

Adaptive Risk Manager Offline
Dashboard and Reporting Guide
10g Release (10.1.4.3.0)

December 2007

ORACLE

Copyright © 2007, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer

Contents

Preface	5
Related Documentation	5
Introduction	6
Access Privileges	6
Monitoring Alerts Using the Dashboard	7
To view the dashboard	7
Performance	7
Summary	8
Dashboards	8
Running Queries	9
To run a query on users	9
To run a query on locations	10
To run a query on devices	11
To run a query on summaries	12
To run a query on security	12
Saving and Exporting a Query	13
To save or export a report	13
Scheduling a Report	14
To schedule a report	14
Viewing Details about a Login Session	15
To view the details about a login session	15
To view details about the user	15
To view details about the user's primary user group	16
To view details about the device	16
Viewing Details about Users	17
To view details about users	17
To view a list of devices used by this user	17
To view a list of locations this user has logged in from	17
To view a list of alerts triggered a user	18
To view a list of logins by this user	18
To view a list of rules run on this user	19
Viewing the Details about Device IDs	20
To view a list of groups this device belongs to	20
To view a list of users that have used this device	20
To view a list of locations from which a device has logged in	20
To view a list of alerts and rules triggered by this device	21
To view a list of logins by this device	21

Viewing Details about Location Groups	23
To view the details about a location group	23
To view details about users from this location	23
To view a list of devices in this location	23
To view a list of alerts and rules triggered from this location	24
To view a list of logins from this location	24
Viewing Details about IP Addresses	26
To view details about the groups in which the IP is included	26
To view details about the users associated with the IP address	26
To view details about the devices associated with the IP address	26
To view details about the alerts/rules associated with the IP address	27
To view details about the logins associated with the IP address	27
Viewing Statistics about KBA Questions	29
To view statistics about question registration	29
To view statistics about challenge responses	29
To view statistics about each challenge question	30
Viewing a List of Saved Reports	31
To view a list of saved reports	31
Viewing a List of Saved Queries	32
To view a list of saved queries	32
Viewing a List of Schedulers	33
To view a list of schedulers	33
Glossary	34

Preface

Adaptive Risk Manager Offline is an offline fraud analysis tool for evaluating existing transaction data. It can be used in two ways:

- As a stand alone security tool to analyze, detect, and alert high risk transactions.
- In conjunction with Adaptive Risk Manager Offline as a supplemental offline analysis tool and as a way to pre-visualize rules against real customer data without impacting customers in real-time environment.

The Adaptive Risk Manager Offline Dashboard and Reporting Guide provides information on using the dashboard and running queries to pre-visualize and evaluate data.

Related Documentation

The Oracle Adaptive Access Manager Offline 10g documentation includes:

- The Oracle® Adaptive Access Manager Offline Dashboard and Reporting Guide
- The Oracle® Adaptive Access Manager Offline Customer Care Guide
- The Oracle® Adaptive Access Manager Offline Managing Data Guide

Introduction

Adaptive Risk Manager Offline is the reporting and administration counterpart to Adaptive Risk Manager Online. It provides sophisticated fraud monitoring by user, location, device, date and more.

When you finish running the session data against the rules, you can use the dashboard and reporting features in Adaptive Risk Manager Offline to see which rules were triggered.

Adaptive Risk Manager Offline includes a dashboard that provides statistics on:

- Locations
- Scoring breakdown
- Login summary
- Alerts breakdown
- Rules breakdown
- Browser/OS breakdown

And it contains a comprehensive collection of reports on:

- Users
- Locations
- Devices
- Summaries
- Security Alerts

This guide provides detailed instructions on how to use the dashboard and reporting functionality within Adaptive Risk Manager Offline.

Access Privileges

Your access privileges define the features that are available to you and the actions you can perform in Adaptive Risk Manager Offline. Your access privileges are based on the group to which you belong. Some functionality described in this guide might not be available to your group.

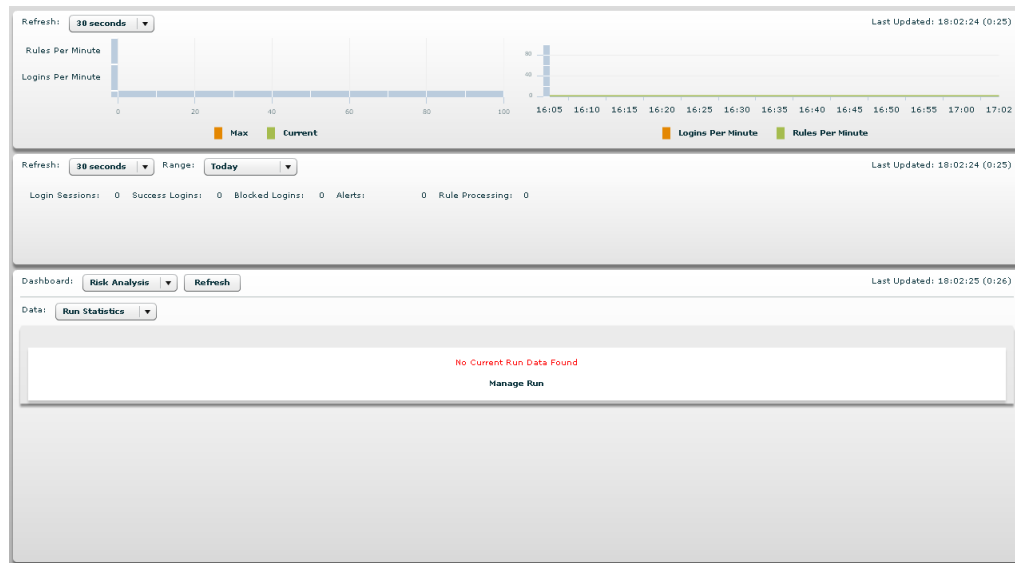
Monitoring Alerts Using the Dashboard

The Adaptive Risk Manager Offline Dashboard uses real-time data to provide a quick, overview of users and devices that have generated alerts and of all alerts by geographic location. It displays three different levels of security alerts: low, medium, and high to help you analyze Offline traffic, identify suspicious behavior, and design rules for fraud prevention. The dashboard also offers both total time views and trending views of performance levels.

To view the dashboard

- **Click Dashboard on the menu bar.**

The dashboard appears.



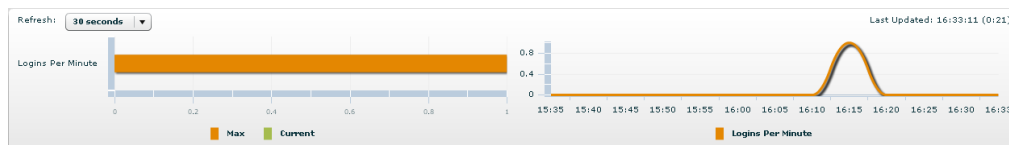
The dashboard is divided into three panels:

- Performance (top)
- Summary (middle)
- Dashboard (bottom)

Performance

The Performance panel, at the top of the page, displays a total login view on the left and a trending view on the right. The total logins view provides statistics on the current volume or rate of logins at the present time. The trending view provides statistics on logins during the past hour.

To change the refresh rate, in the Refresh list, click the rate you want.

