

# Oracle® Cloud

## Using Oracle Security Monitoring and Analytics



E67074-28  
May 2019



Oracle Cloud Using Oracle Security Monitoring and Analytics,

E67074-28

Copyright © 2017, 2020, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## 1 Getting Started with Oracle Security Monitoring and Analytics

---

About Oracle Security Monitoring and Analytics	1-1
Collecting Operating System Logs from Your Host Platforms	1-2
Collect Linux Default Logs	1-3
Collect Windows Default Logs	1-4
About Roles and Users	1-4
Before You Begin with Security Monitoring and Analytics	1-5

## 2 Working with Security Monitoring and Analytics

---

Create a Security Alert Rule	2-1
Fine-tune Event Detection	2-2
Security Correlation Rule System	2-2
Tuning Rule Specs by Editing Its Parameters	2-5
Tuning Rule Exceptions by Whitelisting Rule Attributes	2-7
Administer Machine Learning Capabilities	2-8
Machine Learning Capabilities Overview	2-8
Create a Peer Group Analysis Model	2-9
Create an SQL Analysis Model	2-10
Additional Machine Learning Features for Administrators	2-11
Enable and Disable Models	2-11
Search and View Models	2-12
Perform Security Analysis	2-12
Customize Your Security Dashboards	2-12
Security Intelligence Dashboard	2-13
Security Dashboards	2-19

## 3 Investigating and Analyzing Threats Based on Correlation Rule

---

Investigate and Analyze Threats in Response to an Alert Notification	3-1
Investigating Threats Detected by Correlation Rule	3-1
Investigating and Analyzing Users Associated with Threats	3-2
Isolate Risky Users Associated with Threats	3-3

## A Configuration of Security Log Sources

---

Configuration Quick-Start Guides	A-4
Oracle Audit Vault and Database Firewall	A-5
Oracle Database	A-6
Bluecoat Proxy	A-7
Apache Tomcat	A-9
Cisco ASA Firewall	A-10
F5 Big Firewall	A-11
Fortinet FortiGate Firewall	A-12
MS Active Directory	A-13
Palo Alto Firewall	A-14
Common Tasks	A-15
Prerequisites and Requirements for Security Sources	A-16
Validate Log Collections	A-16

## B SMA Reference

---

Security Monitoring and Analytics Terminology	B-1
Security Event Format - SEF Handbook	B-2
SEF Query Samples	B-2
Filtering SEF Queries	B-2
Commonly Used SEF Fields	B-4
sef   Field Properties	B-4
sefActor   Field Properties	B-5
sefDestination   Field Properties	B-6
sefOriginalActor   Field Properties	B-7
SEF Elements	B-7
Security Intelligence Reference	B-9

## C User Identity Information and Alerting Sources

---

Oracle Identity Cloud Service	C-1
Uploading User Data Using REST API	C-1
Collect User Information from Oracle Identity Cloud Service (IDCS)	C-1
	C-4
Ingest Alert Data from Oracle CASB Service	C-4

# Preface

Oracle Security Monitoring and Analytics enables rapid detection, investigation and remediation of the broadest range of security threats across on-premises and cloud IT assets. Security Monitoring and Analytics provides integrated SIEM and UEBA capabilities built on machine learning, user session awareness, and up-to-date threat intelligence context. This service is built on Oracle Management Cloud's secure, unified big data platform.

## Topics:

- [Audience](#)
- [Related Resources](#)
- [Conventions](#)

## Audience

*Using Oracle Security Monitoring and Analytics* is intended for users who want to monitor and analyze security activity.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Related Resources

For more information, see these Oracle resources:

- <http://cloud.oracle.com>
- Using Oracle Log Analytics
- Using Application Performance Monitoring  
Using IT Analytics Cloud Service

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

# 1

## Getting Started with Oracle Security Monitoring and Analytics

### Topics:

- [About Oracle Security Monitoring and Analytics](#)
- [Before You Begin with Security Monitoring and Analytics](#)
- [About Roles and Users](#)
- [Collecting Operating System Logs from Your Host Platforms](#)

## About Oracle Security Monitoring and Analytics

### Note:

**As of September 2019, no enhancements have been made to this service and this functionality is no longer available to new customers.**

### What is Oracle Security Monitoring and Analytics?

Oracle Security Monitoring and Analytics is a security solution provided as part of Oracle Management Cloud's unified platform. Its core functionality is around cyber security, providing you with IT solutions in the form of anomaly detection and investigations, and remediation of the broadest range of security threats across on-premises and cloud IT assets. Oracle Security Monitoring and Analytics provides integrated security information and event management (SIEM) and user, and entity behavior analytics (UEBA) capabilities built on machine learning, user session awareness, and up-to-date threat intelligence context.

The following diagram shows the integration of Oracle Security Monitoring and Analytics with other cloud solutions also designed as platform components for Oracle Management Cloud.



### Product Key Features

#### **Real-time threat detection based on rules and patterns:**

Universal threat visibility— Collect and analyze any security relevant data.

SOC-ready content— Ready to use, vendor neutral SOC content library.

Threat intelligence leverage— Connect to any threat feed, leverage embedded reputation data.

#### **Advanced threat analytics and visualization:**

Data access anomaly detection— Detect SQL query anomalies for any user, database or application.

Identify anomalous activity of an entity based on instance-based and peer-based behavior baselines.

Multi-dimensional anomaly detection— Detect anomalies across multiple behavioral attributes.

Session awareness and attack chain visualization— Faster detection with user awareness kill chain visualization.

#### **Enhanced Security Monitoring with Oracle Management Cloud Platform:**

Topology awareness— Detect multi-tier application attacks and lateral movement indicators.

Additional features include:

- Correlation Rule-tuning
- Customizable Watchlists
- Storage management
- Integration with IDCS and CASB services

## Collecting Operating System Logs from Your Host Platforms

You can collect log data from your hosts and get immediate insight into potential security threats across your environments.

#### **Topics:**

- [Collect Linux Default Logs](#)
- [Collect Windows Default Logs](#)



## Collect Linux Default Logs

Enable default OS event logs in Linux.

### Prerequisite Checklist

1. Host machine met OS requirements for local agent installations	Requirement for Logs Collection on Unix in <i>Installing and Managing Oracle Management Cloud Agents</i>
2. Oracle Management Cloud environment met the minimum standard setup requirements	To analyze security log data you must first enable Security Monitoring and Analytics (SMA) licensing. SMA licensing assumes that Log Analytics licensing is enabled as well. To enable these components and ensure you meet other prerequisites see <a href="#">Prerequisites and Requirements for Security Sources</a> .

### Configuration Steps

Linux Log Configuration	Task Requirements	For additional details, see...
<b>STEP 1. - Enable</b> host <i>monitoring</i> in OMC.	Enable the Linux host where you installed the agent. By default your host is already added as an entity, however, <i>monitoring</i> is disabled.	Enable Host Monitoring in <i>Using Oracle Infrastructure Monitoring</i>
<b>STEP 2. - Associate</b> your (Linux host) entity for log collection.	From <b>Log Analytics &gt; Log Admin &gt; Entities</b> , click <b>New Association</b> and select the new Linux host.	Configure New Entity Associations in <i>Using Log Analytics</i>
<b>STEP 3. - Select</b> log sources for your new (Linux host) entity.	Select the Linux logs that apply for your environment.	<a href="#">Host Sources</a> Associating Entities to Existing Log Sources in <i>Using Oracle Log Analytics</i>
<b>STEP 4. - Validate</b> your log collection.	Ensure your setup is successfully completed: validate your collection. Navigate to <b>Security Analytics &gt; Security Data Explorer</b> .	<a href="#">Validate Log Collections</a>

For a complete list of supported log sources and quick-start configuration guides, see Appendix [Host Sources](#)

## Collect Windows Default Logs

Enable default logs for Windows platforms.

### Prerequisites

<p>Ensure that your OMC environment meets the typical requirements to enable platform logs.</p>	<p>To analyze security log data you must first enable Security Monitoring and Analytics (SMA) licensing. SMA licensing assumes that Log Analytics licensing is enabled as well. To enable these components and ensure you meet other prerequisites see <a href="#">Prerequisites and Requirements for Security Sources</a>. Environment Requirements in <i>Installing and Managing Oracle Management Cloud Agents</i></p>
---	---

**Table 1-1 Log Configuration Steps**

Windows Log Configuration	Task Requirements	For additional details, see...
<p><b>STEP 1. - Enable</b> host <i>monitoring</i> in OMC.</p>	<p>Enable the Windows host where you installed the agent. By default your host is already added as an entity, however, <i>monitoring</i> is disabled.</p>	<p>Enable Host Monitoring in <i>Using Oracle Infrastructure Monitoring</i></p>
<p><b>STEP 2. - Associate</b> your (Windows host) entity for log collection.</p>	<p>From <b>Log Analytics &gt; Log Admin &gt; Entities</b>, click <b>New Association</b> and select the new Windows host.</p>	<p>Configure New Entity Associations in <i>Using Log Analytics</i></p>
<p><b>STEP 3. - Select</b> log sources for your new (Windows host) entity.</p>	<p>Select the Windows Security Events log source to associate with your Windows host.</p>	<p><a href="#">Host Sources</a> Associating Entities to Existing Log Sources in <i>Using Oracle Log Analytics</i></p>
<p><b>STEP 4. - Validate</b> your log collection.</p>	<p>Ensure your setup is successfully completed: validate your collection. Navigate to <b>Security Analytics &gt; Security Data Explorer</b>.</p>	<p><a href="#">Validate Log Collections</a></p>

For a complete list of supported log sources and quick-start configuration guides, see Appendix [Host Sources](#)

## About Roles and Users

To use Oracle Management Cloud you must be assigned either an OMC Administrator or an OMC User role from Oracle Cloud My Services.

- OMC Administrator role

These users have complete access to the entire platform, including administrative privileges in other suite components like Oracle Log Analytics. Only users with these privileges will be able to perform administrative tasks, such as deploying agents, changing configuration settings, and so on.

- OMC User role

These users have limited access and can only perform tasks such as viewing and monitoring infrastructure or application performance.

**Table 1-2 User roles and typical tasks with Security Monitoring and Analytics, per user role.**

User Role	Tasks
Security Operations Center Administrator ( <i>OMC Administrator</i> )	<ul style="list-style-type: none"> <li>• Set up Oracle Security Monitoring and Analytics.</li> <li>• Configure machine learning models.</li> <li>• Set up Oracle Log Analytics.</li> <li>• Manage cloud agents</li> <li>• Add and delete entities.</li> <li>• Create and administer new log sources.</li> <li>• Configure alert rules.</li> </ul>
Security Operations Center Analyst ( <i>OMC User</i> )	<ul style="list-style-type: none"> <li>• Investigate and analyze user activity.</li> <li>• Investigate and analyze events, anomalies, and alerts.</li> <li>• Monitor the security posture of your organization.</li> </ul>

## Before You Begin with Security Monitoring and Analytics

In this section you learn general concepts and related terms that are commonly used in Oracle Security Monitoring and Analytics.

### Oracle Security Monitoring and Analytics Concepts and Related Terms

Term	Definition
Cloud agent	On-premises interface to Oracle Management Cloud, which is configured to monitor various entities by collecting status, performance, and configuration data.
Asset	A monitored resource, such as a database, a host server, a compute resource, or an application server, that can be monitored in Oracle Enterprise Manager Cloud Control.
Gateway	A cloud agent that acts as a proxy between Oracle Management Cloud and all other cloud agents.
Log entity	The name of a log file.
Log source	A named group of log files. The files that belong to this group can be configured using patterns such as <code>/var/log/ssh*</code> . A log source can be associated with one or more parsers.

Term	Definition
Oracle home	A directory where Oracle products are installed, pointed to by an environment variable.
Parser	A named entity used to define how to parse all log entries in a log source and extract field information. It uses one or multiple parse expressions and a log entry delimiter to parse all log entries in a log source. It also specifies how the parsed content is converted into fields.
Remediation Action	A task, or a set of tasks that implement a fix to a specific issue. A remediation task can be added as a response to an alert.

### SMA Terminology Reference



#### Note:

See:

1. [Security Monitoring and Analytics Terminology](#)
2. [Security Intelligence Reference](#)
3. [SEF Elements](#)

# 2

## Working with Security Monitoring and Analytics


This section includes ways you can configure, administer, and maintain Security Monitoring and Analytics on a regular basis.

Task Description	More Information
Receive alert notifications based on security thresholds values you define.	<a href="#">Create a Security Alert Rule</a>
Tune correlation rules to achieve more relevant detections by adjusting available parameter values.	<a href="#">Tuning Rule Specs by Editing Its Parameters</a>
Specify associated elements in your correlation rule as whitelisted to reduce false positives event detections.	<a href="#">Tuning Rule Exceptions by Whitelisting Rule Attributes</a>
Provide learning orientation by specifying learning attributes using machine learning models.	<a href="#">Administer Machine Learning Capabilities</a>

### Create a Security Alert Rule

Alert rules trigger alert notifications when anomalous activity is detected.

For example, you want Security Monitoring and Analytics to alert you with an notification email when a anomalous activity is detected. First, you need to create an alert rule and define its threshold values.

1. From Security Monitoring and Analytics, click the **Menu** icon , top-left under the product name.
2. Under **Security Admin**, select **Alert Rules**.
3. Click **Create Alert Rule**, top-right under **Alerts**.
4. Enter a name and a description.
5. Alerts can be generated based on two severity levels (warning or critical).
  - a. Select **For All Threats** and then choose one:
    - **Warning Alert** —this generates a **Warning** alert for all threats.
    - **Critical Alert** —this generates a **Critical** alert for all threats.
  - b. Select **Based on Risk Level**.

You can set thresholds for generating a warning or a critical alert based on risk level of the threat.

    - Chose > or < under operator.
    - Under Warning Threshold, select Low, Medium or High for the Threat Risk Level to generate a warning alert.

- Under Critical Threshold, select Medium, High or Critical for the Threat Risk Level to generate a Critical alert.

When generating alerts based on risk level, the warning threshold level (low, medium, high) must be set lower than the critical threshold level (medium, high, critical).

6. Add email recipients for alert notifications.
7. Click **Save**.

## Fine-tune Event Detection

Fine-tuning correlation rules takes into account the ongoing changes in your IT environment.

### Topics:

- [Security Correlation Rule System](#)
- [Tuning Rule Specs by Editing Its Parameters](#)
- [Tuning Rule Exceptions by Whitelisting Rule Attributes](#)

## Security Correlation Rule System

SMA's Correlation Rule Engine comes with a correlation rule system right out of the box.

Category	Description
<a href="#">Account</a>	Account rules identify account management related threats
<a href="#">Authentication</a>	Authentication rules are related to authentication activities
<a href="#">Availability</a>	Availability rules identify availability stature of applications, hosts and devices
<a href="#">Data</a>	Data rules identify data and metadata related threats
<a href="#">Endpoint</a>	Endpoint rules identify threats against endpoints
<a href="#">Network</a>	Network rules are related to network activities

### Account

Account rules identify account management related threats.

1. **LocalAccountCreation:** An account creation event is detected on an endpoint.
2. **MultipleAccountCreation:** Multiple (3 or more) accounts are created by the same user within a 5-minute interval.
3. **MultipleAccountModification:** Multiple (3 or more) accounts are modified within a 5-minute interval.

## Authentication

Authentication rules are related to authentication activities.

