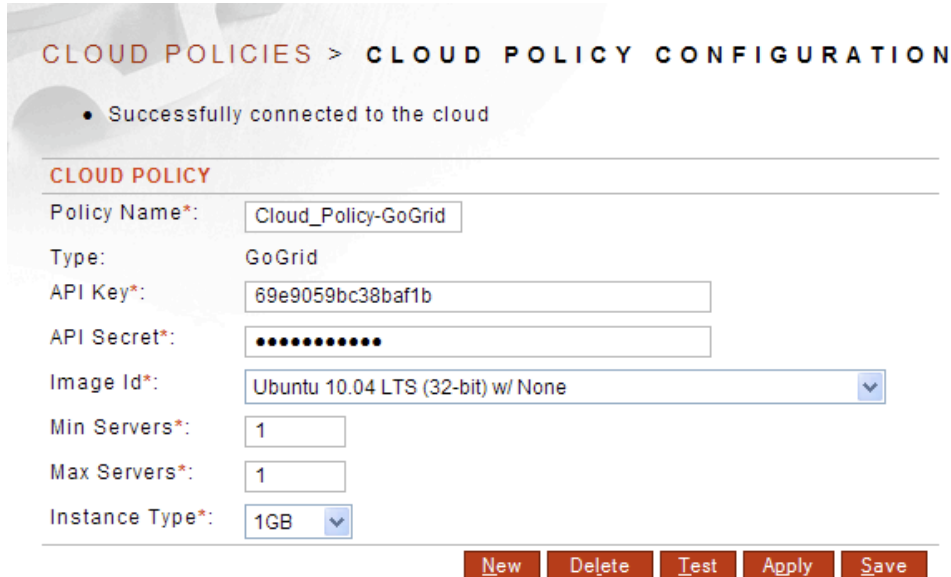


The screenshot shows the GoGrid 'API Keys' page. It has a navigation bar with 'User Management', 'API Keys', 'Usage', and 'Billing'. On the left, there is an 'API Menu' with a link to 'Add an api key'. The main content area is a table with columns 'Key', 'Role', and 'Status'.

Key	Role	Status
69e9059bc38baf1b	System User	Enabled
8eb772bb43dab68c	System User	Enabled

Configure GoGrid Management from Sentry

On successful authentication to GoGrid, the following Configuration screen is presented. Click *Test* to ensure that the connection between Sentry and GoGrid functions as expected.



CLOUD POLICIES > CLOUD POLICY CONFIGURATION

- Successfully connected to the cloud

CLOUD POLICY

Policy Name*: Cloud_Policy-GoGrid

Type: GoGrid

API Key*: 69e9059bc38baf1b

API Secret*:

Image Id*: Ubuntu 10.04 LTS (32-bit) w/ None

Min Servers*: 1

Max Servers*: 1

Instance Type*: 1GB

[New](#) [Delete](#) [Test](#) [Apply](#) [Save](#)

After entering information in all the fields above, click *New* to instantiate select number of instance in the Cloud at GoGrid. The new instance appears in GoGrid as follows:



Term Details: GoGrid Management from Sentry

The following table describes each term and definition for the categories displayed above.

TERM	DEFINITION
Policy Name	The identifier for this Cloud Policy.
Type	Type of the IaaS cloud provider. The product ships with Amazon EC2 and GoGrid management adapters. Additional IaaS providers can be delivered upon request including: <ul style="list-style-type: none">• Rackspace• Opsource• Azure• VMWare
API Key	API Key obtained from IaaS provider. GoGrid provides this under <i>My Account</i> → <i>API Keys</i>
API Secret	API Secret obtained from IaaS provider. GoGrid provides this under <i>My Account</i> → <i>API Keys</i> . The API (Shared) Secret is obtained by clicking on the API Key.
Image ID	Pre-packaged Image ID available at GoGrid. Users can package and install their own images or use prepackaged ones that are already provided.
Min Servers	The minimum number of server instances to be instantiated. This field is a placeholder for future dynamic scaling capabilities that enable auto scaling based on traffic and latency based metrics.
Max Servers	The max number of server instances to be instantiated.
Instance Type	RAM size for instance. 512-MB to 1GB

Configure Network Policies for Cloud Management

In Network Policies, create a new Group Remote Policy and associate the Cloud Policy with the Group Remote Policy as shown in the figure below:

NETWORK POLICIES > GROUP REMOTE POLICY

Contains Remote Policies

<input type="checkbox"/>	NAME	REMOTE ADDRESS	CLOUD POLICY
<input checked="" type="checkbox"/>	Aggregated-Services-Remote	[Cloud_Policy_Amazon_EC2]:8080	Cloud_Policy_Amazon_EC2
<input checked="" type="checkbox"/>	Aggregated-Services-Remote-2	[Cloud_Policy-GoGrid]:8080	Cloud_Policy-GoGrid

Remaining Remote Policies

<input type="checkbox"/>	NAME	REMOTE ADDRESS
--------------------------	------	----------------

Finish

POLICY SELECTIONS

Policy Name:	GroupRemotePolicy
Strategy:	Round Robin
Protocol:	HTTP
Retry Delay:	30
Server Affinity:	None
Remote Policies:	[Aggregated-Services-Remote]

The Group Remote Policy now includes a set of all the IP addresses retrieved from Amazon EC2 and GoGrid. This enables failover and load balancing across a pool of cloud instance that are configured in disparate physical regions for an IaaS provider or across IaaS vendors. Note that the port in the *Remote Address* for the Cloud Policy above is the same since the images are assumed to be identical with services configured on a selected port. The cloud provider will assign unique IP addresses on startup that become the pool of IP address that the Group Remote Policy will cycle through based on the *Strategy*. In the screen show above, the *Strategy* is set to *Round Robin*.