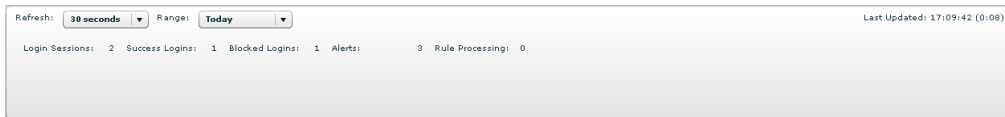


Summary

The Summary panel, in the middle of the page, displays an overview of activity for the specified range or time frame. It provides a summary of login sessions, successful logins, blocked logins, alerts, the number of rules triggered, and the number of rules currently running.

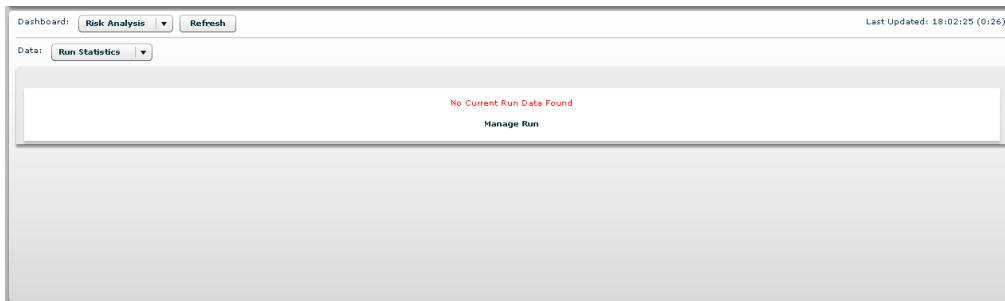
To change the refresh rate, click the Refresh menu and select the rate you want.

To change the timeframe, in the Range list, click the range you want.



Dashboards

The Dashboard panel, at the bottom of the page, displays run or load progress—the number of records loaded or run.



Running Queries

You can query the database for information on many different activities by users, locations, devices, and security alerts.

To run a query on users

1. Click Users on the Queries menu.

The Queries page on user activity appears and defaults to the report on recent logins.

Session Id	User Name	Auth Status	Pre Auth Score	Pre Auth Action	Post Auth Score	Post Auth Action	Login Time	Application Id	OS / Browser
388501	7777	Success	0	PasswordTextPadGeneric	0	RegisterUserOptionalQuestionPad	08/25/2007 12:20 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388801	nnnn	Success	0	PasswordTextPadGeneric	0	RegisterUserOptionalQuestionPad	08/25/2007 10:41 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388703	1111	Success	0	PasswordTextPad	666	ChallengeQuestionPad	08/24/2007 20:44 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388702	1111	Success	0	PasswordTextPad	666	ChallengeQuestionPad	08/24/2007 20:42 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388701	1111	Success	0	PasswordTextPad	0	RegisterQuestionsQuestionPad	08/24/2007 20:37 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388601	1111	Success	0	PasswordTextPad	666	ChallengeQuestionPad	08/24/2007 19:22 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388501	1111	Success	0	PasswordTextPad	666	Allow	08/24/2007 17:02 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388402	cccc	Success	0	PasswordTextPadGeneric	0	RegisterUserOptionalQuestionPad	08/24/2007 15:57 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388401	1111	Success	0	PasswordTextPad	0	RegisterQuestionsQuestionPad	08/24/2007 15:30 (PDT)	bharosaUIOGrn	WinNT 5.1/ Gecko2007(Firefox2.0.0.6)
388301	test	Success	0	PasswordTextPadGeneric	0	RegisterUserOptionalQuestionPad	08/24/2007 14:34 (PDT)	bharosaUIOGrn	WinNT 6.0/ MSIE7.0

2. Enter the search criteria you want and click Run Query.

3. To change the query type, click in the Query Type box and select the query type you want:

- **Recent Logins:** Displays all logins within the specified time range.
- **First Logins:** Displays all users first login attempt occurring during the designated date range.
- **Invalid Logins:** Displays all the login attempts from invalid users occurring during the designated date range.
- **Multiple Devices:** Displays all users that use multiple devices.
- **Frequent Logins:** Displays all users with multiple logins within the specified time range.
- **Multiple Failures:** Displays all users with multiple failures within the specified time range.
- **Challenges:** Displays the success and failure rates of challenges by user.

4. To view the details page for Login ID, Group ID, Device ID, Location, or IP address, click the link in appropriate column.

5. To save the query, see Saving and Exporting a Query.

6. To export the report, see Error! Reference source not found..

7. To schedule a report, see Scheduling a Report.

To run a query on locations

1. Click Location on the Queries menu.

The Queries page on activity by location appears and defaults to the report on recent logins by location.

Session ID	Location	IP Address	User Name	Auth Status	Pre Auth Action	Post Auth Action	Login Time	Application ID	OS / Browser	Device ID	Device ID	Check Type	Alerts
288793	united states california lark	65.3.232.112	2722	Success	PasswordTestPadGeneric	RegisterUserOptionalQuestionPad	08/29/2007 12:30 (PDT)	lharsaUI00gr	WINNT 5.1 / Gecko/2007 Firefox/2.0.0.6	202 / 205	352A01	TextPad	
288791	united states california lark	20.143.76.0	080b	Success	PasswordTestPadGeneric	RegisterUserOptionalQuestionPad	08/25/2007 10:41 (PDT)	lharsaUI00gr	WINNT 5.1 / Gecko/2007 Firefox/2.0.0.6	202 / 205	301	TextPad	
288792	united states california lark	20.143.76.0	1111	Success	PasswordTestPad	ChallengeQuestionPad	08/24/2007 20:44 (PDT)	lharsaUI00gr	WINNT 5.1 / Gecko/2007 Firefox/2.0.0.6	202 / 205	301	Question/Answer	
288792	united states california lark	20.143.76.0	1111	Success	PasswordTestPad	ChallengeQuestionPad	08/24/2007 20:42 (PDT)	lharsaUI00gr	WINNT 5.1 / Gecko/2007 Firefox/2.0.0.6	202 / 205	301	Question/Answer	
288791	united states california lark	20.143.76.0	1111	Success	PasswordTestPad	RegisterQuestionQuestionPad	08/24/2007 20:37 (PDT)	lharsaUI00gr	WINNT 5.1 / Gecko/2007 Firefox/2.0.0.6	202 / 205	301	TextPad	
288891	united states california lark	20.143.76.0	1111	Success	PasswordTestPad	ChallengeQuestionPad	08/24/2007 19:22 (PDT)	lharsaUI00gr	WINNT 5.1 / Gecko/2007 Firefox/2.0.0.6	202 / 205	301	Question/Answer	
288891	united states california lark	20.143.76.0	1111	Success	PasswordTestPad	Allow	08/24/2007 17:02 (PDT)	lharsaUI00gr	WINNT 5.1 / Gecko/2007 Firefox/2.0.0.6	202 / 205	301	TextPad	

2. Enter the search criteria you want and click Run Query.

3. To change the query type, click in the Query Type box and select the query type you want.

- **Recent Logins:** Displays all logins within the specified time range.
- **Multiple Failures:** Displays all locations with multiple failures within the specified time range.
- **Invalid Users:** Displays all the locations with login attempts from invalid users occurring during the designated date range.
- **User Locations:** Displays all locations a user has attempted logins from.
- **Multiple Users:** Displays all locations that have multiple users.
- **Challenges:** Displays success and failure rates of challenges by location.
- **Users by Location:** Displays all users from a given location or IP Address.
- **Frequent Logins:** Displays all locations with multiple logins within the specified time range.
- **Multiple Successful Logins:** Displays all locations with multiple successful logins.
- **Devices by Location:** Displays all devices from a given location or IP Address.
- **Device Locations:** Displays the locations for a specific device.