1. **BruteForceAttack:** Five or more failed login events are followed by a successful login on the same endpoint, associated with the same user account, within 60 seconds.
2. **BruteForceAttackLinux:** 5 or more failed login events are followed by a successful login on the same Linux host, associated with the same user account, within an interval of 60 seconds.
3. **DefaultAccountLogin:** Login event associated with a default account is detected. This rule only applies to Oracle Database events.
4. **DirectRootLogin:** A root login event is detected on an endpoint.
5. **MultipleFailedLogin:** Detects multiple failed login events on 5 or more distinct accounts on the same endpoint within 60 seconds.
6. **MultipleFailedSu:** Five or more failed su (to root) attempts are detected on the same endpoint within 180 seconds.
7. **MultipleFailedSudo:** Five or more failed sudo events initiated by the same account within 180 seconds are detected.
8. **SuspiciousSuLogin:** Two or more failed su (to root) attempts are followed by a successful su (to root) on the same endpoint within a time interval of 180 seconds.
9. **TargetedAccountAttack:** 5 or more failed login events associated with the same user account are detected within an interval of 60 seconds across single or multiple endpoints.
10. **TargetedAccountAttackLinux:** 5 or more failed login events associated with the same user account are detected within an interval of 60 seconds across single or multiple Linux hosts.

## Availability

Availability rules identify availability stature of applications, hosts and devices.

1. **PlatformInstability:** Series of firewall messages that show potential firewall stability issues.
2. **TrafficJam:** Firewall messages that show new connections aren't being accepted as the TCP syslog server can't be reached.
3. **TranslationTableFull:** Series of firewall messages that show that the translation table is full. Traffic will be dropped. This could be a misconfiguration, capacity issue, or the sign of an attack.

## Data

Data rules identify data and metadata related threats.

1. **DataDictionaryCopy:** Copy operation is detected on certain sensitive data dictionary objects. This rule only applies to Oracle Database events.
2. **DataDictionarySynonym:** Synonym creation is detected on certain sensitive data dictionary objects. This rule only applies to Oracle Database events.
3. **WLSBackdoor:** Event that shows the successful upload of known backdoor jsp code.

## Endpoint

Endpoint rules identify threats against endpoints.

1. **CASBRiskIndicator**: Checks for CASB Policy Violations.

## Network

Network rules are related to network activities.

1. **BrowserCoinMiner**: Detects communication to potential sites related to browser hijack for cryptocurrency mining.
2. **DeniedZoneTransfer**: Possible DNS reconnaissance through an attempt zone transfer.
3. **ExternallIPDiscovery**: Detects connection attempts to domains that can be used by malware to detect the external IP address of a network for profiling purposes.
4. **FirewallADDrop**: Series of firewall messages that show traffic being dropped to Microsoft Domain Controllers.
5. **FirewallSiemDrop**: A series of firewall messages that show traffic being dropped to or from the vulnerability assessment scanners.
6. **FirewallVaDrop**: A series of firewall messages that show traffic being dropped to or from the vulnerability assessment scanners.
7. **HorizontalPortScan**: Network communication, originating from the same source IP, is detected on the same port on 10 or more distinct destination IPs within 60 seconds.
8. **PingSweep**: ICMP messages, originating from the same source IP, are detected on 20 or more destination IPs within 60 seconds.
9. **PossibleFirewallRouteIssue**: A series of firewall messages that show potential routing issues with the firewall. This can be indicative of misconfiguration, potential attack, or a general network issue.
10. **PossibleSynFlood**: A series of firewall messages that show potential firewall stability issues.
11. **PTRRecon**: DNS reconnaissance activity where the DNS client performs 5 distinct reverse record lookups (PTR) in a 30 second window.
12. **PunyCodeDomain**: Detects international domain names that can't be displayed in ASCII. Domains in languages like Cyrillic, Japanese, or Farsi that require the Punycode algorithm to convert them into ASCII formats that DNS is able to support.
13. **SIDScan**: SID reconnaissance activity where the client performs five distinct SID connection attempts within 60 seconds.
14. **SuspectedAPT**: Destination traffic matches any entry in the following watch lists: `omc_apt_ip`, `omc_apt_domain`, `omc_apt_url`.
15. **SuspectedMalware**: Destination traffic matches any entry in the following watch lists: `omc_malware_ip`, `omc_malware_domain`, `omc_malware_url`.
16. **SuspectedRansomware**: Destination traffic matches any entry in the following watch lists: `omc_ransomware_ip`, `omc_ransomware_domain`, `omc_ransomware_url`.



17. **SuspectedTOR**: Detects traffic elements that indicate possible connection attempts to TOR and other anonymization networks.
18. **SuspiciousNetworkTraffic**: Destination traffic matches any entry in the following watch lists: `omc_suspicious_ip`, `omc_suspicious_domain`, `omc_suspicious_url`.
19. **TooManyConnection**: A series of firewall messages the show too many connections to an address translation. This could be a misconfiguration, capacity issue, or a sign of an attack.
20. **URLShorteningService**: Tags logs where network traffic is attempted to a URL that's shortened with a known URL shortening service. Triggered when internet traffic to a known URL shortening service is detected.
21. **UserAgentNull**: Proxy suspicious activity occurred where no User Agent is passed to the proxy. This is atypical behavior and should be investigated. Note: this rule is turned off by default.
22. **UserAgentShort**: Detects HTTP traffic with a user agent string less than 40 characters.
23. **VerticalPortScan**: Network communication, originating from the same source IP, is detected on 20 or more distinct ports on the same destination within 60 seconds.

 **Note:**

To fine-tune out-of-the-box correlation rules, see .

## Tuning Rule Specs by Editing Its Parameters

First action item in event detection is to fine-tune your correlation rules by customizing their rule logic through parameter manipulation. Rule-tuning is essential in order to take into account day-to-day changes in your environment

### Task scope:

We use an example, where the user is adjusting the available parameters within the rule to tune it for their network. Where the `Minimum Length` parameter holds a *string-length* value that is compared against the associated `user agent string` SEF field.

### Task results:

- You tune the `UserAgentShort` correlation rule by adjusting the `Minimum Length` parameter value.
- Security Monitoring and Analytics increments the corresponding version number by one, saves it, and enables it by default.

### Putting it in context of a real-world scenario

"Your security team may use a custom user agent string to identify authorized network scanning activity using the following pattern **vuln scan soc@example.com ticket:<6 digit incrementing value>**. As we can see from the rule specification (see table below), the rule is triggered by user agent strings of less than 40 characters by default.

This custom user agent is only 39 characters and would trigger the rule whenever scanning was done, generating false positive events."

**Table 2-1 Example Details**

Item	Details
<b>Out-of-the-Box Correlation Rule:</b>	UserAgentShort
<b>Parameterizing attribute:</b>	Minimum Length
<b>SEF expression:</b>	Pattern for UserAgentShort (SYSTEM.SEF as Event) where Event.sefTransportProtocol IN ("http", "https") AND StrLen(Event.sefActorEPProgramName) > 1 AND StrLen(Event.sefActorEPProgramName) < 40 compute ( UserAgentShort.tags = "risk.indicator", -UserAgentShort.riskLevel = 1)
<b>Rule description in plain English:</b>	<i>Detects HTTP traffic with a user agent string less than 40 characters.</i>

1. From Oracle Management Cloud's home page, go to **Security Monitoring and Analytics, Security Admin**, and select **Correlation Rules**.
2. Expand rule set **Network** and select **UserAgentShort**.
3. Under **Parameters**:
  - Decrease the **Minimum Length** to 39.
4. To keep the new changes, click **Update**.

Notice how the description now reflects your new rule specifications.

<b>SEF expression:</b>	Pattern for UserAgentShort (SYSTEM.SEF as Event) where Event.sefTransportProtocol IN ("http", "https") AND StrLen(Event.sefActorEPProgramName) > 1 AND StrLen(Event.sefActorEPProgramName) < 39 compute ( UserAgentShort.tags = "risk.indicator", -UserAgentShort.riskLevel = 1)
<b>In plain English:</b>	<i>Detects HTTP traffic with a user agent string less than 39 characters.</i>

 **Note:**

Every time you update a correlation rule, Security Monitoring and Analytics increments the version number and enables the newly updated version by default.

5. To view or enable previous versions, select the tab **Versions** right under the correlation rule name.
  - a. Select a **Version** number to view version-specific rule specifications.

- b. Click **Enable** to activate the current selection.

 **Note:**

Only one version is enabled at a time per correlation rule.

## Tuning Rule Exceptions by Whitelisting Rule Attributes

To prevent triggering of a correlation rule or detected event, you implement rule exceptions by whitelisting the associated SEF attributes.

Whitelist entries require the following fields:

- **Attribute** — the SEF field the entry is matching against.
- **Format** — the type of matching being done (literal, regular expression, and CIDR notation).
- **Values** — will contain the items being whitelisted.

 **Note:**

Each whitelist entry can contain up to twenty, comma-separated, unique values.

As part of this task, you perform a whitelisting example where you tune the **UserAgentShort** rule by whitelisting *user agent strings*, known to be used on your network for legitimate purposes.

**Table 2-2 Required values for this example include:**

SEF field	Element Details
<code>sefActorEPPProgramName</code>	Whitelist specific user agents to a more tightly scope than from what's defined in the rule. <ul style="list-style-type: none"> <li>• Add the SEF attribute <code>sefActorEPPProgramName</code> with a regular expression.</li> <li>• <code>^soc@example.com 555-1212 ticket:[0-9]{6}</code></li> </ul>
<code>sefActorEPNwAddress</code>	Whitelist network attribute that contain each subnet being filtered out. <ul style="list-style-type: none"> <li>• Add the SEF attribute <code>sefActorEPNwAddress</code> with CIDR notation.</li> <li>• <code>10.242.0/24, 10.243.0/24, 10.23.100.0/22</code></li> </ul>

1. From Oracle Management Cloud's home page, go to **Security Monitoring and Analytics, Security Admin**, and select **Correlation Rules**.
2. Expand rule set **Network** and select **UserAgentShort**.

3. To add expression for `sefActorEPPProgramName`, click the **Add** button, under **Whitelists**.
  - a. Begin typing `sefActorEPPProgramName` in the **Attribute** field.
  - b. Select `Regular Expression` under **Format**.
  - c. Then enter a regular expression in the **Value** field, such as `^soc@example.com 555-1212 ticket:[0-9]{6}`.
4. To add expression for `sefActorEPNwAddress`, click the **Add** button once again.
  - a. Begin typing `sefActorEPNwAddress` in the **Attribute** field.
  - b. Select `CIDR` under **Format**.
  - c. Enter each of the static user agents as comma separated values in the **Value** field, such as `10.242.0/24, 10.243.0/24, 10.23.100.0/22`.



**Note:**

- All values are treated as "OR" condition.
- Maximum whitelists allowed: 5.

## Administer Machine Learning Capabilities

To leverage deep learning capabilities from Oracle Management Cloud's machine learning, you need to set your training stage with behavioral specifications.

Meet security requirements and stay compliant by managing and administering machine learning models. Perform tasks such as creating, updating, searching/inspecting, enabling/disabling model instances.

**Topics:**

- [Machine Learning Capabilities Overview](#)
- [Create a Peer Group Analysis Model](#)
- [Create an SQL Analysis Model](#)
- [Additional Machine Learning Features for Administrators](#)

## Machine Learning Capabilities Overview

This section gives you a conceptual understanding of attributes and other components that make up each machine learning model.

**Machine Learning-Based Anomaly Detection**

In order to successfully detect anomalies based on learned behavioral patterns from users and assets across your IT enterprise, Security Monitoring and Analytics uses **Peer Group Analysis** models and **SQL Analysis** models. These models are currently the only user-defined models in *machine learning-based anomaly detection*.

**Table 2-3 Detecting Anomalies Based on Machine Learning**


Description	Multidimensional Anomaly Detection	Data Access Anomaly Detection
<b>Security Monitoring and Analytics Machine learning model:</b> <b>Learning components:</b> <b>For example:</b>	<b>Peer Group Analysis model</b>  Authentication Event: Source and Destination IP  <i>"Diane G., a US-based employee, exhibited unusual login behavior when her account was used to log into the network from Tunisia.</i>	SQL Analysis model  Data Access - SQL command executed  <i>A SELECT * query was run against the finance database Customer table, and was detected as anomalous.</i>
<b>Security Monitoring and Analytics — machine learning model attributes:</b>	Security Model: <b>Authentication</b> <ul style="list-style-type: none"> <li>• <b>Username:</b> Authentication user</li> <li>• <b>Source IP:</b> IP address of the source machine</li> <li>• <b>Destination:</b> IP address of the destination machine or asset name</li> <li>• <b>Event Category:</b> Authentication</li> </ul> Security Model: <b>Data Access</b> <ul style="list-style-type: none"> <li>• <b>SQL Text:</b> SQL command executed</li> </ul>	Security Model: <b>Data Access</b> <ul style="list-style-type: none"> <li>• <b>SQL Text:</b> SQL command executed</li> </ul>

**What type of behavior do you need machine learning to learn about?**

I need machine learning to learn about...	Create...
A group of users and their typical activity behavior.	A <b>Peer Group Analysis</b> model as described in <a href="#">Create a Peer Group Analysis Model</a>
SQL execution patterns on a single database.	A <b>SQL Analysis</b> model as described in <a href="#">Create an SQL Analysis Model</a>

## Create a Peer Group Analysis Model

Create a Peer Group Analysis Model to better understand user behavioral patterns in your IT environment.

1. From Security Monitoring and Analytics, click the **Menu** icon , top-left under the product name.
2. Under **Security Admin**, select **Machine Learning Models**.
3. In the Machine Learning Models page, click **Create Model**, and then select **Peer Group Analysis**.
4. In the **Model Attributes** section:
  - Enter the name for your new model.
  - From the drop-down list, select a peer group.  
Peer groups are predefined based on your organization.
5. Click **Learning Parameters**.

6. Select a Security Model: **Authentication** or **Data Access**.

Based on the security model selected, Security Monitoring and Analytics determines the appropriate set of attributes to be extracted from base events (log entries), and ingests them to learn behavioral patterns. These attribute values are compared and contrasted among users that belong to the same peer group in order to detect anomalous behavior.

7. If you're creating a learning model based on an Authentication activity, then follow the steps in **a**. If you're creating a learning model based on data access activity (SQL activity associated with the entire peer group, and may involve one or more databases), then follow the steps in **b**.

**a.** Select **Authentication** as your **Security Model**, and then the following **Learning Attributes** are used to learn behavioral patterns:

- **Username:** Authentication user
- **Destination:** IP address of the destination machine or the asset name
- **Event Category:** Authentication

These attributes encompass all the user activity that machine learning needs to ingest in order to learn and start detecting anomalous behavior.

**b.** Select **Data Access** as your **Security Model**, and then the following **Learning Attributes** are used to learn behavioral patterns:

- **SQL Text:** SQL command executed

This attribute encompasses all the user activity machine learning needs to ingest in order to learn and start detecting anomalous behavior.

8. For **Frequency**, select either **Daily** or **Weekly**.

- The initial learning session begins immediately. Subsequent learning sessions begin at midnight. The duration of each learning session is 24 hours if **Daily** is selected, or 7 days if **Weekly**.
- Learning sessions are repeated indefinitely, unless the model is disabled.
- To enhance and expedite the learning process, up to 30 days of historical events are ingested as learning input, if sources are available.

9. For **Learning Period**, specify the value and select either Hours, Days, or Weeks from **Time Unit**


Note that learning will occur on the data gathered in the last x-amount of hours, days or weeks.

10. Click **Save**.

## Create an SQL Analysis Model

Create new SQL analysis models and define parameters and attribute relevant to your needs.

