



FORUM SENTRY™ VERSION 9

AMAZON EC2 INTEGRATION 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.

FORUMOST™ 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™ Version 9 Amazon EC2 Integration Guide, published May 2024.

D-ASF-SE-543811

Table of Contents

AMAZON EC2 INSTALLATION 4

 Overview 4

FORUM SENTRY AMAZON EC2 INTEGRATION 5

 Overview 5

 Forum Sentry agent privileges 5

 Forum Sentry agent security 5

 Forum Sentry agent updates 6

 Telemetry data lifecycle 6

AMAZON EC2 INSTALLATION

Overview

Forum Sentry is available in a number of form factors for deployment in the Amazon EC Cloud. These include a Marketplace AMI image, a Linux software package, and a Windows software package. The Forum Sentry AMI is available to launch from the AWS Marketplace. The Linux and Windows form factors can be deployed on a Linux or Windows EC2 instance.

The Forum Sentry AMI is available to launch either from the AWS Marketplace or directly from the AWS EC2 Management console. Once you have launched an AWS Instance from the Forum Sentry AMI or installed the Linux or Windows agent, you will need to license Sentry and configure an administrator account.

The Forum Sentry AMI is licensed as BYOL (bring your own license) which means a license from Forum Systems or a Forum Systems' partner is required to use the product. AWS usage fees are separate from this license.

For more information about installing the Forum Sentry AMI, please refer to the FORUM SYSTEMS SENTRY™ AMAZON AMI INSTALLATION GUIDE. For more information about installing the Forum Sentry Linux or Windows agent, please refer to the FORUM SYSTEMS SENTRY™ SOFTWARE INSTALLATION GUIDE. For the full documentation set, FAQs, best practices, and more, please visit the [Forum Systems Support Help Desk](#) site.

FORUM SENTRY AMAZON EC2 INTEGRATION

Overview

Forum Sentry is available in a number of form factors for deployment in the Amazon EC Cloud. These include a Marketplace AMI image, a Linux software package, and a Windows software package. The Forum Sentry AMI is available to launch from the AWS Marketplace. Forum Sentry Linux and Windows form factors can be deployed on a Linux or Windows EC2 instance and are available at <https://downloads.forumsys.com> (registration required for access).

Forum Sentry agent privileges

The Forum Sentry AMI form factor is a stand-alone image which includes the Forum Sentry Agent running on the ForumOS™ which is a FIPS 140-2 and Common Criteria NDDP security hardened operating system. This image type has provides no direct shell access and all administration and provisioning is done via the Command-Line Interface, the Web Based Administration Interface, or the REST API interface. Privileged commands in the Web Based Interface, the REST API, and the command-line interface are run under privileged Forum Sentry user accounts provisioned at installation time.

The Forum Sentry Linux or Windows software provide a software package that will install the Forum Sentry API Gateway Agent as a daemon or service on the Guest OS that is chosen by the EC2 administrator. You must have administrator or root privileges to install the Sentry agent. On the supported Linux systems, the Sentry agent consists of a user-mode executable that runs as a daemon with root access. On supported Windows-based operating systems, the Forum agent is installed as a service running under the user account with administrator privileges used during the installation.

Forum Sentry agent security

Forum Sentry operates as a reverse proxy from a network perspective. This means that there are connections inbound to the agent and there are connections outbound from the agent. The inbound rules are the TCP IP and ports that will be exposed for accepting inbound protocol connections by the Forum Sentry agent, known as Sentry Listener policies. These inbound policies accept requests from other network infrastructure and connections are established with IP and port of the Sentry Agent per defined policy. The Sentry content policies then define to process workflows and what types of identity, security, and mediation processing to apply. Then a new connection is established outbound to broker the processed information to the remote applications, services and APIs that are being protected by the Sentry policies. These remote application protocol connections are defined as Sentry Remote Policies and represent the IP and port settings for connections to outbound systems. The Sentry agent allows for configuring many different IP and ports for inbound, as well as for outbound connections, so the EC2 security policies will need to be aligned with these settings to ensure the EC2 instance running Forum Sentry has proper EC2 networking connectivity. Note that EC load balancing can be used for the inbound and outbound policy ports and IPs.

For inbound policies, the security policies need to be defined to allow the access to the ports from the client applications or from the EC2 load balancer. For outbound policies, the security policies need to allow the Sentry agent to communicate to the networking infrastructure or directly to the target IPs and ports representing these endpoints, or to the EC2 load balancer.

The Forum Sentry agent has specified ports for Web Based Administration and the CLI (for the AMI image type). If using the AMI, TCP ports 5050 and 22 should be added to your EC security policies before you can initialize the agent. If you are using the Linux or Windows agent, only TCP port 5050 is

required as there is no CLI for these form factors. These ports are configurable by the Sentry administration and may be changed after agent initialization.

For any connections inbound or outbound that require TLS, this is configured directly within the Forum Sentry agent and requires no additional EC2 provisioning. Forum Sentry handles the authentication, data security in motion, data security at rest, and logging and monitoring aspects and require no additional EC2 provisioning.

Forum Sentry agent updates

Update packages for Forum Sentry product releases are available for registered customers and available from <https://downloads.forumsys.com>. These updates are single-package installations and applied to the AMI image via the secure Web Based Administration. For the Linux or Windows instances these installs are performed via root or administrator access in the same manner as the initial installation. The update package will recognize the existing Sentry installation and perform the upgrade of the Sentry agent in-place with full backward compatibility of existing policies.

Telemetry data lifecycle

Telemetry data from Forum Sentry agents depend on the provisioning for logging, monitoring and metrics gathering.

For outbound logging, the Sentry agent can be configured for one or more SYSLOG based targets to collect logging information for transactions flowing through the agent as well as logging for any provisioning that occurs on the Sentry agent itself. SYSLOG policies on Sentry can be configured as TCP or UDP. The default port is 514, but is configurable and can be changed by the Sentry administrator.

For monitoring and metrics, the Sentry agent can be configured for inbound SNMP monitoring to allow SNMP agents to query the Sentry agent for collecting metrics about the instance. The default port for SNMP is 161, but is configurable and can be changed by the Sentry administrator. Additionally, monitoring can be configured on a REST API. The monitoring API is configurable as to the IP and port to be used for inbound monitoring REST API requests. These requests can be made in XML or JSON format.