4. To view the details page for Login ID, Group ID, Device ID, Location, or IP address, click the link in appropriate column.

5. To save the query, see Saving and Exporting a Query.

6. To export the report, see Error! Reference source not found..

7. To schedule a report, see Scheduling a Report.

To run a query on devices

1. Click Device on the Queries menu.

The Queries page on activity by devices appears and defaults to the report on recent logins by location.

The screenshot displays the 'Device - Recent Logins' query results. The interface includes a search sidebar on the left, a table of login records in the center, and a bottom navigation bar. The table shows four records with columns for Session ID, Device ID, User Name, Auth Status, Pre Auth Score, Pre Auth Action, Post Auth Score, Post Auth Action, Login Time, Application ID, and OS/Browser.

Session ID	Device ID	User Name	Auth Status	Pre Auth Score	Pre Auth Action	Post Auth Score	Post Auth Action	Login Time	Application ID	OS/Browser
390202	356901	seven	Blocked	0	PasswordTextPad	1000	ChallengeQuestionPad	08/28/2007 15:55 (PDT)	bharosaUIOGrp	WinNT 6.0/ Gecko2007(Firefo
320201	356901	seven	Success	0	PasswordTextPadGeneric	0	RegisterUserOptionalQuestionPad	08/28/2007 15:54 (PDT)	bharosaUIOGrp	WinNT 6.0/ Gecko2007(Firefo
390123	356901	rinkuji	Blocked	0	PasswordTextPad	1000	ChallengeQuestionPad	08/28/2007 15:33 (PDT)	bharosaUIOGrp	WinNT 6.0/ Gecko2007(Firefo
320122	356901	rinkuji	Success	0	PasswordTextPadGeneric	1000	RegisterUserOptionalQuestionPad	08/28/2007 15:33 (PDT)	bharosaUIOGrp	WinNT 6.0/ Gecko2007(Firefo

2. Enter the search criteria you want and click Run Query.

3. To change the query type, click in the Query Type box and select the query type you want.

- **Recent Logins:** Displays all logins within the specified time range.
- **Frequent Logins:** Displays all devices with multiple logins within the specified time range.
- **New Devices:** Displays all new device IDs created within the specified time range.
- **Multiple Users:** Displays all devices that have multiple users.
- **Multiple Successful Logins:** Displays all devices with multiple successful logins.
- **Multiple Failures:** Displays all devices with multiple failures within the specified time range.
- **Users by Device:** Displays all users from a given device.
- **Devices by Users:** Displays all devices for a given User.
- **Challenges:** Displays statistics about device challenged within specified time range.
- **Invalid Users:** Displays all the devices with login attempts from invalid users occurring during the designated date range.

4. To view the details page Login ID, Group ID, Device ID, Location, or IP address, click the link in appropriate column.

5. To save the query, see Saving and Exporting a Query.

6. To export the report, see Saving and Exporting a Query.

7. To schedule a report, see Scheduling a Report.

To run a query on summaries

1. Click Summary on the Queries menu.

The query page on summaries appears and defaults to an aggregate summary of logins by date range.

2. To change the query type, click in the Query Type box and select the query type you want.

- Logins: Displays login aggregate summary for the designated date range.
- Averages: Displays average summary for the designated date range.

3. To change the start and end date of the search, click the calendar icons and select the From and To dates you want.

4. Click Run Query.

To run a query on security

1. Click Security on the Queries menu.

The query page on security appears and defaults to the alerts report on low, medium, and high level alerts that were generated during the specified timeframe.

2. Enter the search criteria you want and click Run Query.

3. To specify a particular location, in the Location list, click the location you want.

4. To change the alert level, in the Alert Level list, click the level you want.

5. To change the alert type, in the Alert Type list, click the type you want.
6. To find a specific alert, rule, user ID, or user name, type the search criteria in the appropriate field.
7. To change the query type, click in the Query Type box and select the query type you want.
 - Alerts: Displays all the alerts generated during the designated date range.
 - Alerts Breakdown: Displays alert breakdown summary for the designated date range.
 - Rules Breakdown: Displays rules breakdown summary for the designated date range.
 - Pre-authorization Scoring: Displays pre-authorization scoring summary for the designated date range.
 - Post-authorization Scoring: Displays post-auth scoring summary for the designated date range.
 - Score Combinations: Displays score combination summary for the designated date range.
8. To change the start and end date of the search, click the calendar icons and select the From and To dates you want.
9. To view the alert, session, or user details page, click the link you want in the report.

Saving and Exporting a Query

You can save or export a report of any query, formatted in PDF, HTML or Comma Separated Values.

To save or export a report

1. On the Queries page, click Save Report.

The Save/Export page appears.

2. Type a name for the query.
3. Click the File Type box and select the file type you want.
4. Click Next.

An Open/Save dialog box appears.

5. If you want to open the report, click Open.
6. If you want to save the file to disk, click Save to Disk, and then click OK.

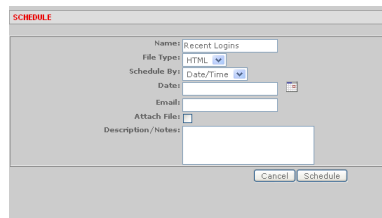
Scheduling a Report

You can schedule a report to run on a particular day and time in the future or at periodic intervals such as daily, weekly, or monthly. If you want, you may have Oracle Adaptive Risk Manager Offline notify you by email when it finishes running the report and even have it attach the report to the notification.

To schedule a report

1. On the Queries page, click Schedule Report.

The schedule page appears.



The screenshot shows a dialog box titled "SCHEDULE" with the following fields and options:

- Name: Recent Logins
- File Type: HTML
- Schedule By: Date/Time
- Date: [Empty field]
- Email: [Empty field]
- Attach File:
- Description/Notes: [Empty text area]

Buttons: Cancel, Schedule

2. Type a name for the report.
3. Click in the File Type box and select the file type you want.
4. Click in the Time box and select Date/Time or Interval.
5. If you chose Day/Time, enter the date and time on which you want the report to run.
6. If you chose Interval,
 - Click in the Frequency box and select the interval that you want.
 - Click in the Range box and select the period of time you want the report to cover.
 - If applicable, set the day and time you would like the report to run on.
7. Type your email address.
8. If you want Oracle Adaptive Risk Manager Offline (OARM Offline) to attach the file to the email, click Attach File.
9. Click Schedule and then click Close.

Viewing Details about a Login Session

The Session Details page displays an overview of the events that transpired during a particular session including the rules that ran and the rules that were triggered, the risk scores and those actions and alerts that took place.

To view the details about a login session

1. On the User, Device, or Location report page, click the Session ID for the customer login you want.

The Session Details page appears.

ADMIN > SESSION DETAILS

Request ID: 182_39229fb1a978faa74d594972f219899a
Session ID: 390302
User Name: nnnn
Device ID: 301
Status: Success
IP Address: 70.143.76.0

Login Time: 08/29/2007 10:32 (PDT)
Device Score: 0
User Group: bharosaUIOSGr
Location: united_states, california, bharosa
Pre Auth Scores: 0
Post Auth Scores: 0
Pre Auth Action: PasswordTextPad
Post Auth Action: RegisterQuestionsQuestionPad
Country CF: 99
State CF: 97
City CF: 95
Is Derived: false
OS: WinNT 5.1
Browsers: Gecko2007(Firefox2.0.0.6)
Secure Cookie: 152_d6c409e1ffa0ea27e1ffd90162ba1a7
Digital Cookie: 153_a6f4344e9ac67e30d0637eab3bb3ef66
Expected Secure Cookie: 152_d6c409e1ffa0ea27e1ffd90162ba1a7
Expected Digital Cookie: 153_a6f4344e9ac67e30d0637eab3bb3ef66
Secure Fingerprint Id: 201
Digital Fingerprint Id: 205

Info: Low: Medium: High:

Device Identification: 0
Pre-Authentication: Weighted maximum Score: 0
Business Policy: Active Executed Maximum 100%
Post-Authentication: Weighted maximum Score: 0
RegisterQuestionsQuestionPad
Security Policy: Active Executed Maximum 100%
Business Policy: Active Executed Maximum 100%

In the top section of the Session Details page, OARM Offline displays specific details about the session such as Session ID and User ID.