To create a machine learning model that focuses on a specific database and its typical query execution activity, and the number and order of SQL executions performed by mobile apps, web browsers, direct users, and so on:

1. From Security Monitoring and Analytics, click the **Menu** icon , top-left under the product name.

2. Under **Security Admin**, select **Machine Learning Models**.
3. In the Machine Learning Models page, click **Create Model**, and then select **SQL Analysis**.
4. In the **Model Attributes** section:
  - Enter the name for your new model.
  - From the drop-down list, select a database.

 **Note:**

Databases listed here *must* have auditing enabled, and have their audit logs collected by Log Analytics.

- (Optional) Enter the description of your new model.
5. Click **Learning Parameters**.

The Security Model is based on **Data Access**.

Data Access attributes contain data related to events that read, modify, or delete data, such as the SQL commands executed and the sequential order of execution.

The following **Learning Attributes** are used to learn behavioral patterns:

    - **SQL Text:** SQL command executed
  6. For **Frequency**, select either **Daily** or **Weekly**.
    - The initial learning session begins immediately. Subsequent learning sessions begin at midnight. The duration of each learning session is 24 hours if **Daily** is selected, or 7 days if **Weekly**.
    - Learning sessions are repeated indefinitely, unless the model is disabled.
    - To enhance and expedite the learning process, up to 30 days of historical events are ingested as learning input, if sources are available.
  7. For **Learning Period**, specify the value and select either Hours, Days, or Weeks from **Time Unit**

Learning will occur on the data gathered in the last x-amount of hours, days or weeks.
  8. Click **Save**.

## Additional Machine Learning Features for Administrators

This section provides a quick overview of other tasks in machine learning models.

- [Enable and Disable Models](#)
- [Search and View Models](#)

## Enable and Disable Models

You can toggle enable/disable models based on their current status.

1. From the tree view on the left side, select the model you want to enable or disable. Additionally, you can use the **Search** field.

- In the details section, on the top-right corner, click the toggle button to either **Enable** or **Disable** the selected model.

## Search and View Models

Search and view existing machine learning models

In the **Machine Learning Models** page, use the **Search** field to find the existing models. Alternatively, you can select models by using the tree list.



### Note:

You can add a search filter based on the models that are **Enabled Only** or **Disabled Only**.

## Perform Security Analysis

Use OMC tools and SMA's out-of-the-box dashboards to monitor security events and perform drill-down security analysis.

Task	More Information
Create an alert rule to trigger notifications based on your predefined security threshold values and severity levels.	<a href="#">Create a Security Alert Rule</a>
Use the Visualize panel of Oracle Log Analytics to present search data in a form that helps you better understand and analyze.	Visualize Data Using Charts and Controls in <i>Using Log Analytics</i>
Clustering uses machine learning to identify the pattern of log records, and then to group the logs that have a similar pattern.	Clusters Visualization in <i>Using Log Analytics</i>
You should use the SQL queries that are used to extract the data carefully.	SQL Query Guidelines in <i>Using Log Analytics</i>
Create and customize as many security dashboards as you need.	<a href="#">Security Dashboards</a>

## Customize Your Security Dashboards

Start with SMA's, out-of-the-box, default dashboards to begin with your security customization.

- Duplicate the desired (out-of-the-box) dashboard
- Personalize it
- Save it



# Security Intelligence Dashboard

SMA's dashboards analyze and monitor activity events from users and assets in your organization.

## Security Intelligence Dashboard

- [Overview](#)
- [Use Security Widgets to Analyze Suspicious and Malicious Activity](#)
  - [Triage widgets](#)
  - [Specific data elements widgets](#)
- [Other components not shown](#)

### Overview

The Security Intelligence dashboard displays information from log data that has been enriched by SMA's integrated threat intelligence service. These are primarily related to web traffic but can also include other log types that contain external (routable) IP addresses, domains, FQDNs or URLs like AV/HIPS, DLP, email, SSH, etc – Enabling analysts to view all relevant information regardless of the log type or source. The service can deliver over 80 different categories, most of which cover normal web activity like *personal finance, social media, dating, travel, music, etc.*

This dashboard focuses on two small subsets of categories known as *suspicious* and *malicious*, which are comprised of those most useful for security analysis.

The information related to each subset resides on separate dashboard tabs, **Suspicious** and **Malicious**, which share the same format.

- **Suspicious** tab - Focuses on domains and IPs related to: proxy, TOR, spam, adult, gambling, P2P, as well as dead or parked sites.
- **Malicious** tab - Focuses on domains and IPs related to: malware sites, phishing, botnets web attacks, windows exploits, and spyware. This view is further simplified by combining malware sites, windows exploits, and web attacks into a subcategory called 'Malware'. The full category names are listed in the table below.

For the full category list and category descriptions, see Appendix: [Security Intelligence Reference](#).

### Use Security Widgets to Analyze Suspicious and Malicious Activity

Analyze data across both tabs focusing on either suspicious or malicious activity

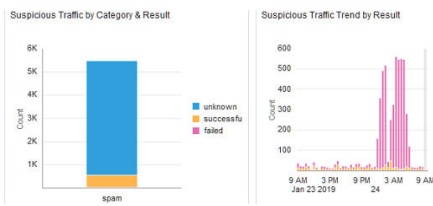
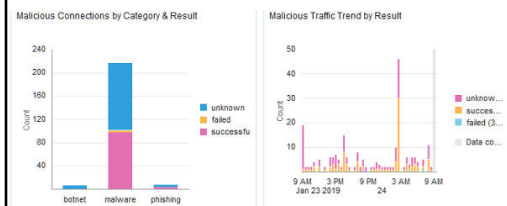
The data displayed on the Security Intelligence dashboard follows a distinct pattern, with the same widgets on both tabs, in the same order. The only difference is the focus on categories grouped as 'Suspicious' or 'Malicious' depending on the tab being viewed. General information in the first row provides a quick overview of the activity and to provide context for the rest of the widgets on the dashboard. The information gets more and more specific flowing towards a table at the bottom of the page containing individual data elements from the logs that populate the dashboard.

### Triage widgets

From this top row analysts should be able to quickly triage any activity of interest and gather the overall activity level, categories that may be of concern, whether those connections are successful or now, and where in the timeline being viewed shifts in successful/denied connections may have occurred. In a glance users should be able to identify key investigation elements and have a sense of whether deeper digging is required and the priority the investigation should be given.

<p style="text-align: center;"> <span style="color: blue; font-weight: bold; text-decoration: underline;">Suspicious</span>    Malicious         </p>	<p style="text-align: center;"> <span style="color: blue; font-weight: bold; text-decoration: underline;">Malicious</span>    Suspicious         </p>
<p><b>Figure 2-1 Overview of Suspicious vs Malicious Activity</b></p>	<p><b>Figure 2-2 Overview of Malicious vs Suspicious Activity</b></p>
<p>Tiles show:</p> <ul style="list-style-type: none"> <li>• an overview of <i>suspicious &amp; malicious</i> activity</li> <li>• <i>suspicious</i> traffic by category</li> </ul>	<p>Tiles show:</p> <ul style="list-style-type: none"> <li>• an overview of <i>malicious &amp; suspicious</i> activity</li> <li>• <i>malicious</i> traffic by category</li> </ul>

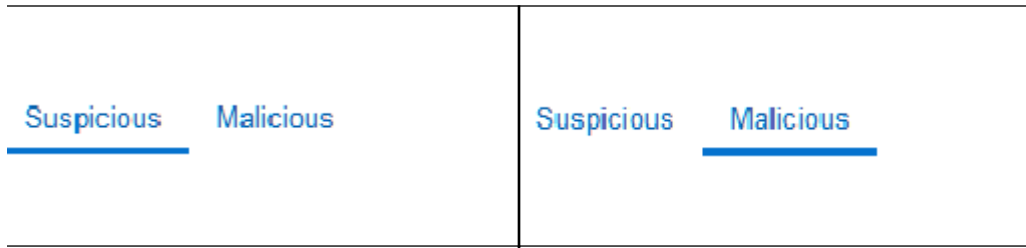
- The **Overview of Suspicious & Malicious/Malicious & Suspicious Activity** widget reveals the percentage of all logs currently being evaluated in the dashboard that are identified as Suspicious and Malicious, compared to all other logs containing an IP, Domain, or URL being categorized. This provides scale, and will be the first place to look for significant changes. Over time analysts will notice a normal range of percentages for Suspicious and Malicious categorizations seen on their network. Spikes outside this normal range are a warning sign that something may require investigating.
- The **Suspicious/Malicious Traffic by Category** widget displays the percentage of the logs with elements categorized as *Suspicious/Malicious* by category, providing a quick way to determine which specific categories of Suspicious or Malicious entities are involved in any spikes or shifts in expected levels. The specific categories involved will help analysts triage issues and prioritize their investigations. For example a spike in "dead/parked" sites seen may be an indication of an infected system beaconing to domains or IPs that are no longer active. While worth investigating this may not be as critical as a spike in other categories like Phishing or Malware which may pose a more immediate threat

<p><u>Suspicious</u>   Malicious</p>	<p>Suspicious   <u>Malicious</u></p>
<p><b>Figure 2-3 Suspicious Traffic by Category and Suspicious, and Traffic Trend by Result</b></p> 	<p><b>Figure 2-4 Malicious Connections by Category and Result, Malicious Traffic Trend by Result</b></p> 
<p>Tiles show <i>suspicious</i>:</p> <ul style="list-style-type: none"> <li>• traffic by category and result</li> <li>• traffic trend by result</li> </ul>	<p>Tiles show <i>malicious</i>:</p> <ul style="list-style-type: none"> <li>• traffic by category and result</li> <li>• traffic trend by result</li> </ul>

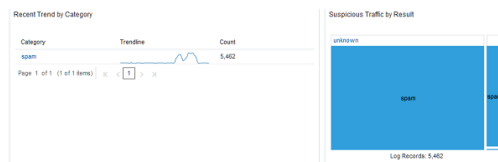
- The **Suspicious/Malicious Traffic by Category & Result** widget shows the percentage of each individual category that has been blocked or denied, vs those connections that were successful, or those where the relevant information isn't available in the logs. Again this information helps analysts triage spikes in activity quickly and prioritize which items require immediate attention.
- The **Suspicious/Malicious Traffic Trend by Result** widget illustrates the overall ratio of success/failed/unknown connections for all categories that make up the Suspicious grouping. This can assist analysts by quickly showing specific timeframes that may require deeper investigation helping to narrow the scope and amount of logs that need to be investigated.

**Specific data elements widgets**

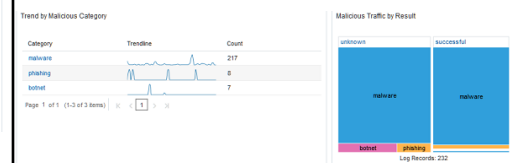
From this dashboard analysts can gather all the elements they need to evaluate activity of interest and gather all the relevant information required for deeper investigation if it is warranted. These details will help narrow the search if users need to pivot to the data explorer to dig into the data further and zero in on the related activity using more advanced queries and filters.



**Figure 2-5 Recent Trend by Category and Suspicious Traffic by Result**



**Figure 2-6 Trend by Malicious Category and Malicious Traffic by Result**



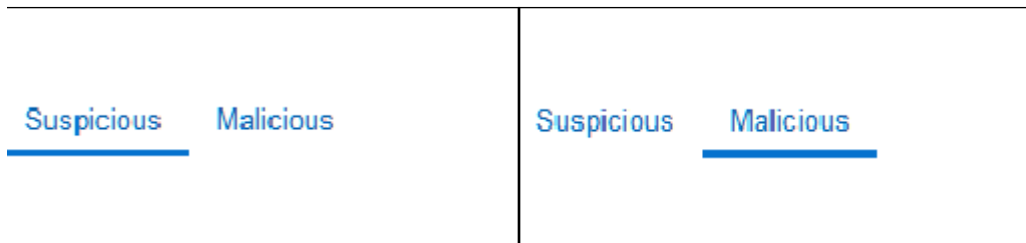
Tiles show:

- recent trend by category
- suspicious traffic by result

Tiles show:

- trend by malicious category
- malicious traffic by result

- The **Recent Trend by Category** widget shows the counts by individual category on a sparkline making spikes in activity related to each category easy to identify, helping to narrow the timeline of an investigation.
- The **Suspicious/Malicious Traffic by Result** widget provides a different view of the same data displayed in the widget above it "Suspicious/Malicious Traffic Trend by Result". Where the previous widget displayed the information on a timeline, this widget groups the counts of successful, failed or unknown traffic in groups. The size of each element shows the ratio of activity by category and result, giving analysts a better sense of the volume of each category and the number for those that were successful.





## Security Domains

Dashboard	Overview
<b>DNS</b>	Data extracted from a network's DNS logs, providing insight into an organizations Internet traffic. Information is displayed in a variety of ways to aid in determining a baseline of normal activity, investigating trends, and identifying anomalies that may warrant deeper investigation.
<b>Firewall</b>	Data extracted from a network's firewall logs. This dashboard is helpful for investigating enterprise wide trends across this family of network security products. Information about denied connection attempts, ports and protocols, source and destination IP addresses and more is collected and displayed in a variety of chart types to provide insight into this layer of an enterprise's network security.
<b>Host Security</b>	<p>Data extracted from SSH related logs, focusing on unsuccessful login attempts around three primary elements:</p> <ul style="list-style-type: none"> <li>• Actor IP - <code>source</code></li> <li>• Destination Name - <code>target host</code></li> <li>• Destination Account (the login is attempted with) - <code>account name</code></li> </ul> <p>The dashboard is split into three horizontal zones. The format of each zone is consistent, allowing the three histograms to line up displaying different aspects of the same activity on the same timeline to allow analysts to better understand the attacks they face and more easily spot suspicious activity.</p> <ul style="list-style-type: none"> <li>• <i>Zone 1</i> is focused on the Actor IP, which is the address the connection attempt emanated from. That information is displayed as a histogram showing the activity trend for the time frame being viewed, a pie chart displaying the most frequently seen Actor IPs, and table showing each source IP and the number of times SSH connection attempts were seen from that IP during the time frame being analyzed.</li> <li>• <i>Zone 2</i> is focused on the Destination IP, the network address of the system the SSH login was attempted.</li> <li>• <i>Zone 3</i> is focused on the Destination Account, which is the account name being used in each SSH connection.</li> </ul>

## Security Databases

Dashboard	Overview
<b>DB2 Database</b>	Data extracted from a network's DB2 database logs. Information about database accounts, schemas, data access and other aspects of an enterprise's DB2 databases are displayed in a variety of chart types.

<b>Dashboard</b>	<b>Overview</b>
	Together these different aspects related to all the DB2 databases on the network provide insight into the activity surrounding an organization's data.
<b>MySQL Database</b>	Data extracted from a network's MySQL database logs. Information about database accounts, schemas, data access and other aspects of an enterprise's MySQL databases are displayed in a variety of chart types. Together these different aspects related to all the MySQL databases on the network provide insight into the activity surrounding an organization's data.
<b>Oracle Database</b>	Data extracted from a network's Oracle database logs. Information about database accounts, schemas, data access and other aspects of an enterprise's Oracle databases are displayed in a variety of chart types. Together these different aspects related to all the Oracle databases on the network provide insight into the activity surrounding an organization's data.

## Security Dashboards

SMA's dashboards specialize in the security element of events generated by user and asset activity.