In the bottom area, at the default state, OARM Offline displays the runtimes and a master list of the actions and alerts that were triggered at those runtimes.

To view details about the policies, click the plus sign to expand the section.

To view details about the user

- On the Session Details page, click User Name.

The User Details page appears.

ADMIN - USER

User Details

Bharosa ID: 341101
User Name: nnnn
User ID: 9_fa1608b99c09e679d5982bdc92291404
User Group: bharosaUIOSGr
Application ID: bharosaUIOSGr
IsValid User: true
Create Time: Sat, 25 Aug 2007 10:41 AM -0700 (PDT)
Notes:

Groups Devices Locations Alerts Logins Rules

Search: Showing Records: 1 - 1 of 1

Cache Policy: All Full Cache None

Group Name: Run Query

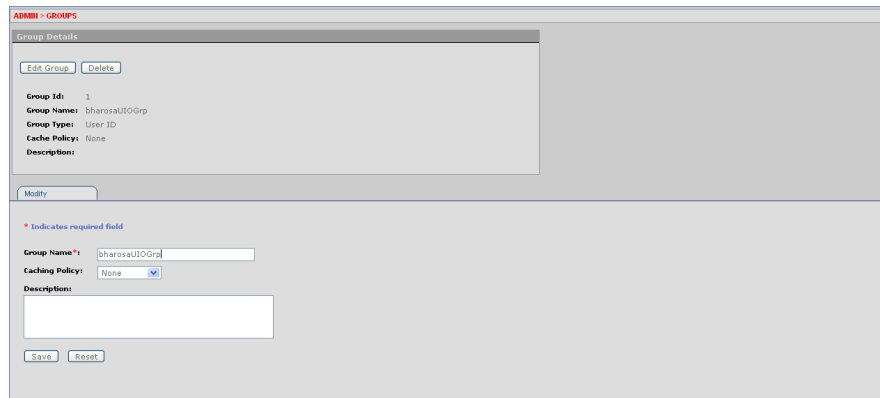
Group Name	Group Type	Cache Policy	Description
bharosaUIOSGr	User ID	None	

Showing Records: 1 - 1 of 1

To view details about the user's primary user group

- On the Session Details page, click User Groups.

The Group Details page appears.



The screenshot shows the 'ADMIN - GROUPS' section with a 'Group Details' form. The form displays the following information:

- Group Id: 1
- Group Name: bharosau10Grp
- Group Type: User ID
- Cache Policy: None
- Description:

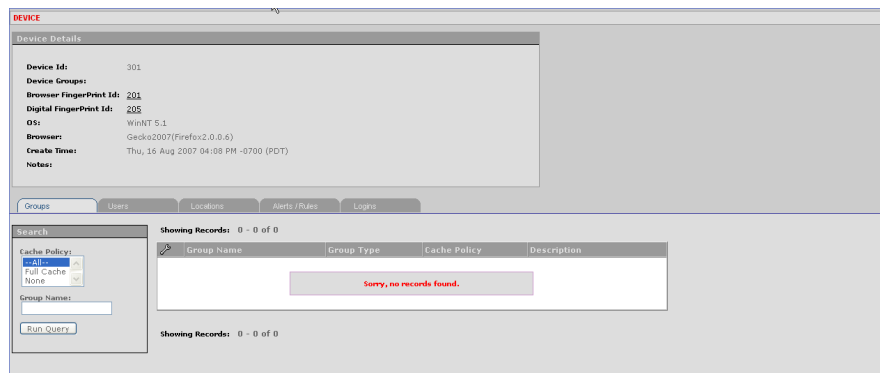
Below the form, there are 'Edit Group' and 'Delete' buttons. A 'Modify' button is also present. A search section below the form includes a text input field with 'bharosau10Grp', a 'Cache Policy' dropdown menu set to 'None', and a 'Description' text area. At the bottom of the search section are 'Save' and 'Reset' buttons.

The Group Details page displays information about the primary group in which the user belongs.

To view details about the device

- On the Session Details page, click Device ID.

The Device Details page appears.



The screenshot shows the 'DEVICE' section with a 'Device Details' form. The form displays the following information:

- Device Id: 301
- Device Groups:
- Browser FingerPrint Id: 201
- Digital FingerPrint Id: 325
- OS: WinNT 5.1
- Browser: Gecko2007(Firefox2.0.0.6)
- Create Time: Thu, 16 Aug 2007 04:08 PM -0700 (PDT)
- Notes:

Below the form, there are tabs for 'Groups', 'Users', 'Locations', 'Alerts / Rules', and 'Logins'. A search section below the tabs includes a 'Cache Policy' dropdown menu set to 'Full Cache', a 'Group Name' text input field, and a 'Run Query' button. A table below the search section shows 'Showing Records: 0 - 0 of 0' and a message 'Sorry, no records found.'

The top section of the Device Details page displays information about the device used to log in.

The bottom section of the page provides access to the groups, users, actions/rule, and logins associated with that device.

Viewing Details about Users

To view details about users

1. On the User, Device, or Location report page, click the User Name you want.

The User Details page appears.

The screenshot shows the 'ADMIN - USER' page. The 'User Details' section displays the following information:

- Bharsa Id:** 341101
- User Name:** nnnn
- User Id:** 9_fa1608b99c09e679d5982bd92291404
- User Groups:** bharsaUI0Grp
- Application Id:** bharsaUI0Grp
- IsValid User:** true
- Create Time:** Sat, 25 Aug 2007 10:41 AM -0700 (PDT)
- Notes:**

Below the details are tabs for Groups, Devices, Locations, Alerts, Logins, and Rules. A search section on the left includes a 'Cache Policy' dropdown (set to 'Full Cache'), a 'Group Name' input field, and a 'Run Query' button. The main area shows a table with one record:

Group Name	Group Type	Cache Policy	Description
bharsaUI0Grp	User ID	None	

2. Enter the search criteria you want and click Run Query.

To view a list of devices used by this user

1. On the User Details page, click the Devices tab.

The list of devices appears.