### Topics:

- [Dashboards Overview](#)
- [Customize Your Security Dashboards](#)
- [Security Intelligence Dashboard](#)

### Dashboards Overview

<b>Related Security Components</b>	<b>Associated Dashboards</b>
DNS, Firewall, SSH, Failed Logins	<a href="#">Security Domain Dashboards</a>
Oracle Database, DB2 Database, MySQL Database	<a href="#">Security Database Dashboards</a>
Security Intelligence	<a href="#">Security Intelligence Dashboard</a>

### Security Domain Dashboards

<b>Dashboard</b>	<b>Overview</b>
<b>DNS</b>	Data extracted from a network's DNS logs, providing insight into an organizations Internet traffic. Information is displayed in a variety of ways to aid in determining a baseline of normal activity, investigating trends, and identifying anomalies that may warrant deeper investigation.
<b>Firewall</b>	Data extracted from a network's firewall logs. This dashboard is helpful for investigating enterprise wide trends across this family of network

Dashboard	Overview
	<p>security products. Information about denied connection attempts, ports and protocols, source and destination IP addresses and more is collected and displayed in a variety of chart types to provide insight into this layer of an enterprise's network security.</p>
<p><b>Host Security</b></p>	<p>Data extracted from SSH related logs, focusing on unsuccessful login attempts around three primary elements:</p> <ul style="list-style-type: none"> <li>• Actor IP - <code>source</code></li> <li>• Destination Name - <code>target host</code></li> <li>• Destination Account (the login is attempted with) - <code>account name</code></li> </ul> <p>The dashboard is split into three horizontal zones. The format of each zone is consistent, allowing the three histograms to line up displaying different aspects of the same activity on the same timeline to allow analysts to better understand the attacks they face and more easily spot suspicious activity.</p> <ul style="list-style-type: none"> <li>• <i>Zone 1</i> is focused on the Actor IP, which is the address the connection attempt emanated from. That information is displayed as a histogram showing the activity trend for the time frame being viewed, a pie chart displaying the most frequently seen Actor IPs, and table showing each source IP and the number of times SSH connection attempts were seen from that IP during the time frame being analyzed.</li> <li>• <i>Zone 2</i> is focused on the Destination IP, the network address of the system the SSH login was attempted.</li> <li>• <i>Zone 3</i> is focused on the Destination Account, which is the account name being used in each SSH connection.</li> </ul>

### Security Database Dashboards

Dashboard	Overview
<p><b>DB2 Database</b></p>	<p>Data extracted from a network's DB2 database logs. Information about database accounts, schemas, data access and other aspects of an enterprise's DB2 databases are displayed in a variety of chart types. Together these different aspects related to all the DB2 databases on the network provide insight into the activity surrounding an organization's data.</p>
<p><b>MySQL Database</b></p>	<p>Data extracted from a network's MySQL database logs. Information about database accounts, schemas, data access and other aspects of an enterprise's MySQL databases are displayed in a variety of chart types. Together these different aspects related to all the MySQL databases on the network provide insight into the activity surrounding an organization's data.</p>



<b>Dashboard</b>	<b>Overview</b>
<b>Oracle Database</b>	Data extracted from a network's Oracle database logs. Information about database accounts, schemas, data access and other aspects of an enterprise's Oracle databases are displayed in a variety of chart types. Together these different aspects related to all the Oracle databases on the network provide insight into the activity surrounding an organization's data.

**Related Topics:**

- [Customize Your Security Dashboards](#)
- [Security Intelligence Dashboard](#)

# 3

## Investigating and Analyzing Threats Based on Correlation Rule

With Oracle Security Monitoring and Analytics, you can investigate unusual user activity, and analyze threats and anomalies found throughout your enterprise.

### Topics:

- [Investigate and Analyze Threats in Response to an Alert Notification](#)
- [Isolate Risky Users Associated with Threats](#)
- [Isolate Assets Associated with Threats](#)

## Investigate and Analyze Threats in Response to an Alert Notification

You can investigate and analyze threats starting with an alert notification.

For example, you receive an alert notification letting you know that there was a threat, and it was flagged with a risk level of medium. This alert occurred because it exceeded the risk level threshold that you configured in the alert rules. Based on the content of the email, you know general information, such as the threat ID, type of threat (for example, `TargetedAccountAttack`), severity level, and the time stamp of the occurrence.

Note that you must configure alert rules first. For details, see [Create a Security Alert Rule](#).

## Investigating Threats Detected by Correlation Rule

After you receive the alert notification, you want to identify and learn more about the threat details related to the user activity. You want to find out the nature of the threat, the threat category it falls under, how many users were involved, and so on.

1. In the **Threat Details** page, copy and paste the threat ID from the email to the **ID** filter field, and click **Apply**.

The **Description** column in **Threat Details** table shows the correlation rule that detected this threat. For a full list of correlation rules and their definitions, see [Security Correlation Rule System](#).

Note that in this example, the threat was detected by the correlation rule `TargetedAccountAttack`; the category is `infiltration`; and it's composed of 8 activities.

2. To find out if this threat activity was based on one or multiple users, click the item number in the **Activities** column.

To help you with your investigation, the **Activity Explorer** page includes two interactive charts and one table.

3. To view all the activity events within this threat, use the **Activity Timeline** chart. To get details about threat events, use the **Threat Timeline**.
  - a. In order to focus on specific sections of the timeline, the **Zoom In/Out** buttons (toward the left side of the chart) can be used, or the **Time Selector** can be adjusted to show a more narrow time range.
  - b. By default, the **Selected Threats** button is active. If you want to include all other typical security events during this time range, click the **All Activities** button.

You can investigate event activity by selecting the solid circles, grouped by category, in the **Activity Timeline** chart, and by referring to the **Activity Details** table for deeper context.

4. To show **Activity Details** only for that user, while the **Selected Threats** button is selected, click any solid circle. Additionally, you can select multiple activity events (solid circles). Click anywhere on the chart. To close the rectangular selection, click again. The table refreshes showing the details that pertain to your selection only. Click anywhere on the graph to deselect activity events.

Now you know what users were involved, and the type of activity events that make up this threat.

These investigation steps quickly uncovered the following details:

- Asset `finance1.host.oracle.com` was affected.
- A single user was involved.
- The duration of the threat was approximately 6 seconds.
- This threat is categorized as `infiltration`.
- It was generated because of multiple failed account logins (according to the correlation rule `TargetedAccountAttack`).

## Investigating and Analyzing Users Associated with Threats

After you collect security details about the threat, you can start investigating and analyzing the associated users.

You proceed with your investigation by collecting more security-based details about this group of users. After completing this task, you'll be able to identify which users are involved and what organizations they belong to, understand their unusual activity patterns and associations with other threats or anomalies, and so on.

It's assumed that you know (from the notification email):

- Threat ID
  - Time of occurrence
1. In the **Threat Dashboard** page, click the **View List** button, and copy and paste the threat ID from the email to the **ID** filter field, and click **Apply**.
  2. To get a list of the users involved, click the threat **ID** shown in the **Threat Details** table.

To help you with your investigation, the **Activity Explorer** page includes a table with threat details, enabling you to drill down further.

3. To see the user details, click a **User** from the **Activity Details** table.

4. From the **User Details** page, you can get general user information, and you can cycle through its tabs to learn about:
  - **Summary** — data related to threats and risky assets
  - **Threats** — associated with this user
  - **Assets** — affected by threats associated with this user
  - **Accounts** — that belong to this user, including associated threats per account
  - **Roles** — assigned to this user
  - **Groups** — that this user belongs to
5. To learn details about other users associated with this threat, repeat Step 3.

## Isolate Risky Users Associated with Threats

You can analyze user activity by isolating users based on criteria required by your particular investigation or type of analysis.

For example, after receiving a notification email and learning more about the threat detected, you want to find out if this user (or users) is on the **Top Risky Users** list. Then, you want to gather a list of users based on the organization that contains the most risky users, and, within this organization, generate a list of users (and identify the asset) that were part of the highest threat attack on a single asset.

To quickly find the top 5 risky users, look at the **Top Risky Users By Threats** tile in the **Users** dashboard.

The pie chart is made up of slices that represent the top affected user organizations based on the number of risky users. You also learn that the user from the notification email is part of the top risky users by looking at the **Top Risky Users by Threats** tile.

1. To start filtering data, click the pie slice that represents the marketing department in the **Risky Users By Organization** chart.

The users dashboard updates, and shows data that pertains to the selected user's organization only.

2. To see the full list of risky users within the selected organization, click the risky users number in the **Risky Users Summary** tile. Alternatively, you can click the **List View** icon, top-right corner under the **Time Selector**.

The **Users** page includes two charts and table:

- **Threats By Top Risky Users** histogram — shows threat activity. Bar segments represent activity by each risky user. You can click any segment to apply a filtering layer and have the entire page show data that pertains to the selected user only.
- **Threats By All Risky Users** histogram — shows a visual representation of threats. It starts with the selected **Risky Users** (bar fill-in), and each bar has an outline that represents the other (additional) risky users. Overall, a bar represents the total number of risky users at a given time period.
- **Risky User Summary** table — based on your filtering criteria (selected users versus one user). The table includes key information such as:
  - **User Name** — takes you to the **User Details** page, where you can get information such as asset and threat associations and a summary of user activity.

- **Threats** — takes you to the **Threats** page, where you can learn about all the threats associated with this user.
3. To view the data about a particular user, click any bar segment in the **Threats By Top Risky Users** chart.

The **Threats By Top Risky Users** chart now shows more detailed data that pertains to this user only. The **Threats By All Risky Users** chart highlights the selected user and includes the threat activity from other users.
  4. Go back to the initial group of users, and remove the **Filter Term** that starts with "User Name=".
  5. To go back to the dashboard view, click the **Graphical View** icon, at the top, right corner under the **Time Selector**.
  6. To view data based on these users and the most risky asset, click the bar with the highest number of threats found in the **Top Risky Asset By Threats** tile.

The entire dashboard gets updated, representing data based on your filtering criteria.
  7. Now, you can use the information in the **Users Summary** tile to:
    - Get asset information such as threat and user associations.
    - See a list of users and conduct further data manipulation.
    - See a list of threats associated with this group of users and the selected asset.

## Isolate Assets Associated with Threats

You can investigate asset activity and analyze assets by isolating affected assets.

For example, after receiving a notification email and learning more about the threat detected, you want to find out if these assets are part of the **Top Risky Assets** list. You also want to gather a list of individual assets based on the asset type that had the highest number of threat attacks, or you want to generate a list of individual threats that made up the highest number of threat attacks on assets grouped by asset type (for example, asset type Linux Servers).


In the **Assets** dashboard, you can quickly find the top 5 risky assets in the **Top Risky Assets By Threats** tile.

To start narrowing down on the threat attacks, click the largest pie slice in the **Risky Assets By Asset Type** chart.

The dashboard refreshes and shows data that pertains to risky assets according to your latest selection.

1. To start narrowing down on the threat attacks, click the largest pie slice in the **Risky Assets By Asset Type** chart.

The dashboard refreshes and shows data that pertains to risky assets according to your latest selection. Now, you can learn the top threat categories distributed among the risky assets within the selected asset type (for example, asset type `host`). The **Threats by Asset Type** tile shows the total number of threats associated with the asset type `host`.
2. To see the **Risky Assets** list, you can either select the number from the **Assets** mini tile, or click the **List View** icon, top-right under the **Time Selector**.

3. To generate a list of threats associated with the largest asset type affected, remove the filter element in the filter bar, and then click the largest pie slice in the **Threats By Asset Type** chart. Alternately, you can click the **Remove** icon .
4. To see the full **Threats** list for each asset within the selected category, click the threats number in the **Risky Asset Summary** table.
5. You can break down your **Threats** list further by adding the following filtering layers: in the filter field **Destination** and **User**, add the asset name and user name (for example, `Destination=finance1.host.oracle.com` and `User=John_Doe@oracle.com`).

Now, the list only shows threats associated with the specified asset and user.

This is one of many drilldowns that Security Monitoring and Analytics enables you to perform during your security-based investigations. Here, you started analyzing data by filtering data that only pertains to the asset type most affected by threats. You then applied additional threat filters to refine your list based on an asset and user (both within the most affected asset type list). You can continue your investigation and analysis by applying more drilldowns, and gather details, such as what threat associations the asset and the user have in common, and what unusual activity was monitored and logged over a period of time for each, individually.

# A

## Configuration of Security Log Sources

Log source specifications and configuration support for log collection.

[Database Sources](#) | [Host Sources](#) | [Security Device Sources](#) | [Web Application Server Sources](#)

### Database Sources

Vendor	Log Type	Log Location/ Name	Supported Versions	Supported Platform
IBM	IBM DB2 Audit	{inst_home} /sqllib/ db2dump/ db2diag*.log	-	Linux, AIX, Windows
Microsoft	Microsoft SQL Server Audit	Object Explorer > Security > Audits folder	-	-
MySQL	MySQL Audit Log	/var/lib/ mysql/ audit*.log	5.5	-
Oracle	Oracle Database Alert	{diagnostic_dest}/ diag/rdbms/ <db_unique_name>/ <instance_name>/trace	12.1	AIX, HPUX, Linux, Solaris, Windows
Oracle	Oracle Database Listener	{log_dir_path}/*.xml	12.1	AIX, HPUX, Linux, Solaris, Windows
Oracle	<a href="#">Oracle Database Audit Trail</a> 11g- .AUD, XML File Audit, Oracle Audit 12c and 18c- .AUD, XML, Unified Audit Trail, Audit Records	{audit_dest}/*.aud	11.2 & 12.1	Linux, Solaris, Windows
Oracle	Oracle TNS Trace	{trace_dir_path}/*.log	12.1	AIX, HPUX, Linux, Solaris, Windows

## Host Sources

Vendor	Log Type	File Name/ Location	Supported Versions	Supported Platform
IBM	AIX Audit	/audit/ *.out	6.1	AIX
Oracle	Linux Audit	/var/log/ audit/ audit*	-	Linux
Oracle	Linux DHCP	<Configur ed to write to Syslog>	-	Linux
Oracle	Linux DNS (BIND)	<Configur ed to write to Syslog>	-	Linux
Oracle	Linux Maillog	/var/log/ maillog*	-	Linux
Oracle	Linux Syslog	/var/log/ messages*	-	Linux
Oracle	Linux SUDO	/var/log/ sudo.log*	-	Linux
CentOS	Linux YUM	/var/log/ yum.log*	-	Linux
Microsoft	Microsoft DHCP	%windir% \System32 \Dhcp	-	Windows Server
Microsoft	Microsoft Active Directory Audit		208, 2008 R2	
Oracle	Solaris Audit	/var/ audit/ audit*	12.1	Linux, Solaris, Windows
Oracle	Solaris Syslog	<Configur ed to write to Syslog>	-	Linux
Ubuntu	Ubuntu Secure	/var/log/ secure	-	Ubuntu
Ubuntu	Ubuntu Syslog	/var/log/ syslog	-	Ubuntu



## Security Device Sources

Vendor	Log Type	User	Supported Versions	Supported Platform
Blue Coat	Bluecoat Proxy	/var/log/bluecoat/w3c* & c:\bluecoatLog\w3c*	SGOS 6.5 and later	AIX, HPUX, Linux, Solaris, Windows
Cisco	Cisco ASA Firewall	<Configured to write to Syslog>	9.5	N/A
Cisco	Cisco ASA VPN	<Configured to write to Syslog>	9.5	N/A
Check Point	Check Point Firewall LEA Log Format	-	R77.30	AIX, Linux, Solaris, Windows
F5 Networks	-	/var/log	11	HO-UX, AIX, Linux, Solaris
Fortinet	Fortinet FortiGate Firewall	Configured to write to Syslog: /var/log/Fortinet.*	FortiGate 5.6.0 - 5.2	VMware ESXi v4.0 and newer, Microsoft Hyper-V 2008R2 and newer, Fortinet FortiHypervisor v1.0 and newer
IBM	Qradar Leef	/var/log/qradar.log	-	AIX, Linux, Solaris, Windows
netfilter	ipTables	/var/log/iptables*	-	Linux
Open Source	ipTraffic	/var/log/iptraf/ip_traffic.log	1.3 and later	Linux
Palo Alto Networks	Palo Alto Firewall	-	PAN - OS 7.1	PA-200, PA-500, PA-2000 Series, PA-3020, PA-3050, PA-3060, PA-4000 Series, PA-5000 Series, PA-7050, PA-7080, and all the Virtual Appliances.