The screenshot shows the 'ADMIN - USER' page with the 'Devices' tab selected. The search criteria are:

- Auth Status:** Pending activation
- From Date:** 08/29/2007 14:33
- To Date:** 08/29/2007 23:59

The results table shows one record:

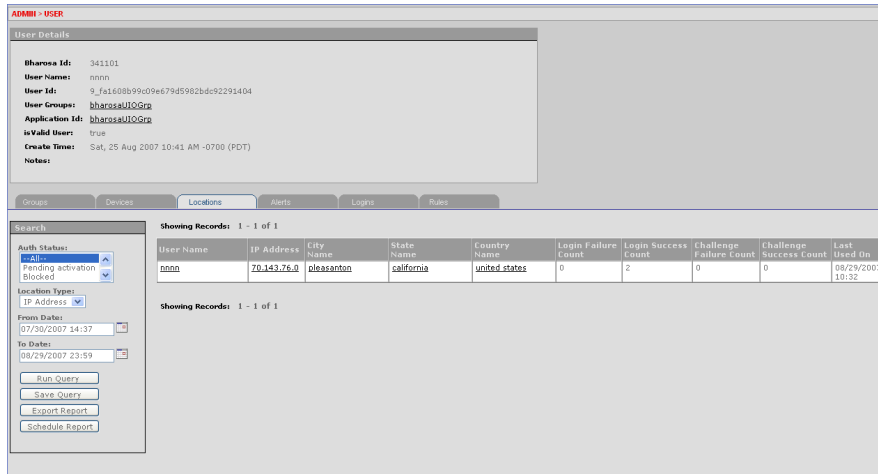
User Name	Device Id	Login Failures	Login Successes	Challenge Failures	Challenge Successes	Last Used On
nnnn	301	0	1	0	0	08/29/2007 10:32 (PDT)

2. Enter the search criteria you want and click Run Query.

To view a list of locations this user has logged in from

1. On the User Details page, click the Location tab.

The list of locations appears.

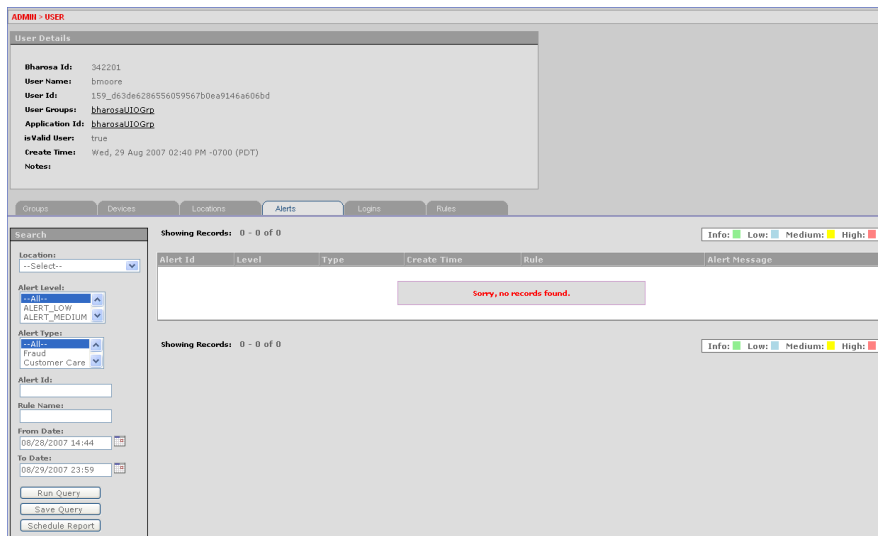


2. Enter the search criteria you want and click Run Query.

To view a list of alerts triggered a user

1. On the User Details page, click the Alerts tab.

The list of alerts appears.



2. To search for alerts, enter the search criteria you want and then click Run Query.

To view a list of logins by this user

1. On the User Details page, click the Logins tab.

The list of logins appears.

ADMIN - USER

User Details:

Bharosa Id: 342201
User Name: bmoore
User Id: 159_d63de628655609567b0ea9146a06bd
User Group: bharosAU0Grp
Application Id: bharosAU0Grp
IsValid User: true
Create Time: Wed, 29 Aug 2007 02:40 PM -0700 (PDT)
Notes:

Groups Devices Locations Alerts Logins **Rules**

Search:

Auth Status: All (Pending activation, Invalid)

Client Type: All (OCSP Question, Slider)

Check Alert Level: All (ALERT_LOW, ALERT_MEDIUM)

Application Id: All

Device Id:

IP Address:

Session Id:

From Date: 08/28/2007 14:45

To Date:

Showing Records: 1 - 1 of 1

Session Id	User Name	Auth Status	Pre Auth Score	Pre Auth Action	Post Auth Score	Post Auth Action	Login Time	Application Id	OS / Browser	Pre / Post
328501	bmoore	Success	0	PasswordTextPadGeneric	0	RegisterUserOptionalQuestionPad	08/29/2007 14:40 (PDT)	bharosAU0Grp	WinNT 5.1 / Gecko2007(Firefox2.0.0.6)	20 / 321

Showing Records: 1 - 1 of 1

2. Enter the search criteria you want and click Run Query.

To view a list of rules run on this user

1. On the User Details page, click the Rules tab.

The list of rules appears.

ADMIN - USER

User Details:

Bharosa Id: 342201
User Name: bmoore
User Id: 159_d63de628655609567b0ea9146a06bd
User Group: bharosAU0Grp
Application Id: bharosAU0Grp
IsValid User: true
Create Time: Wed, 29 Aug 2007 02:40 PM -0700 (PDT)
Notes:

Groups Devices Locations Alerts Logins **Rules**

Search:

Policy Type: All (Business, Third Party)

Model Run Times: All (Device Identification, AuthenPad)

Run Query

[- Expand All -] [- Collapse All -]

<input type="checkbox"/>	Preferences	Active	Weighted maximum Score
<input type="checkbox"/>	Pre-Authentication	Active	Weighted maximum Score
<input type="checkbox"/>	CC Challenge	Active	Weighted maximum Score
<input type="checkbox"/>	Fernet Password	Active	Weighted maximum Score
<input type="checkbox"/>	Post-Authentication	Active	Weighted maximum Score
<input type="checkbox"/>	Challenge-Question	Active	Weighted maximum Score

2. Enter the search criteria you want and click run Query.

Viewing the Details about Device IDs

The Device ID page provides information about the device used to login and cross-references information about the device including groups, users, locations, alerts and rules, and logins.

To view a list of groups this device belongs to

1. On the Device Details page, click the Group tab.

The list of groups appears.

The screenshot shows the 'DEVICE' page with the 'Groups' tab selected. The 'Device Details' section includes:

- Device Id: 357101
- Device Groups:
- Browser Fingerprint Id: 201
- Digital Fingerprint Id: 9701
- OS: WinNT 5.1
- Browser: Gecko2007(Firefox2.0.0.6)
- Create Time: Sat, 25 Aug 2007 00:20 PM -0700 (PDT)
- Notes:

The search interface below shows 'Showing Records: 0 - 0 of 0' and a message 'Sorry, no records found.'

2. Enter the search criteria you want and click Run Query.

To view a list of users that have used this device

1. On the Device Details page, click the Users tab.

The list of users appears.

The screenshot shows the 'DEVICE' page with the 'Users' tab selected. The 'Device Details' section is the same as in the previous screenshot.

The search interface shows 'Showing Records: 1 - 2 of 2' and a table of results:

User Name	Device Id	Login Failures	Login Successes	Challenge Failures	Challenge Successes	Last Used On
2222	357101	0	1	0	0	08/25/2007 12:20 (PDT)
bmooze	357101	0	1	0	0	08/29/2007 14:40 (PDT)

The search interface also includes buttons for 'Run Query', 'Save Query', 'Export Report', and 'Schedule Report'.

2. Enter the search criteria you want and click Run Query.

To view a list of locations from which a device has logged in

1. On the Device Details page, click the Locations tab.

The list of locations appears.