## Web Application Server Sources

Vendor	Log Type	Log Location/Name	Supported Versions	Supported Platform
Oracle	FMW Oracle Access Manager (OAM) Audit	{oracle_instance}/auditlogs/OAM/{ias_internal_name}/audit*.log	12.1	Linux, Solaris, Windows

Vendor	Log Type	Log Location/Name	Supported Versions	Supported Platforms
Oracle	FMW Oracle HTTP Server (OHS) Access	{ohs_home}/servers/{component_name}/logs/access_log*	11.2	Linux, Solaris, Windows
Oracle	FMW Oracle HTTP Server (OHS) Admin	{ohs_home}/servers/{component_name}/logs/admin_log*	11.2	Linux, Solaris, Windows
Oracle	FMW Oracle Internet Directory (OID) Audit	{oracle_instance}/auditlogs/OID/{ias_internal_name}/audit-pid*.log	12.1	Linux, Solaris, Windows
Oracle	FMW WLS Server Access	{ohs_home}/diagnostics/logs/OHS/{component_name}/access_log*	12.1	Linux, Solaris, Windows
Apache	Tomcat Access	/var/log/<tomcat_version>/access.log	-	Linux, Windows
Apache	Tomcat Catalina V8.5	\${catalina_base}/logs/catalina	-	Linux, Windows
Apache	Tomcat Host	/var/log/tomcat7/*.log	-	Linux, Windows
Apache	Tomcat Manager V9	/var/log/<tomcat_version>/manager.log	-	Linux, Windows

## Configuration Quick-Start Guides

Step-by-step log configuration for supported for log sources.

### All Oracle Log Sources

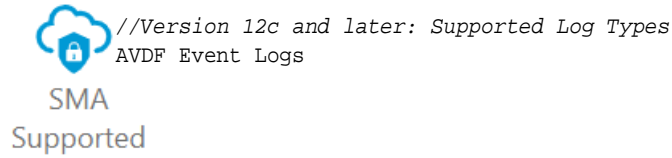
[Oracle Database Audit Trail , AVDF](#)

### Log Sources From Other Vendors

<a href="#">Host Sources</a>	<a href="#">Collect Linux Default Logs</a> , <a href="#">Collect Windows Default Logs</a>
<a href="#">Security Device Sources</a>	<a href="#">Bluecoat Proxy</a> , <a href="#">Cisco ASA Firewall</a> , <a href="#">Fortinet FortiGate Firewall</a> , <a href="#">Palo Alto Firewall</a>
<a href="#">Web Application Server Sources</a>	<a href="#">Apache Tomcat</a>

# Oracle Audit Vault and Database Firewall

[Related Documentation](#) | [Oracle Management Cloud Configuration Steps](#) | [Implementation and Setup Profile](#)



## Implementation and Setup Profile

Source Implementation	Handshake Implementation
Source output: AVDF Event Logs Source logs: AV server configuration	Source side:: AV Host with AVDF events stored in database and cloud agent installation Cloud side: AVDF Event in Oracle Database database instance

## Oracle Management Cloud Configuration Steps

AVDF Logs	Task Details and Requirements	Supporting Documentation
1. Confirm that your environment meets the prerequisites. – Install an Oracle Management Cloud agent on the Audit Vault Server host.	Ensure that you perform any tasks that correspond to missing requirements, if any. – The cloud agent must have access to the AVSYS . EVENT_LOG table to upload data to Oracle Management Cloud. Events related to your Oracle Database are collected via the EVENT_LOG table.	– <a href="#">Prerequisites and Requirements for Security Sources</a> See your database documentation on enabling auditing.
2. Register the Audit Vault Server database credentials in the agent store.	-	– Provide the Database Entity Credentials in <i>Using Oracle Log Analytics</i>
3. Discover the Audit Vault Server database in Oracle Management Cloud.	-	Discover Oracle Database Systems in <i>Using Oracle Infrastructure Monitoring</i>
4. Associate this Audit Vault database instance with the Audit Vault Server host.	Associate the new database entity with log source: AVDF Event in Oracle Database	– Configure New Entity Associations in <i>Using Oracle Log Analytics</i> – <a href="#">Database Sources</a>
5. Validate your log collection.	Confirm your setup was successful.	– <a href="#">Validate Log Collections</a>

## Related Documentation

Setup and configuration details from vendors and related sources.

- [Supported Server Platforms](#)
- [Audit Collection: Supported Secured Target Types and Versions](#)
- [Database Firewall Protection: Supported Secured Target Types and Versions](#)
- [Audit Vault Agent: Supported Platforms and Versions](#)

## Oracle Database

This section provides configuration details for collecting Oracle Database logs data.

### Support Specifications

Version:

- **11g** - .AUD, XML File Audit and Oracle Audit
- **12c and 18c** - .AUD, XML and Oracle Database Unified Audit Trail

### Setup Prerequisites

Prerequisite	Description	For additional details, see...
Access Oracle Management Cloud	Create an Oracle Cloud account and an OMC instance.	<a href="#">How Do I Access Oracle Management Cloud? in <i>Managing and Monitoring Oracle Cloud About Roles and Users</i></a>
Cloud agent(s) installed and Log Analytics licensing enabled	<ul style="list-style-type: none"> <li>- Install a cloud agent on the host where an Oracle database is installed.</li> <li>- Ensure that the agent has access to the database log files.</li> </ul>	Install the Cloud Agent and Enable Oracle Log Analytics in <a href="#">Using Log Analytics Environment Requirements in <i>Installing and Managing Oracle Management Cloud Agents</i></a>
Security Monitoring and Analytics licensing enabled	<b>Navigate to the OMC main menu &gt; Administration &gt; Entity Configuration.</b> On the Licensing page, click DISABLED in the SMA Enrichment tile. Toggle and Apply.	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <a href="#">Getting Started with Oracle Management Cloud</a>
Auditing enabled on your Oracle Database	Oracle database auditing is enabled by default. However, unified auditing is disabled by default starting with version 12c, where it was first introduced.	See your Oracle Database documentation for more details.

## Configuration Steps

STEP	Task Details / Requirements	For more details, see...
<b>STEP 1.</b> - Add the Oracle database <b>credentials</b> to the OMC cloud agents.	This is required if your audit data is stored in the Oracle Database.	Providing Entity Credentials section in Set Up Database Instance Monitoring in <i>Using Oracle Log Analytics</i>
<b>STEP 2.</b> - Add and <b>Discover</b> the Oracle database from your Management Cloud console.	Add a new database entity to your OMC environment then associate with your newly discovered Oracle database.	Add Entities for Infrastructure Monitoring in <i>Using Oracle Infrastructure Monitoring</i>
<b>STEP 3.</b> - Review existing log sources supported in Log Analytics and <b>associate</b> your database entity with the Oracle database log sources. Note: Several database auditing sources are supported out of the box.	Your newly added database entity must generate a log type that matches with one supported by OMC. Navigate to <b>Log Analytics &gt; Log Admin &gt; Sources</b> , and <i>search</i> for <b>Entity Type = Oracle Database Instance</b> . For example, select the <i>Oracle DB Audit Log Source Stored in the Database</i> , or <i>Database Audit XML Logs</i> . Audit data will be extracted from the Oracle database based on the SQL query provided in the log source configuration.	Work with Entity Associations in <i>Using Log Analytics</i>
<b>STEP 4.</b> - <b>Validate</b> your log collection in Security Monitoring and Analytics.	To ensure all setup is complete, validate your collection. Navigate to <b>Security Analytics &gt; Security Data Explorer</b> .	<a href="#">Validate Log Collections</a>

For additional compatibility info, see [Database Sources](#).

## Bluecoat Proxy

This Quick Start Guide provides log configuration details for SMA support: W3C and SQUID using FTP hosting (Linux/Windows).

### Support Specifications:

Version: 6.5 and later

### Configuration Prerequisites:

Prerequisite	Description	For additional details, see...
1. Access to Oracle Management Cloud	You must have an Oracle Cloud account containing an OMC instance with administrator privileges.	How Do I Access Oracle Management Cloud? in <i>Managing and Monitoring Oracle Cloud</i> <a href="#">About Roles and Users</a>

Prerequisite	Description	For additional details, see...
2. The FTP Server configured with default settings	The FTP server is your log host ( <i>OMC entity</i> ), where log sources upload and store logs.	Deploy an FTP Server in Symantec's <i>Reporter 10.x WebGuide</i>
3. Cloud agent(s) installed and Log Analytics licensing enabled	Have a Cloud Agent installed on the FTP server. This host will be discovered as an entity in OMC.	Install the Cloud Agent and Enable Oracle Log Analytics in <i>Using Log Analytics Environment Requirements in Installing and Managing Oracle Management Cloud Agents</i>
4. Security Monitoring and Analytics licensing enabled	Note that SMA Data Enrichment is disabled by default.	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <i>Getting Started with Oracle Management Cloud</i>

### Configuration Steps:

Procedure	Task requirements	For additional details, see...
<b>STEP 1. - Configure</b> the Blue Coat SG proxy to upload logs to your FTP server ( <i>OMC entity</i> ).	Ensure that your logs provide the <i>field list</i> and data format as indicated in the <a href="#">W3C Logs Format</a> and <a href="#">SQUID Logs Format</a> section.	Upload Access Logs to FTP Server in Symantec's <i>Reporter 10.x WebGuide</i>
<b>STEP 2. - Add an Entity Association</b> to support the new logs in OMC using Log Analytics.	Associate Bluecoat Proxy W3C Logs and/or Bluecoat Proxy SQUID Logs with your OMC entity (the FTP server where you installed the OMC agent). Ensure that the logs follow the formats as listed below, accordingly. <b>Note:</b> the log directory under <b>File Name Pattern</b> must align with the logs directory on your FTP server.	<a href="#">Security Device Sources</a> Associating Log Sources to Existing Entities in <i>Using Oracle Log Analytics</i>
<b>STEP 3. - Validate</b> your log collection.	Confirm your setup was successful.	<a href="#">Validate Log Collections</a>

### W3C Logs Format

Field list order and data format for Bluecoat Proxy W3C Logs

```
date time time-taken c-ip sc-status s-action sc-bytes cs-bytes cs-method cs-uri
cs-username s-hierarchy s-supplier-name rs(Content-Type) cs(User-Agent)
sc-filter-result sc-filter-category x-virus-id s-ip s-sitename
x-virus-details x-icap-error-code x-icap-error-details
```


## SQUID Logs Format

Format for Bluecoat Proxy SQUID Logs

```
%g %e %a %w/%s %b %m %i %u %H/%d %c
```

## Apache Tomcat

[Implementation and Setup Profile | Oracle Management Cloud Configuration Steps | Supported Log Format Specifications](#)

 <b>SMA</b> Supported	<i>//Version 8.5 and later, Supported Log Types:</i> Tomcat Access, Tomcat Catalina V8.5, Tomcat Host, Tomcat Manager V9
--	---

### Implementation and Setup Profile

Source Implementation	Handshake Implementation
Source output: See <a href="#">Supported Log Format Specifications</a>	Source-end: Host configured with a cloud agent and logging directory
Source logs: Local platform logs	Cloud-end: <b>File Pattern</b> with matching log directory for each log type

### Oracle Management Cloud Configuration Steps

Apache Tomcat	Task Requirements	Supporting Documentation
1. Confirm that your environment meets the <b>prerequisites</b> .	Ensure you perform any tasks that correspond to missing requirements, if any.	– <a href="#">Prerequisites and Requirements for Security Sources</a>
2. Associate the new Apache Tomcat Web Logic Server in Oracle Management Cloud.	Add associations for the host entity with the following supported log sources: <ul style="list-style-type: none"> <li>– Apache Tomcat Access Logs</li> <li>– Apache Tomcat Catalina Logs</li> <li>– Apache Tomcat Host Logs</li> <li>– Apache Tomcat Manager Logs</li> </ul>	– <a href="#">Security Device Sources</a> – <a href="#">Associating Log Sources to Existing Entities in Using Oracle Log Analytics</a>
3. Validate your log collection.	Confirm your setup was successful.	– <a href="#">Validate Log Collections</a>

### Supported Log Format Specifications

#### Tomcat Access

Apache Tomcat WebServer Access Log

### Tomcat Catalina V8.5

Apache Tomcat WebServer Catalina Log Format (v8.5 and v9)  
Apache Tomcat WebServer Catalina Log Format

### Tomcat Host

Apache Tomcat WebServer Catalina Log Format (v8.5 and v9)  
Apache Tomcat WebServer Host Log

### Tomcat Manager V9

Apache Tomcat WebServer Manager Format  
Apache Tomcat WebServer Manager v9 Format

Log Type	Supported Formats / Out-of-the-Box Parsers
<b>Tomcat Access</b>	Apache Tomcat WebServer Access Log
<b>Tomcat Catalina V8.5</b>	Apache Tomcat WebServer Catalina Log Format (v8.5 and v9) Apache Tomcat WebServer Catalina Log Format
<b>Tomcat Host</b>	Apache Tomcat WebServer Catalina Log Format (v8.5 and v9) Apache Tomcat WebServer Host Log
<b>Tomcat Manager V9</b>	Apache Tomcat WebServer Manager Format Apache Tomcat WebServer Manager v9 Format

## Cisco ASA Firewall

This Quick Start Guide provides log configuration details for SMA support: Cisco ASA SMA using FTP hosting (Linux).

### Support Specifications:

Version: Cisco ASA 5.2 - 5.6

### Configuration Prerequisites:

Prerequisite	Description	For additional details...
1. Access to Oracle Management Cloud	You must have an Oracle Cloud account containing an OMC instance with administrator privileges.	How Do I Access Oracle Management Cloud? in <i>Managing and Monitoring Oracle Cloud About Roles and Users</i>
2. The FTP Server configured with default settings	The FTP server is your log host ( <i>OMC entity</i> ), where log sources upload and store logs.	See FTP Server documentation provided by your vendor.