DEVICE

Device Details

Device Id: 357101
 Device Groups:
 Browser Fingerprint Id: 201
 Digital Fingerprint Id: 9701
 OS: WinNT 5.1
 Browser: Gecko2007(Firefox2.0.0.6)
 Create Time: Sat, 25 Aug 2007 00:20 PM -0700 (PDT)
 Notes:

Groups Users Locations Alerts / Rules Logins

Showing Records: 1 - 2 of 2 [Sort ▲]

Device Id	IP Address	City Name	State Name	Country Name	Login Failures	Login Successes	Challenge Failure Count	Challenge Success Count	Last Used On
357101	67.101.92.232	san francisco	california	united states	0	1	0	0	08/29/2007 15:46
357101	69.3.232.112	san francisco	california	united states	0	1	0	0	08/25/2007 12:20

Showing Records: 1 - 2 of 2 [Sort ▲]

Search

Auth Status: Pending activation (Blocked)

Location Type: IP Address

From Date: 07/30/2007 15:44

To Date: 08/29/2007 23:59

Run Query Save Query Export Report Schedule Report

2. Enter the search criteria you want and click Run Query.

To view a list of alerts and rules triggered by this device

1. On the Device Details page, click the Alerts/Rules tab.

The list of alerts and rules appears.

DEVICE

Device Details

Device Id: 357101
 Device Groups:
 Browser Fingerprint Id: 201
 Digital Fingerprint Id: 9701
 OS: WinNT 5.1
 Browser: Gecko2007(Firefox2.0.0.6)
 Create Time: Sat, 25 Aug 2007 00:20 PM -0700 (PDT)
 Notes:

Groups Users Locations Alerts / Rules Logins

Showing Records: 0 - 0 of 0

Alert Id Level Type Create Time Rule Alert Message

Sorry, no records found.

Showing Records: 0 - 0 of 0

Search

Location: --Select--

Alert Level: All

Alert Type: Fraud (Customer Care)

Alert Id:

Rule Name:

User Name:

From Date: 08/28/2007 15:46

To Date: 08/29/2007 23:59

Run Query Save Query Schedule Report

2. Enter the search criteria you want and click Run Query.

To view a list of logins by this device

1. On the Device Details page, click the Logins tab.

The list of logins appears.

DEVICE

Device Details

Device Id: 357101
 Device Group:
 Browser Fingerprint Id: 203
 Digital Fingerprint Id: 203
 OS: WinNT 5.1
 Browser: Gecko2007(Firefox2.0.0.6)
 Create Time: Sat, 25 Aug 2007 00:29 PM -0700 (PDT)
 Notes:

Groups Users Locations Alerts Rules Login

Showing Records: 1 - 1 of 1

Info: ■ Low ■ Medium ■ High

Session Id	Device Id	User Name	Auth. Status	Pre Auth. Score	Pre Auth. Action	Post Auth. Score	Post Auth. Action	Login Time	Application Id	OS / Browser	Browser Fingerprint	Location	IP Address	Client Type	Alerts
235551	357101	smoate	Success	0	PasswordTextPadGeneric	0	RegisterUserOptionalQuestionPad	08/23/2007 14:48 (PDT)	sharsaf@Corp	WinNT 5.1 / Gecko2007(Firefox2.0.0.6)	203 / 203	United States California San Francisco	62.101.97.232	Tei@Pad	

Showing Records: 1 - 1 of 1

Info: ■ Low ■ Medium ■ High

Search

Auth. Status: Pending activation, Blocked

Check Type: All, CAC Question, Error

Check Alert Level: All, ALERT_LOW, ALERT_MEDIUM

Application Id: All

User Name: []

IP Address: []

Session Id: []

From Date: [08/23/2007 15:49]

To Date: [08/23/2007 23:59]

Run Query
 Save Query
 Export Report
 Schedule Report

2. Enter the search criteria you want and click Run Query.

Viewing Details about Location Groups

To view the details about a location group

1. On the User, Device, or Location report page, click the Location for the customer login you want.

Or,

On the Dashboard page, click the information icon next to the item you want.

The Location Details page appears.

The screenshot shows the 'LOCATION - COUNTRY' page. The 'Country Details' section displays: Country Id: 1, Country Code: us, Country Name: united states, List All: States, and Notes. Below this is a navigation bar with tabs for Groups, Users, Devices, Alerts/Rules, and Logs. A search panel on the left includes a 'Cache Policy' dropdown (set to Full Cache), a 'Group Name' input field, and a 'Run Query' button. The main table shows one record: Demo-BL countries, Countries, Full Cache, and delete this group after demo.

Group Name	Group Type	Cache Policy	Description
Demo-BL countries	Countries	Full Cache	delete this group after demo

2. Enter the search criteria you want and click Run Query.

To view details about users from this location

1. On the Location Details page, click the Users tab.

The list of users appears.

The screenshot shows the 'LOCATION - COUNTRY' page with the 'Users' tab selected. The 'Country Details' section is the same as in the previous screenshot. The search panel on the left includes 'Auth Status' (set to All), 'From Date' (07/30/2007 16:29), and 'To Date' (08/29/2007 23:59). The main table has columns: User Name, Country Name, Login Failure Count, Login Success Count, Challenge Failure Count, Challenge Success Count, and Last Used On. A red message box says 'Click Run Query with appropriate search criteria.'

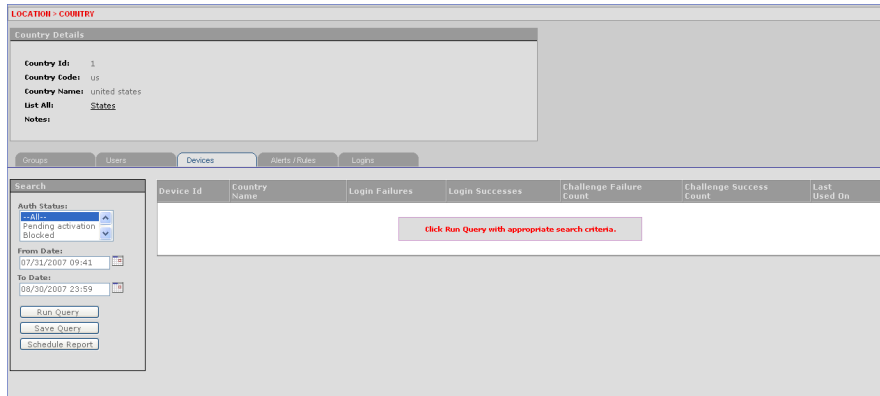
User Name	Country Name	Login Failure Count	Login Success Count	Challenge Failure Count	Challenge Success Count	Last Used On
-----------	--------------	---------------------	---------------------	-------------------------	-------------------------	--------------

2. Enter the search criteria you want and click Run Query.

To view a list of devices in this location

1. On the Location Details page, click the Devices tab.

The list of devices appears.

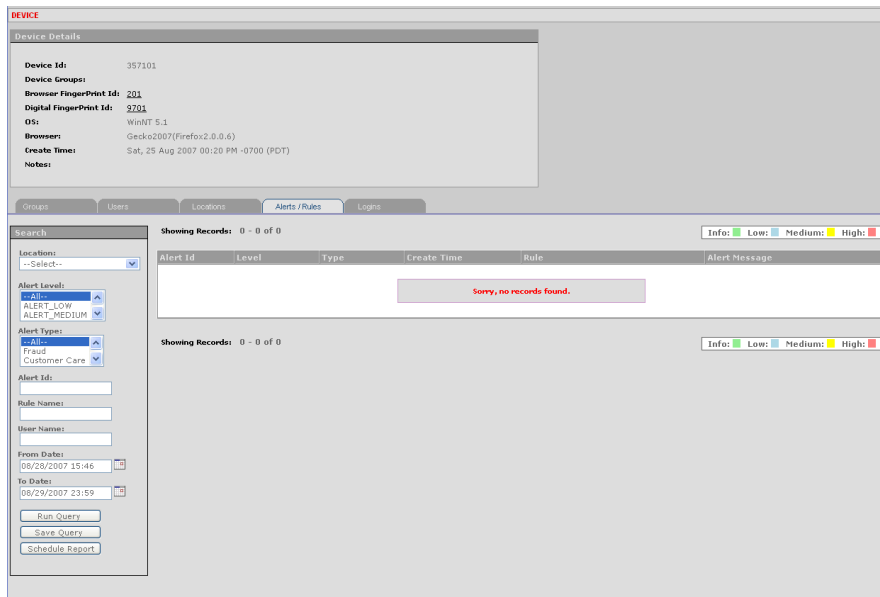


2. Enter the search criteria you want and click Run Query.

To view a list of alerts and rules triggered from this location

1. On the Location Details page, click the Alerts/Rules tab.

The list of alerts and rules appears.