Prerequisite	Description	For additional details...
3. Cloud agent(s) installed and Log Analytics licensing enabled	Have a Cloud Agent installed on the FTP server. This host will be discovered as an entity in OMC.	Install the Cloud Agent and Enable Oracle Log Analytics in <i>Using Log Analytics Environment Requirements in Installing and Managing Oracle Management Cloud Agents</i>
4. Security Monitoring and Analytics licensing enabled	Note that <b>SMA Data Enrichment</b> is disabled by default.	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <i>Getting Started with Oracle Management Cloud</i>

### Configuration Steps:

Cisco ASA Firewall data config.	Task requirements	For additional details, see...
<b>STEP 1. - Configure</b> your Cisco ASA firewall to upload logs to your FTP server ( <i>OMC entity</i> ).	-	<a href="#">Configuring System Message Logging in Catalyst 3750-X and 3560-X Switch Software Configuration Guide</a>
<b>STEP 2. - Add an Entity Association</b> to support the new logs in OMC using Log Analytics.	Associate Cisco ASA Logs with your OMC entity (the FTP server where you installed the OMC agent). <b>Note:</b> the <b>File Name Pattern</b> (directory) parameter must match with your FTP server.	<a href="#">Security Device Sources</a> Associating Entities to Existing Log Sources in <i>Using Oracle Log Analytics</i>
<b>STEP 3. - Validate</b> your log collection.	Confirm your setup was successful.	<a href="#">Validate Log Collections</a>

## F5 Big Firewall

[Implementation and Setup Profile](#) | [Oracle Management Cloud Configuration Steps](#) | [Related Documentation](#)

 <b>SMA</b> Supported	<pre>//Version 11: Supported Log Types F5 Big IP Syslog Format, Syslog Format Logs</pre>
--	--

### Implementation and Setup Profile

Source Implementation	Handshake Implementation
Source output: BIGIPsyslog	Source side: Cloud agent listening for syslog messages on the associated host

Source logs: Remote logging using syslog forwarding	Cloud side: syslog listener
---	-----------------------------

## Oracle Management Cloud Configuration Steps

F5 Big Firewall Logs	Task Details and Requirements	Supporting Documentation
1. Confirm that your environment meets the prerequisites.	Ensure you perform any tasks that correspond to missing requirements, if any. – An Oracle Management Cloud agent must be installed on the Syslog server host.	– <a href="#">Prerequisites and Requirements for Security Sources</a>
2. Associate the new <i>F5 Big Firewall</i> source with the host where the agent is located in Oracle Management Cloud.	Add this association using the syslog listener for: F5 Big IP Logs	– <a href="#">Security Device Sources</a> – Associating Log Sources to Existing Entities in <i>Using Oracle Log Analytics</i>
3. Validate your log collection.	Confirm your setup was successful.	– <a href="#">Validate Log Collections</a>

### Related Documentation

- For firewall configuration details, see [About Logging](#) in *Security Logs and Checkpoint Firewall-1*

## Fortinet FortiGate Firewall

This Quick Start Guide provides log configuration details for SMA support: Fortinet Log Event Logs using Syslog hosting (Linux).

### Support Specifications:

Version: FortiGate 5.2 - 5.6

### Prerequisites:

To complete this task, you must have an Oracle Cloud account containing an OMC instance with administrator privileges.

Prerequisite	Description	For additional details...
1. Access to Oracle Management Cloud	You must have an Oracle Cloud account containing an OMC instance with administrator privileges.	How Do I Access Oracle Management Cloud? in <i>Managing and Monitoring Oracle Cloud About Roles and Users</i>

Prerequisite	Description	For additional details...
2. Cloud agent(s) installed and Log Analytics licensing enabled	Have a Cloud Agent installed on the FTP server. This host will be discovered as an entity in OMC.	Install the Cloud Agent and Enable Oracle Log Analytics in <i>Using Log Analytics Environment Requirements in Installing and Managing Oracle Management Cloud Agents</i>
3. Security Monitoring and Analytics licensing enabled	Note that <b>SMA Data Enrichment</b> is disabled by default.	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <i>Getting Started with Oracle Management Cloud</i>

### Configuration Steps:

Fortinet Firewall	Task requirements	For additional details, see...
<b>STEP 1. - Configure</b> your syslog server.	<ul style="list-style-type: none"> <li>– Redirect logs to file: <code>/var/log/fortinet.*</code></li> <li>– Be configured to receive logs via UDP</li> <li>– Have an OMC cloud agent installed.</li> </ul>	Syslog server documentation provided by your vendor. Install Cloud Agents in <i>Installing and Managing Oracle Management Cloud Agents</i>
<b>STEP 2. - Configure</b> your firewall to upload logs to your Syslog server ( <i>OMC entity</i> ).	Send Syslog events from your Fortinet Firewall to your remote Syslog Server host using UDP.	<a href="#">Logging and Reporting</a> in <i>FortiOS Handbook</i> . and <code>syslogd</code> in <i>FortiOS CLI Reference</i>
<b>STEP 3. - Add an Entity Association</b> to support the new logs in OMC using Log Analytics.	Associate Fortinet Log Event Logs with your OMC entity (the Syslog server where you installed the OMC Cloud Agent).	<a href="#">Security Device Sources</a> Associating Log Sources to Existing Entities in <i>Using Oracle Log Analytics</i>
<b>STEP 4. - Validate</b> your log collection.	Confirm your setup was successful.	<a href="#">Validate Log Collections</a>

## MS Active Directory

This Quick Start Guide provides configuration details for SMA support:: Windows Security Events using Windows Event Forwarding (Windows).

### Support Specifications:

Version: Windows Server 2008 and later

### Configuration Prerequisites:

Prerequisite	Description	For additional details, see...
1. Access to Oracle Management Cloud	You must have an Oracle Cloud account containing an OMC instance with administrator privileges.	How Do I Access Oracle Management Cloud? in <i>Managing and Monitoring Oracle Cloud About Roles and Users</i>
2. The dedicated Windows server configured with default settings	This is where the logs are being stored.	<a href="#">Install and Deploy Windows Server</a> in <i>Windows Server 2008 R2 and Windows Server 2008</i>
3. Cloud agent(s) installed and Log Analytics licensing enabled	The dedicated Windows host that's running Windows Event Collector. This host will be discovered as an entity in OMC.	Install the Cloud Agent and Enable Oracle Log Analytics in <i>Using Log Analytics Environment Requirements</i> in <i>Installing and Managing Oracle Management Cloud Agents</i>
4. Security Monitoring and Analytics licensing enabled	Note that <b>SMA Data Enrichment</b> is disabled by default.	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <i>Getting Started with Oracle Management Cloud</i>

### OMC Configuration Steps:

Windows Events Config.	Task requirements	For additional details, see...
<b>STEP 1. - Enable</b> Windows Event Forwarding and Auditing is enabled on the dedicated Windows host.	Configure your audit and forwarding policies based on your environment requirements.	<a href="#">AD DS Auditing Step-by-Step Guide</a> and <a href="#">Audit Policy Recommendations</a> in <i>Windows Server 2008 R2 and Windows Server 2008</i>
<b>STEP 2. - Enable Log Collection</b> in Security Monitoring and Analytics.	-	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <i>Getting Started with Oracle Management Cloud</i>
<b>STEP 3. - Add an Entity Association</b> to support the new logs in OMC using Log Analytics.	Associate Windows Security Events with your OMC entity (the dedicated Windows server where you installed the OMC agent).	Associating Log Sources to Existing Entities in <i>Using Oracle Log Analytics</i>
<b>STEP 4. - Validate</b> your log collection.	Confirm your setup was successful.	<a href="#">Validate Log Collections</a>

## Palo Alto Firewall

This Quick Start Guide provides log configuration details for SMA support: Palo Alto Syslog using Syslog hosting (Linux).

### Support Specifications:

PAN - OS 7.1

**Configuration Prerequisites:**

To complete this task, you must have an Oracle Cloud account containing an OMC instance with administrator privileges.

Prerequisite	Description	For additional details...
1. Access to Oracle Management Cloud	You must have an Oracle Cloud account containing an OMC instance with administrator privileges.	How Do I Access Oracle Management Cloud? in <i>Managing and Monitoring Oracle Cloud About Roles and Users</i>
2. The Syslog server configured with default settings	The Syslog server is your log host ( <i>OMC entity</i> ), where log sources upload and store logs.	See FTP Server documentation provided by your vendor.
3. Cloud agent(s) installed and Log Analytics licensing enabled	Have a Cloud Agent installed on the FTP server. This host will be discovered as an entity in OMC.	Install the Cloud Agent and Enable Oracle Log Analytics in <i>Using Log Analytics Environment Requirements in Installing and Managing Oracle Management Cloud Agents</i>
4. Security Monitoring and Analytics licensing enabled	Note that <b>SMA Data Enrichment</b> is disabled by default.	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <i>Getting Started with Oracle Management Cloud</i>

**Configuration Steps:**

Palo Alto Firewall	Task requirements	For additional details, see...
<b>STEP 1. - Configure</b> your firewall to upload logs to your Syslog server ( <i>OMC entity</i> ).	-	<a href="#">Configure Syslog Monitoring in PAN-OS 7.1 Administrator's Guide</a>
<b>STEP 2. - Add an Entity Association</b> to support the new logs in OMC using Log Analytics.	Associate Palo Alto Syslog Logs with your OMC entity (the Syslog server where you installed the OMC Cloud Agent).	<a href="#">Security Device Sources Associating Log Sources to Existing Entities in Using Oracle Log Analytics</a>
<b>STEP 3. - Validate</b> your log collection.	Confirm your setup was successful.	<a href="#">Validate Log Collections</a>

## Common Tasks

These tasks are typically performed when setting up log collections from monitoring sources in your IT enterprise.

Requirements and Prerequisites	<a href="#">Prerequisites and Requirements for Security Sources</a>
How to...	<a href="#">Validate Log Collections</a>

## Prerequisites and Requirements for Security Sources

Environment prerequisites and configuration requirements for enabling security log sources.

### OMC Prerequisite Tasks

Prerequisite	Description	For additional details and examples see...
1. Access to Oracle Management Cloud	Have an Oracle Cloud account containing an OMC instance with administrator privileges.	How Do I Access Oracle Management Cloud? in <i>Managing and Monitoring Oracle Cloud About Roles and Users</i>
2. Cloud agent(s) installed and Log Analytics licensing enabled	<ul style="list-style-type: none"> <li>– Meet cloud agent prerequisites on UNIX systems.</li> <li>– Install the cloud agent on the <i>host</i> you selected for storing logs.</li> </ul> <p><b>Note</b> that your log host is listed in the <b>Support Specifications</b> section of your quick-start guide.</p>	<p>Environment Requirements in <i>Installing and Managing Oracle Management Cloud Agents</i></p> <p>Install the Cloud Agent and Enable Oracle Log Analytics in <i>Using Log Analytics</i></p>
3. Security Monitoring and Analytics licensing enabled	<b>SMA Data Enrichment</b> is disabled by default.	Enabling Automatic Log Analytics and Security Monitoring and Analytics Data Collection in <i>Getting Started with Oracle Management Cloud</i>

## Validate Log Collections

Post configuring your log collection, perform these tasks to validate a successful setup.

### Note:

Security Monitoring and Analytics may take up to 30 minutes for log data to start showing.

### Validation Scenario 1

- Set the timeframe to reflect the expected timeframe in the logs being sent. If implementing a new log source to send current logs set the timeframe to "Last Hour" or some shortened timeframe to focus on the most recent logs ingested by SMA.
- Run a generic query in Security Data Explorer, to view logs being ingested by a data element unique to the new log source being created. If the new source is the first of it's kind then filtering by "Log Source" will be sufficient to see when those

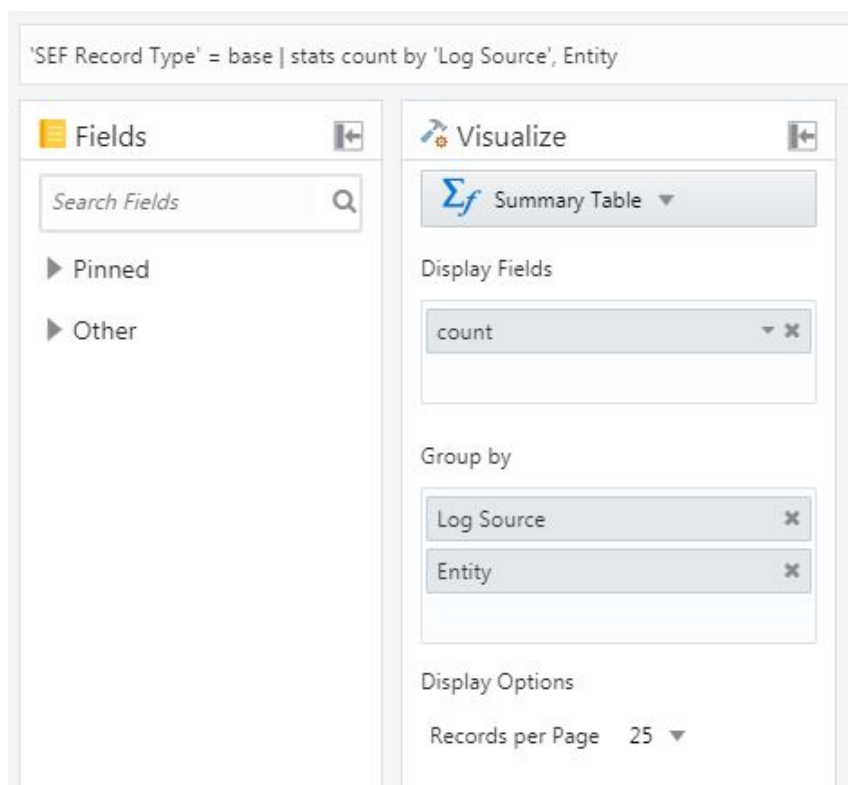
new logs start to show up in SMA using a basic visualization like pie/bar chart or summary table.

- Query examples include:
  - 'SEF Record Type' = base | stats count by 'Log Source'
  - 'SEF Record Type' = base and 'Log Source' = 'Bluecoat Proxy W3C Logs' | stats count by 'Log Source'

### Validation Scenario 2

- If the new log source is an addition to existing source, like a newly created Oracle database, a *Summary Table* organized by 'Log Source' and 'Entity' will display all the entity names per log source type. Look for the name of the new 'Entity' created in the previous steps.
- Query examples include:
  - View all entity names by log source 'SEF Record Type' = base | stats count by Log Source', Entity'

**Figure A-1 Filtering logs image**



- View all entity names for a specific log source: 'SEF Record Type' = base AND 'Log Source' = 'Linux Cron Logs' | stats count by 'Log Source', Entity

# B

## SMA Reference

### Topics:

- [Security Monitoring and Analytics Terminology](#)
- [Security Event Format - SEF Handbook](#)
- [Security Intelligence Reference](#)

## Security Monitoring and Analytics Terminology

Terminology used throughout the SMA's documentation and the user interface.

### SMA Terms and Concepts

General Terminology	<a href="#">UI and SMA Concepts</a>   <a href="#">Machine Learning</a>
Security Event Format	<a href="#">Actor</a>   <a href="#">Asset</a>   <a href="#">Destination</a>   <a href="#">Source</a>   <a href="#">User</a>
SEF Field Properties	<a href="#">Commonly Used SEF Fields</a>

### UI and SMA Concepts

Security Alert rule	Defines detection conditions that generate alerts, and notifies recipients when alerts are triggered.
Data Enrichment	Adding additional information or context to the data present in the raw logs as they are ingested to increase the analytical value.
Watchlist	A named list of elements of the same type (account, user, IP address / Cidr notation, or string) that can be leveraged by correlation rules to look for matches against specifically defined OSEF fields. These lists can be populated by adding individual elements, uploading from a file, or by setting up a feed.
Whitelist	A list that contains known and trusted entities that will not be considered during threat evaluations, providing detection results less prone to <i>false positives</i> .

### Machine Learning

Machine learning	Ingests activity data (collected through Log Analytics) and uses learning models to understand typical user and asset behavior.
------------------	---



	Therefore, it's capable of detecting anomalies and making predictions based on learned behavioral patterns.
Analysis model	User-defined learning model that is implemented in machine learning as a building block.
Peer Group Analysis model	A model type that learns typical behavior of users based on what organizations they belong to.
SQL Analysis model	A model type that learns typical SQL execution, in terms of statements executed and the order of their execution, for a single database. Databases must have auditing enabled, and the audit logs must be collected by Log Analytics before learning models can be created.