2. Enter the search criteria you want and click Run Query.

To view a list of logins from this location

1. On the Location Details page, click the Logins tab.

The list of logins appears.

LOCATION - COUNTRY

Country Details

Country Id: 1
Country Code: US
Country Name: United States
Iso 3166: US252
Notes:

Groups Users Devices Alerts/Rules Logs

Showing Records: 1 - 5 of 5 [Start ▼]

Session Id	Location	IP_Address	User_Name	Auth Status	Pre Auth Score	Post Auth Action	Post Auth Score	Leads_Time	Application Id	OS / Browser	Browser Page / Page ID	Device ID	Alert Type	Alerts
295608	United States California San Francisco	65.12.172.148	test09302007012112	Pending	0	PasswordTextPad	1000	08/30/2007 01:21 (PDT)	shansa11050	WINNT 5.1/ Opera 9.5	2826 / 287302	287302	TextPad	Alert: User attempted to login from the same device a second time period
295607	United States California San Francisco	65.12.172.148	test09302007012112	Success	0	PasswordTextPadGeneric	1000	08/30/2007 01:21 (PDT)	shansa11050	MacOSX/ Gsk-e2096/Carnot 0.8.11	2823 / 287302	287302	TextPad	Alert: User attempted to login from the same device a second time period
295605	United States California San Francisco	65.12.172.148	test09302007012104	Pending	0	PasswordTextPad		08/30/2007 01:21 (PDT)	shansa11050	MacOSX/ Gsk-e2096/Carnot 0.8.11	2823 / 287302	287302	Login Page	
295605	United States California San Francisco	65.12.172.148	test09302007012104	Success	0	PasswordTextPadGeneric	1000	08/30/2007 01:21 (PDT)	shansa11050	WINNT 5.1/ MSIE 6.0	2826 / 287302	287302	TextPad	Alert: User attempted to login from the same device a second time period
295606	United States California San Francisco	65.12.172.148	test09302007012050	Success	0	PasswordTextPadGeneric	0	08/30/2007 01:21 (PDT)	shansa11050	WINNT 5.1/ MSIE 6.0	2826 / 287302	287302	TextPad	

Showing Records: 1 - 5 of 5 [Start ▼]

Info Low Medium High

2. Enter the search criteria you want and click Run Query.

Viewing Details about IP Addresses

To view details about the groups in which the IP is included

1. On the User, Device, or Location report page, click IP Address.

The IP Details page appears

A list of groups that include the IP is displayed.

The screenshot shows the 'LOCATION - IP' page. The 'IP Details' section displays the following information:

IP Address:	67.101.97.237	Notes:	
City Name:	san francisco	City CF:	90
State Name:	california	State CF:	94
Country Name:	united states	Country CF:	99
Top Level Domain:	net	Second Level Domain:	covad.net
Connection Type:	DSL	Connection Speed:	Medium
Is Aol:	No	Routing Type:	Fixed
ASN:	18566	Carrier:	covad communications co.

Below the IP details is a search interface for groups. The search criteria are set to 'All' for Cache Policy. The search results show 'Showing Records: 0 - 0 of 0' and a message: 'Sorry, no records found.'

2. Enter the search criteria you want and click Run Query.

To view details about the users associated with the IP address

1. On the IP Details page, click the Users tab.

A list of users who have used the IP is displayed.

The screenshot shows the 'LOCATION - IP' page with the 'Users' tab selected. The 'IP Details' section is the same as in the previous screenshot. The search interface for users is active, showing search criteria for Auth Status (All), From Date (07/31/2007 10:46), and To Date (08/20/2007 23:59). The search results show 'Showing Records: 1 - 1 of 1' and a table with the following data:

User Name	IP Address	City Name	State Name	Country Name	Login Failure Count	Login Success Count	Challenge Failure Count	Challenge Success Count	Last Used On
bmoore	67.101.97.237	san francisco	california	united states	0	1	0	1	08/29/2007 14:40

2. Enter the search criteria you want and click Run Query.

To view details about the devices associated with the IP address

1. On the IP Details page, click the Devices tab.

A list of devices with the IP address is displayed.

LOCATION = IP

IP Details

IP Address: 67.101.97.237 **Notes:**
City Name: san francisco **City CF:** 90
State Name: california **State CF:** 94
Country Name: united states **Country CF:** 99
Top Level Domain: net **Second Level Domain:** covad.net
Connection Type: DSL **Connection Speed:** Medium
Is Aol: No **Routing Type:** Fixed
ASN: 18566 **Carrier:** covad communications co.

Groups Users **Devices** Alerts / Rules Logins

Search

Auth Status: All (Pending activation, Blocked)

From Date: 07/31/2007 10:48
To Date: 08/30/2007 23:59

Run Query Save Query Export Report Schedule Report

Showing Records: 1 - 1 of 1

Device ID	IP Address	City Name	State Name	Country Name	Login Failures	Login Successes	Challenge Failure Count	Challenge Success Count	Last Used On
357101	67.101.97.232	san francisco	california	united states	0	2	0	2	08/29/2007 14:49

Showing Records: 1 - 1 of 1

2. Enter the search criteria you want, and click Run Query.

To view details about the alerts/rules associated with the IP address

1. On the IP Details page, click the Alerts/Rules tab.

A list of alerts/rules associated linked to the IP is displayed.

LOCATION = IP

IP Details

IP Address: 67.101.97.237 **Notes:**
City Name: san francisco **City CF:** 90
State Name: california **State CF:** 94
Country Name: united states **Country CF:** 99
Top Level Domain: net **Second Level Domain:** covad.net
Connection Type: DSL **Connection Speed:** Medium
Is Aol: No **Routing Type:** Fixed
ASN: 18566 **Carrier:** covad communications co.

Groups Users Devices **Alerts / Rules** Logins

Search

Alert Level: All (ALERT_LOW, ALERT_MEDIUM)

Alert Type: All (Fixed, Customer Care)

Alert ID: []

Rule Name: []

User Name: []

From Date: 08/29/2007 10:49
To Date: 08/30/2007 23:59

Run Query Save Query Schedule Report

Showing Records: 0 - 0 of 0

Alert ID	Level	Type	Create Time	Rule	Alert Message
Sorry, no records found.					

Showing Records: 0 - 0 of 0

2. Enter the search criteria you want and click Run Query.

To view details about the logins associated with the IP address

1. On the IP Details page, click the Logins tab.

A list of logins made from the included IPs is displayed.