## Security Event Format - SEF Handbook

SEF is Oracle's data-centric event framework designed to extract, structure, and enrich log components into event elements with state-of-the-art security elements .

### Topics:

- [SEF Elements](#)
- [SEF Query Samples](#)
- [Commonly Used SEF Fields](#)

## SEF Query Samples

Filtering SEF Queries	<ol style="list-style-type: none"> <li>1. <a href="#">Filtering with wildcards</a></li> <li>2. <a href="#">Filtering with null values</a></li> <li>3. <a href="#">Filtering based on Network Port vs Application Protocol attributes</a></li> </ol>
-----------------------	---

## Filtering SEF Queries

These query samples show how to construct SEF queries.

When looking for all records related to administrator level changes to hosts you can refer to the `sefCategory` field. In these instances the possible values are numerous: `system.admin.(startup|shutdown|restart|disable|enable|create|modify)`

### Filtering with *wildcards*

### Example B-1

There are other log source types that contain additional `system.admin` values. Filter using wildcards to remove irrelevant information:

```
'SEF Device Class' = host
```

Instead of creating an 'IN' statement containing all possible values we can leverage a wildcard value to capture all possible values, making the query:

```
'SEF Device Class' = host and 'sef Category' = 'system.admin.%'
```

## Filtering with `null` values

### Example B-2 Filter out `null` values

```
'SEF Destination Endpoint Account Name' != null and 'SEF Actor Endpoint Network Address' not in (null, 10.0.14.1, 10.0.14.2, 10.0.14.3)
```

### Example B-3 Filtering `null` values in specific fields only

Find only records that have `null` values in specific fields

```
'SEF Application Protocol' = http and 'SEF Destination Top Level Domain' = null  
'SEF Actor Endpoint Name' in (null, localhost, 127.0.0.1)
```

## Filtering based on Network Port vs Application Protocol attributes

While these fields can be used to find similar information, they have subtle differences between them but each have significant impact on the data returned when choosing one over the other. This can be affected by elements of each individual network, as well as the log sources being sent to SMA.

Some security devices, like firewalls, are 'protocol aware' where the protocol names (`http`, `dns`, `ftp`) are recorded in your log data when these protocols are detected. This information is implemented during the data-enrichment phase for security logs, where:

- SMA assigns it to `sefApplicationProtocol` field pending such log records are provided by your *security log sources*
- SMA automatically fills it in for selected **security log sources** even if no such data record is provided.

### Scenario Examples

1. Web server logs may have 'HTTP' set for `sefApplicationProtocol`. In other cases where only the destination port number is available and protocol can't be assumed with a high degree of accuracy, `sefApplicationProtocol` is not populated.
  - a. It is possible that `sefDestinationEndpointNetworkAddressPort = 80` will return information that isn't HTTP related, like network scanning activity. It could also potentially miss HTTP related log entries where port information isn't available in the log data, or when alternative ports are used for some HTTP traffic (81, 8080, 8081, 8888).

2. The same holds true for `sefDestinationEndpointNetworkAddressPort`, if the protocol is known but no port information is available in the log data, the field will be left blank.
  - a. Similarly, `sefApplicationProtocol = HTTP` will return logs known to be related to web traffic, but will not return logs where no protocol is recorded and the information can't be assumed with a high degree of accuracy.

#### Example B-4 Filtering with SEF field combinations

In general it is a good idea to leverage both fields together to ensure the most complete information is returned in SDE (Software-Defined Environment), custom queries, and dashboards. The best solution will depend on your network and the log sources being sent to SMA, and may require some testing.

```
'sef Destination Endpoint Network Address Port' = 80 OR 'sef Application Protocol' = http
```

#### Example B-5 Filtering with SEF field combinations and parameter specifications

In an environment where web development takes place, or where custom apps are configured to use alternative ports for HTTP traffic those additional ports may need to be added to an 'IN' statement in the query:

```
'sef Destination Endpoint Network Address Port' IN (80, 8080, 8081, 8888) OR 'sef Application Protocol' = HTTP
```

#### Example B-6 Filtering with more complex SEF field combinations and parameter specifications

Incorporating HTTPS into the query requires an additional 'IN' statement and additional ports:

```
'sef Destination Endpoint Network Address Port' IN (80, 8080, 8081, 8888, 443, 4343, 8043) OR 'sef Application Protocol' IN (http, https)
```

## Commonly Used SEF Fields

Each field provides a set of attributes with enriched event data from your data logs.

### Commonly Used SEF Fields

- [sef | Field Properties](#)
- [sefActor | Field Properties](#)
- [sefDestination | Field Properties](#)
- [sefOriginalActor | Field Properties](#)

### sef | Field Properties

<b>sef</b> { data   mlti-val?}	<b>SEF Display Label</b> <i>Description</i>
<code>sefAddlAttrs</code> { STRING   Yes }	<b>SEF Additional Attributes</b> <i>not provided</i>

<b>sef</b> <b>{ data   mlti-val?}</b>	<b>SEF Display Label</b> <b>Description</b>
sefEnrichmentTime { TIMESTAMP   No }	<b>SEF Enrichment Time</b> <i>Time at which event was enriched</i>
sefRecordType { STRING   Yes }	<b>SEF Record Type</b> <i>Type of SEF event (base, anomaly, correlation)</i>

## sefActor | Field Properties

<b>sefActor</b>	<b>Data Type</b>	<b>Mul- ti- val- ued ?</b>	<b>SEF Display Label</b>	<b>Description</b>
sefActorEPAccountSummaryRisk	STRING	No	SEF Actor Endpoint Account Summary Risk	Summary Risk associated with the Actor Account Name.
sefActorEPADdlAttrs	STRING	Yes	SEF Actor Endpoint Additional Attributes	Customized attributes
sefActorEPCriticality	STRING	No	SEF Actor Endpoint Criticality	Criticality associated with the actor endpoint. For example low, medium, and high.
sefActorEPLocation	STRING	Yes	SEF Actor Endpoint Location	Location of endpoint actor. This can be a street address, datacenter name, rack location, etc.
sefActorEPSecurityCategory	STRING	No	SEF Actor Endpoint Security Category	Security categorization of the actor endpoint.
sefActorEPTags	STRING	Yes	SEF Actor Endpoint Tags	Tags associated with Actor Endpoint.
sefActorUserName	STRING	No	SEF Actor Username	User associated with the actor endpoint account name.
sefActorUserOrgs	STRING	Yes	SEF Actor User Organizations	Organization(s) of the actor user.
sefActorUserPrimaryOrg	STRING	No	SEF Actor User Primary Organization	The primary organization of the user associated with the actor endpoint account.
sefActorUserSummaryRisk	STRING	No	SEF Actor User Summary Risk	Summary risk associated with the actor user account.

## sefDestination | Field Properties

<b>sef { data   mlti-val?}</b>	<b>SEF Display Label Description</b>
sefDestinationEPAccountSummaryRisk { STRING   No }	<b>SEF Destination Endpoint Account Summary Risk</b> <i>Summary Risk associated with the destination account</i>
sefDestinationEPAddlAttrs { STRING   Yes }	<b>SEF Destination Endpoint Additional Attributes</b> <i>Additional attributes related to the destination endpoint</i>
sefDestinationEPClassCategory { STRING   No }	<b>SEF Destination Endpoint Class Category</b> <i>Categorization of destination endpoint</i>
sefDestinationEPClassSubCategory { STRING   No }	<b>SEF Destination Endpoint Class Subcategory</b> <i>Subcategory of the service that is publishing the destination endpoint</i>
sefDestinationEPClassService { STRING   No }	<b>SEF Destination Endpoint Class Service</b> <i>Category of the service that is publishing the destination endpoint</i>
sefDestinationEPCriticality { STRING   No }	<b>SEF Destination Endpoint Criticality</b> <i>Criticality associated with the destination endpoint</i>
sefDestinationEPLocation { STRING   Yes }	<b>SEF Destination Endpoint Location</b> <i>Location can be Street Address, Rack location in data center</i>
sefDestinationEPSecurityCategory { STRING   No }	<b>SEF Destination Endpoint Security Category</b> <i>Security categorization of the destination endpoint</i>
sefDestinationEPServiceProvider { STRING   No }	<b>SEF Destination Endpoint Service Provider</b> <i>The service provider for the destination endpoint</i>
sefDestinationEPTags { STRING   Yes }	<b>SEF Destination Endpoint Tags</b> <i>Tags that have been applied to this log entry because of some criteria of the destination endpoint</i>
sefDestinationUserName { STRING   No }	<b>SEF Destination Username</b> <i>User associated with the destination account</i>
sefDestinationUserOrgs { STRING   Yes }	<b>SEF Destination User Organizations</b> <i>Organization(s) of the SEF Destination User</i>
sefDestinationUserPrimaryOrg { STRING   No }	<b>SEF Destination User Primary Organization</b>
sefDestinationUserSummaryRisk { STRING   No }	<b>SEF Destination User Summary Risk</b>

## sefOriginalActor | Field Properties

**(SEF) ORIGINAL ACTOR** has Endpoint, User elements, part of SEF Field: **sefOriginalActor**

**Table B-1 Field Properties: sefOriginalActor[ EP|User ]Attributes.**

sefOriginal Actor	Data Type	Mul ti-val ued ?	SEF Display Label	Applied Action
sefOriginalActorEffectiveAccountName	STRING	No	SEF Original Actor Effective Account Name	The effective account used by the original sessionized actor
sefOriginalActorEndpointLocation	STRING	Yes	SEF Original Actor Endpoint Location	Location can be a street address, rack location in data center, etc.
sefOriginalActorUsername	STRING	No	SEF Original Actor Username	The username of the original actor for a security event

sefOriginalActorEffectiveAccountName	The effective account used by the original sessionized actor	
	Type:	STRING
	Multi-valued:	No
	SEF Label:	SEF Original Actor Effective Account Name
sefOriginalActorEndpointLocation	Location can be a street address, rack location in data center, etc.	
	Type:	STRING
	Multi-valued:	No
	SEF Label:	SEF Original Actor Endpoint Location
sefOriginalActorUsername	The username of the original actor for a security event	
	Type:	STRING
	Multi-valued:	No
	SEF Label:	SEF Original Actor Username

## SEF Elements

### Actor

Actor IP	Represents the IP address of the system an action was initiated on or from, if applicable.
Actor Endpoint	The device, application, or asset through which the actor took the action.
Original Actor	<p>The original actor who performed the action that was determined by looking at a series of events. For instance, if we see a series of three events:</p> <ul style="list-style-type: none"> <li>JSMITH_us (owned by John Smith) logged in to machine abc123 (with IP of 10.228.241.156).</li> <li>5 minutes after the first login, FJOHNSON_us logged in to machine xyz123 (IP 10.248.30.150) from 10.228.241.156.</li> <li>5 minutes from the second login, PANDERSON logged in to machine idc123 (with IP 10.268.251.154) from IP 10.248.30.150.</li> </ul> <p>The original actor may be deemed by the event enrichment service to be John Smith for all three logins, although different accounts (belonging to different persons) were used in each login action.</p>
Original actor endpoint	The actor endpoint associated with the original actor.

### Asset

Accessed Asset	A <i>destination asset</i> provides log records indicating its activity information during the specified time period.
Active Asset	A monitored resource, such as a database, a host server, a compute resource, or an application server.
Risky Asset	Underlying components (such as VMs, servers, databases, and software applications) throughout your enterprise that have shown unusual activity.

### Destination

Destination account	This could represent the secure shell (SSH) account used to log into a network host, or the single sign-on (SSO) account used to access a network resource. These can be different than the actor account on the host the request is made from.
Example	<p><i>Real world scenario:</i> User bkeen is logged into his laptop (laptop_226 / 10.2.0.226), and initiates an SSH login to webServer1 (10.2.43.16) as root.</p> <p><i>SEF characterization:</i></p>

	<pre>ActorEndpointAccountName = bkeen ActorEndpointName = laptop_226 ActorEndpointNwAddress = 10.2.0.226 DestinationEndpointName = webServer1 DestinationEndpointNwAddress = 10.2.43.16 DestinationEndpointAccountName = root</pre>
Destination effective account	For instance, if JSMITH_it invokes a definer's rights procedure defined by FJOHNSON on a database to create a table, then the destination account is JSMITH_it, whereas the destination effective account is FJOHNSON.
Destination endpoint	The container asset where the destination resource resides.
sefDestination Fields	<a href="#">sefDestination   Field Properties</a>

#### Source

Source account	The account used by the actor at the source endpoint to access the source resource (such as a host, a service, or an application).
Source endpoint	The container asset where the source resource resides. For instance, if the source resource is a table in a database, then the source endpoint is associated with the database.
Source resource	The resource that contributed to the action of the destination resource. For instance, if you copy a file <code>/etc/passwd</code> to <code>/tmp/x</code> , then the destination resource is <code>/tmp/x</code> , and the source resource is <code>/etc/passwd</code> .

#### User

User	Underlying components (such as VMs, servers, databases, and software applications) throughout your enterprise that have shown unusual activity.
Active User	Active users are those users with log records indicating the activity they initiated during a specified time period
Risky User	Users that have shown unusual activity compared to their typical activity and behavioral patterns.

## Security Intelligence Reference

The Security Intelligence dashboard provides information based on IP categories, and domain and URL categories.

- [IP Categories](#)



- [Domain and URL Categories](#)

### IP Categories

Category	Includes...
Spam Sources	Tunneling Spam messages through proxy, anomalous SMTP activities, Forum Spam activities.
Windows Exploits	Active IP Address offering or distributing malware, shell code, rootkits, worms or viruses
Web Attacks	Cross site scripting, iFrame injection, SQL injection, cross domain injection, or domain password brute force attack
Botnets Botnet	Botnet C&C channels, and infected zombie machine controlled by Bot master
Scanners	All reconnaissance such as probes, host scan, domain scan and password brute force attack
Denial of Services	DOS, DDOS, anomalous sync flood, anomalous traffic detection
Reputation	Deny access from IP addresses currently known to be infected with malware. This category also includes IPs with average low Webroot Reputation Index score. Enabling this category will prevent access from sources identified to contact malware distribution points
Phishing	IP addresses hosting phishing sites, other kind of fraud activities such as Ad Click Fraud or Gaming fraud
Proxy	IP addresses providing proxy and def services.
Mobile Threats Mobile Threat	IP addresses of malicious and unwanted mobile applications. This category leverages data from Webroot mobile threat research team.
Tor Proxy	IP addresses acting as exit nodes for the Tor Network. Exit nodes are the last point along the proxy chain and make a direct connection to the originator's intended destination.

### Domain and URL Categories

No.	Category	Includes...
1	<b>Real Estate</b>	Information on renting, buying, or selling real estate or properties. Tips on buying or selling a home. Real estate agents, rental or relocation services, and property improvement.
2	<b>Computer and Internet Security</b>	Computer/Internet security, security discussion groups.
3	<b>Financial Services</b>	Banking services and other types of financial information, such as loans, accountancy, actuaries, banks, mortgages, and general insurance companies. Does not include sites that offer market information, brokerage or trading services.
4	<b>Business and Economy</b>	Business firms, corporate websites , business information, economics, marketing, management, and entrepreneurship.
5	<b>Computer and Internet Info</b>	General computer and Internet sites, technical information. SaaS sites and other URLs that deliver internet services.
6	<b>Auctions</b>	Sites that support the offering and purchasing of goods between individuals as their main purpose. Does not include classified advertisements.

No.	Category	Includes...
7	<b>Shopping</b>	Department stores, retail stores, company catalogs and other sites that allow online consumer or business shopping and the purchase of goods and services.
8	<b>Cult and Occult</b>	Methods, means of instruction, or other resources to interpret, affect or influence real events through the use of astrology, spells, curses, magic powers, satanic or supernatural beings. Includes horoscope sites.
9	<b>Travel</b>	Airlines and flight booking agencies. Travel planning, reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. Car rentals.
10	<b>Abused Drugs</b>	Discussion or remedies for illegal, illicit, or abused drugs such as heroin, cocaine, or other street drugs. Information on " legal highs" : glue sniffing, misuse of prescription drugs or abuse of other legal substances.
11	<b>Adult and Pornography</b>	Sexually explicit material for the purpose of arousing a sexual or prurient interest. Adult products including sex toys, CD-ROMs, and videos. Online groups, including newsgroups and forums, that are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including videoconferencing, escort services, and strip clubs. Sexually explicit art.
12	<b>Home and Garden</b>	Home issues and products, including maintenance, home safety, decor, cooking, gardening, home electronics, design, etc.
13	<b>Military</b>	Information on military branches, armed services, and military history.
14	<b>Social Networking</b>	These are social networking sites that have user communities where users interact, post messages, pictures, and otherwise communicate. These sites were formerly part of Personal Sites and Blogs but have been removed to this new category to provide differentiation and more granular policy.
15	<b>Dead Sites</b>	These are dead sites that do not respond to http queries. Policy engines should usually treat these as "Uncategorized" sites.
16	<b>Individual Stock Advice and Tools</b>	Promotion and facilitation of securities trading and management of investment assets. Also includes information on financial investment strategies, quotes, and news.
17	<b>Training and Tools</b>	Distance education and trade schools, online courses, vocational training, software training, skills training.
18	<b>Dating</b>	Dating websites focused on establishing personal relationships.
19	<b>Sex Education</b>	Information on reproduction, sexual development, safe sex practices, sexually transmitted diseases, sexuality, birth control, sexual development, tips for better sex as well as products used for sexual enhancement, and contraceptives.
20	<b>Religion</b>	Conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship.
21	<b>Entertainment and Arts</b>	Motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. Performing arts (theatre, vaudeville, opera, symphonies, etc.). Museums, galleries, artist sites (sculpture, photography, etc.).
22	<b>Personal sites and Blogs</b>	Personal websites posted by individuals or groups, as well as blogs.
23	<b>Legal</b>	Legal websites, law firms, discussions and analysis of legal issues.
24	<b>Local Information</b>	City guides and tourist information, including restaurants, area/regional information, and local points of interest.
25	<b>Streaming Media</b>	Sales, delivery, or streaming of audio or video content, including sites that provide downloads for such viewers.

No.	Category	Includes...
26	<b>Job Search</b>	Assistance in finding employment, and tools for locating prospective employers, or employers looking for employees.
27	<b>Gambling</b>	Gambling or lottery web sites that invite the use of real or virtual money. Information or advice for placing wagers, participating in lotteries, gambling, or running numbers. Virtual casinos and offshore gambling ventures. Sports picks and betting pools. Virtual sports and fantasy leagues that offer large rewards or request significant wagers. Hotel and Resort sites that do not enable gambling on the site are categorized in Travel or Local Information.
28	<b>Translation</b>	URL and language translation sites that allow users to see URL pages in other languages. These sites can also allow users to circumvent filtering as the target page's content is presented within the context of the translator's URL. These sites were formerly part of Proxy Avoidance and Anonymizers, but have been removed to this new category to provide differentiation and more granular policy.
29	<b>Reference and Research</b>	Personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogues, genealogy, and scientific information.
30	<b>Shareware and Freeware</b>	Software, screensavers, icons, wallpapers, utilities, ringtones. Includes downloads that request a donation, and open source projects.
31	<b>Peer to Peer</b>	Peer to peer clients and access. Includes torrents, music download programs.
32	<b>Marijuana</b>	Marijuana use, cultivation, history, culture, legal issues.
33	<b>Hacking</b>	Illegal or questionable access to or the use of communications equipment/software. Development and distribution of programs that may allow compromise of networks and systems. Avoidance of licensing and fees for computer programs and other systems.
34	<b>Games</b>	Game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. Also includes sites dedicated to selling board games as well as journals and magazines dedicated to game playing. Includes sites that support or host online sweepstakes and giveaways. Includes fantasy sports sites that also host games or game-playing.
35	<b>Philosophy and Political Advocacy</b>	Politics, philosophy, discussions, promotion of a particular viewpoint or stance in order to further a cause.
36	<b>Weapons</b>	Sales, reviews, or descriptions of weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications.
37	<b>Pay to Surf</b>	Sites that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
38	<b>Hunting and Fishing</b>	Sport hunting, gun clubs, and fishing.
39	<b>Society</b>	A variety of topics, groups, and associations relevant to the general populace, broad issues that impact a variety of people, including safety, children, societies, and philanthropic groups.
40	<b>Educational Institutions</b>	Pre-school, elementary, secondary, high school, college, university, and vocational school and other educational content and information, including enrollment, tuition, and syllabus.
41	<b>Online Greeting cards</b>	Online Greeting card sites.

No.	Category	Includes...
42	<b>Sports</b>	Team or conference web sites, international, national, college, professional scores and schedules; sports-related online magazines or newsletters, fantasy sports and virtual sports leagues.
43	<b>Swimsuits &amp; Intimate Apparel</b>	Swimsuits, intimate apparel or other types of suggestive clothing.
44	<b>Questionable</b>	Tasteless humor, " get rich quick" sites, and sites that manipulate the browser user experience or client in some unusual, unexpected, or suspicious manner.
45	<b>Kids</b>	Sites designed specifically for children and teenagers.
46	<b>Hate and Racism</b>	Sites that contain content and language in support of hate crimes and racism such as Nazi, neo-Nazi, Ku Klux Klan, etc.
47	<b>Personal Storage</b>	Online storage and posting of files, music, pictures, and other data.
48	<b>Violence</b>	Sites that advocate violence, depictions, and methods, including game/comic violence and suicide.
49	<b>Keyloggers and Monitoring</b>	Downloads and discussion of software agents that track a user's keystrokes or monitor their web surfing habits.
50	<b>Search Engines</b>	Search interfaces using key words or phrases. Returned results may include text, websites, images, videos, and files.
51	<b>Internet Portals</b>	Web sites that aggregate a broader set of Internet content and topics, and which typically serve as the starting point for an end user.
52	<b>Web Advertisements</b>	Advertisements, media, content, and banners.
53	<b>Cheating</b>	Sites that support cheating and contain such materials, including free essays, exam copies, plagiarism, etc.
54	<b>Gross</b>	Vomit and other bodily functions, bloody clothing, etc.
55	<b>Web based email</b>	Sites offering web based email and email clients.
56	<b>Malware Sites</b>	Malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code.
57	<b>Phishing and Other Frauds</b>	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. These sites are typically quite short-lived, so examples don't last long. Please contact us if you need fresh data.
58	<b>Proxy Avoidance and Anonymizers</b>	Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering.
59	<b>Spyware and Adware</b>	Spyware or Adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization, also unsolicited advertising popups and programs that may be installed on a user's computer.
60	<b>Music</b>	Music sales, distribution, streaming, information on musical groups and performances, lyrics, and the music business.
61	<b>Government</b>	Information on government, government agencies and government services such as taxation, public, and emergency services. Also includes sites that discuss or explain laws of various governmental entities. Includes local, county, state, and national government sites.

No.	Category	Includes...
62	<b>Nudity</b>	Nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.
63	<b>News and Media</b>	Current events or contemporary issues of the day. Also includes radio stations and magazines, newspapers online, headline news sites, newswire services, personalized news services, and weather sites
64	<b>Illegal</b>	Criminal activity, how not to get caught, copyright and intellectual property violations, etc.
65	<b>Content Delivery Networks</b>	Delivery of content and data for third parties, including ads, media, files, images, and video.
66	<b>Internet Communications</b>	Internet telephony, messaging, VoIP services and related businesses.
67	<b>Bot Nets</b>	These are URLs, typically IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.
68	<b>Abortion</b>	Abortion topics, either pro-life or pro-choice.
69	<b>Health and Medicine</b>	General health, fitness, well-being, including traditional and non-traditional methods and topics. Medical information on ailments, various conditions, dentistry, psychiatry, optometry, and other specialties. Hospitals and doctor offices. Medical insurance. Cosmetic surgery.
71	<b>SPAM URLs</b>	URLs contained in SPAM.
75	<b>Parked Domains</b>	Domains that generate content dynamically based on arguments to their URL or other information (like geo-location) on the incoming web request.
76	<b>Alcohol and Tobacco</b>	Sites that provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.
78	<b>Image and Video Search</b>	Photo and image searches, online photo albums/digital photo exchange, image hosting.
79	<b>Fashion and Beauty</b>	Fashion or glamour magazines, beauty, clothes, cosmetics, style.
80	<b>Recreation and Hobbies</b>	Information, associations, forums and publications on recreational pastimes such as collecting, kit airplanes, outdoor activities such as hiking, camping, rock climbing, specific arts, craft, or techniques; animal and pet related information, including breed-specifics, training, shows and humane societies.
81	<b>Motor Vehicles</b>	Car reviews, vehicle purchasing or sales tips, parts catalogs. Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs. Journals and magazines on vehicle modifications.
82	<b>Web Hosting</b>	Free or paid hosting services for web pages and information concerning their development, publication and promotion.

# C

## User Identity Information and Alerting Sources

Configuration support for data integration with external solutions, or manual data uploads using REST API.

### Topics:

- [Oracle Identity Cloud Service](#)
- [Ingest Alert Data from Oracle CASB Service](#)

## Oracle Identity Cloud Service

Obtain user details through integration with another service or by uploading user data using REST API endpoints.

- [Uploading User Data Using REST API](#)
- [Collect User Information from Oracle Identity Cloud Service \(IDCS\)](#)

## Uploading User Data Using REST API

Use REST API to upload your user identity data in either SCIM or LDIF format.

Regardless of your identity management platform, as long as the data is exported in SCIM or LDIF format, you can upload this data using Oracle Management Cloud's REST API endpoints. However, this documentation is not available for general distribution. For access see note below.

REST API documentation will be made available to approved customers only. Contact your Oracle Support or Sales Representative for more information about accessing and using the *Oracle Security Monitoring and Analytics REST API* guide. When inquiring details, use the following doc identification as "My Oracle Support Note." Doc ID 2244391.1

## Collect User Information from Oracle Identity Cloud Service (IDCS)

This task shows how to configure Security Monitoring and Analytics integration with Oracle Identity Cloud Service (IDCS) for user details.

This is a two part task, skip to the second part if you meet the criteria described in part 1.

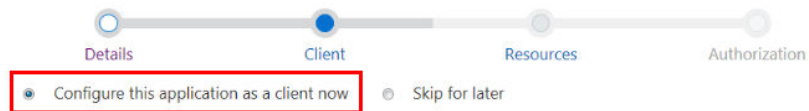
- Part 1 — Obtain the *identity context* access credentials from your trusted application in Oracle Identity Cloud Service.
- Part 2 — Once you configure your *identity context integration* settings in Security Monitoring and Analytics.

### Task prerequisites

Administrative access to both platforms: Oracle Identity Cloud Service and Oracle Management Cloud.

### Part 1. Obtaining The *Identity Context* Access Credentials from Oracle Identity Cloud Service

1. Login to Oracle Identity Cloud Service as an administrator.
2. If you already have a **Trusted Application** instance created in Oracle Identity Cloud Service, skip to Step 3.
  - a. In Oracle access details from Identity Cloud Service, go to the **Applications** page and click **Add**.
  - b. Select **Trusted Application**.
  - c. In the **Add Trusted Application** page, provide items below and click **Next**.
    - Instance name
    - Instance description (optional)
  - d. In the **Client** page, do the following and click **Next**.
    - Select **Configure this application as a client now**.
    - Under **Authorization** for **Allowed Grant Types**, select **Client Credentials**, **JWT Assertion** and **SAML2 Assertion**.



- At the bottom of the page, select **Grant the client access to Identity Cloud Service Admin APIs**, and enter `Audit Administrator` and `Identity Domain Administrator` in its text field.

### Accessing APIs from Other Applications

Trust Scope  All resources  
 Allowed tags  
 Allowed scopes

Allowed Tags

+ Add Tag

Allowed Scopes

+ Add ✕ Remove

Application	Allowed Scope
No data to display.	

Grant the client access to Identity Cloud Service Admin APIs.

Audit Administrator ✕ Identity Domain Administrator ✕

- e. In the **Expose APIs to Other Applications** page, leave **Skip for later** selected, and click **Next**.
  - f. Click **Activate** to finish creating your application instance.
3. In the trusted application's home page, select tab: **Configuration** .

SMA App  
Trusted app developed by Oracle.

Details **Configuration** Users Groups

General Information

Client ID 53c2d2de70d44d638bb13a0536be5d77

Client Secret Show Secret Regenerate

4. Copy values for the following (as they are required when configuring integration settings in Oracle Security Monitoring and Analytics):
  - Client ID: Under **General Information**.
  - Client Secret: Click **Show Secret**.



- Base URL: From your browser's URL field.

Base URL includes the REST endpoint, the recourse that you want to access, and other query parameters, if needed. The Base URL value includes everything, starting with `https` and ending with `.com`. It should look similar to this sample:

`https://idcs-abccbhvcjkhbadf.identity.x1yz.x2yz.com`

## Part 2. Configuring *Identity Context* Integration in Oracle Security Monitoring and Analytics

1. Login to Oracle Management Cloud as an administrator.
2. From Oracle Management Cloud's home page, go to **Security Monitoring and Analytics, Security Admin**, and select **Identity Context**.
3. Provide values your Access credentials: Base URL, Client ID, Client Secret, select a time interval for **Upload Identity Data** (optional), and **Save**.

**Create Identity Context Configuration**

⚠ Identity context access has not been configured. Please enter the access information and the upload schedule to regularly retrieve the latest identity context information.

Identity Provider Oracle Identity Cloud Service(IDCS)

Access

Authentication OAuth 2.0

\* Base URL

\* Client ID

\* Client Secret

\* Scope urn:opc:ldm:\_\_myscopes\_\_

\* Grant Type client\_credentials

Upload Identity Data

Repeat Daily

Time 12:00 AM

America/Mexico\_City

Save Cancel

## Ingest Alert Data from Oracle CASB Service

Uploading alert data, directly from Oracle CASB Cloud Service.

Task prerequisites:

- Access credentials for Oracle CASB Cloud Service (Base URL, Access Key, Access Secret).

For instructions to obtain these credentials, go to the Quick Start section, see **Step 2 Get the Oracle CASB Cloud Service Tenant Access Key and Secret Key**, found in the Quick Start section of *REST API for Oracle CASB Cloud Service's* Quick Start section.

1. In Security Monitoring and Analytics, go to **Security Admin** and select **CASB**.
2. Add access credentials from and for Oracle CASB Cloud Service in the **Base URL**, **Access Key**, **Access Secret** fields and **Save**.

The **Base URL** includes the REST endpoint and other components such as the recourse that you want to access or related query parameters that are applicable to your request type. When you provide **Base URL** information, include the URL beginning with `https` and ending with `.com`. It should look similar to the sample below.

`https://idcs-abccbhvcjkhbadf.identity.x1yz.x2yz.com`

**CASB Configuration**

⚠ CASB has not been configured. Please enter the access information to regularly retrieve the latest risk events.

Service Provider: Oracle CASB

**Access**

Authorization: API Token

\* Base URL:

\* Access Key:  \* Access Secret:

**Upload**

Schedule: Every 5 minutes

Save Cancel