LOCATM - IP

IP Details

IP Address:	67.151.97.237	Network:	
City Name:	san francisco	City CF:	90
State Name:	california	State CF:	94
Country Name:	united states	Country CF:	99
Top Level Domain:	net	Second Level Domain:	comcast.net
Connection Type:	DSL	Connection Speed:	Medium
AS Addr:	80	Routing Type:	Fixed
ASN:	18566	Carrier:	comcast communications co.

[Groups](#)
[Users](#)
[Devices](#)
[Alerts/Flags](#)
[Logout](#)

Showing Records: 1 - 1 of 1

Session ID	Location	IP Address	User Name	Auth Status	Auth. Score	Pre Auth Action	Post Auth Score	Post Auth Action	Login Time	Application ID	Browser	Browser Fingerprint ID	Device ID	Client Type	Alerts
155561		67.151.97.237	anonymous	Success	0	PasswordTextFieldGeneric	0	RegisterUserOptionalQuestion	08/29/2007 24:42 (PDT)	sharon@1066	win7 5.LF	206 / 326	351304	Tablet	

Showing Records: 1 - 1 of 1

Alerts: Info Low Medium High

2. Enter the search criteria you want and click Run Query.

Viewing Statistics about KBA Questions

You can statistics on question registration and challenge questions.

To view statistics about question registration

1. Click KBA on the Queries menu.

The KBA Registration page appears.

The report displays the number of users that performed each of the actions listed in the Item column and the percentage rate of successful challenges.

Item	Count	Percentages
Registrations	6	
Opt-outs	1	
Users who opted-out	1	
Question resets	0	0%
Users whose questions were reset	0	0%
Average question resets per user	0	
Question Set resets	0	0%
Users whose question sets were reset	0	0%
Average question set resets per user	0	

2. To locate the reports you want, enter the search criteria and then click Submit Query.

- To filter the list by primary authenticator for accounts, click in the Client Type box and select the authenticator you want.
- To Filter the list by the application ID of users, click in the Click in the Application ID box and select the ID you want.
- To filter the list by date range, click the calendar icons and select the From and To dates.

To view statistics about challenge responses

1. Click KBA on the Queries menu.

The KBA Challenge Response page appears.

The report displays the number of users that performed each of the actions listed in the Item column and the percentage of customers that responded to each question.

Item	Count	Percentages
Challenges	9	100%
Users Who Were Challenged	6	100%
Successful challenge responses	6	66.67%
Users who passed challenge	6	100%
Failed challenges	0	0%
Users who failed challenges	0	0%
Challenge question lockouts	0	0%
Users who were locked out	0	0%
Users with Failure counter > 0	0	0%
Average Challenges per user	1	
Users with multiple failures	0	0%

2. To locate the reports you want, enter the search criteria and then click Submit Query.
 - To filter the list by primary authenticator for accounts, click in the Client Type box and select the authenticator you want.
 - To Filter the list by the application ID of users, click in the Click in the Application ID box and select the ID you want.
 - To filter the list by date range, click the calendar icons and select the From and To dates.

To view statistics about each challenge question

1. Click KBA on the Queries menu.

The KBA Registration page appears.

The report displays the number of users that performed each of the actions listed in the Item column and the percentage of challenged customers.

Id #	Category	Question	Question Sets with Question	Users Registered For Question	% of Users Registered For Question	% of Successful Challenges	% of Unsuccessful Challenges
78	Education	What year did you graduate from college?	1	0	0 %	0%	0%
79	Education	What was your combined SAT score?	1	1	100 %	0%	0%
80	Education	What year did you start college?	0	0	0 %	0%	0%
81	Education	What was your major in college?	0	0	0 %	0%	0%
82	Education	What is the last name of your kindergarten teacher?	0	0	0 %	0%	0%
83	Education	What is the last name of your first grade teacher?	0	0	0 %	0%	0%
84	Education	What the the first school you ever attended?	0	0	0 %	0%	0%
85	Education	What was the name of your first roommate in college?	0	0	0 %	0%	0%
86	Education	In what city was your first elementary school?	0	0	0 %	0%	0%
87	Education	What is the first name of your high school best friend?	0	0	0 %	0%	0%
88	Education	What is the last name of your high school best friend?	0	0	0 %	0%	0%
89	Education	What is the name of a college you applied to but did not attend?	0	0	0 %	0%	0%
90	Education	What is the last name of your favorite teacher in High School?	0	0	0 %	0%	0%
91	Education	What is the last name of your favorite professor in college?	0	0	0 %	0%	0%
92	Miscellaneous	What is your best friend's birthday (MMDD)?	0	0	0 %	0%	100%
93	Miscellaneous	What color was your first bicycle?	0	0	0 %	0%	0%
94	Miscellaneous	What is the name of the first musical group you saw in concert?	1	0	0 %	0%	0%
95	Miscellaneous	What is your height? (for example 6 foot 0 inches = 60)	1	0	0 %	0%	0%
96	Miscellaneous	What year did you go to your first music concert?	2	0	0 %	0%	0%
97	Miscellaneous	What are the last four digits of your lotto numbers?	2	0	0 %	0%	0%

2. To locate the reports you want, enter the search criteria and then click Submit Query.
 - To filter the list by question category, click in the Category box and select the category you want.
 - To filter out all questions containing a specific word, enter the word in the Question Keyword field.
 - To filter the list by status, select the status you want from the status list.
 - To filter the list by date range, click the calendar icons and select the From and To dates.

Viewing a List of Saved Reports

To view a list of saved reports

1. Click Saved Reports on the Queries menu.

The Saved Reports page appears listing all the saved reports.

Download	Report Name	Description	Created Date	Status
For Getting Saved Reports List, click Submit Query with appropriate search criteria.				

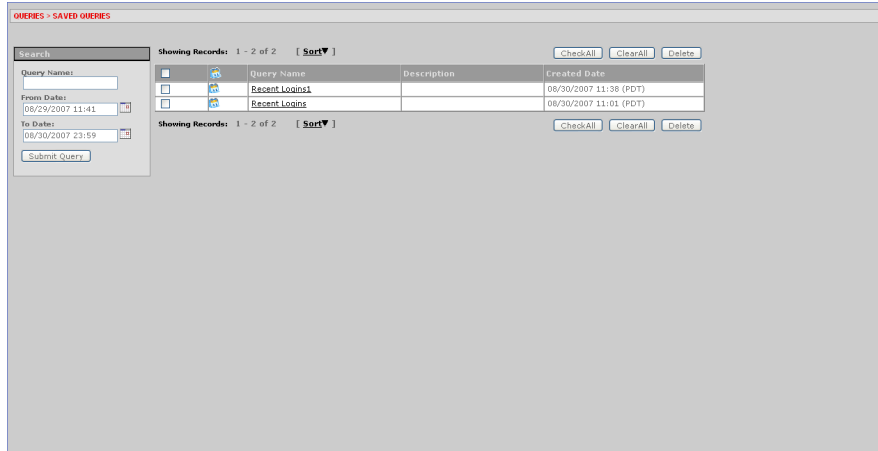
2. To locate the reports you want, enter the search criteria and then click Submit Query.
3. Select the button to the left of the report you want to download.
4. Click in the File Type box and select the type you want.
5. Click Download.

Viewing a List of Saved Queries

To view a list of saved queries

1. Click Saved Queries on the Queries menu.

The Saved Queries page appears listing all the saved queries.



2. To locate the saved queries you want, click the calendar icons and select the From and To dates you want.
3. Click the Query Name to view search criteria.
The search parameters appear to the right.
4. To run the query, click Run Query.
5. To delete a query click the check box next to the query name then hit the delete button.

You can also edit, re-save, and schedule a saved query.

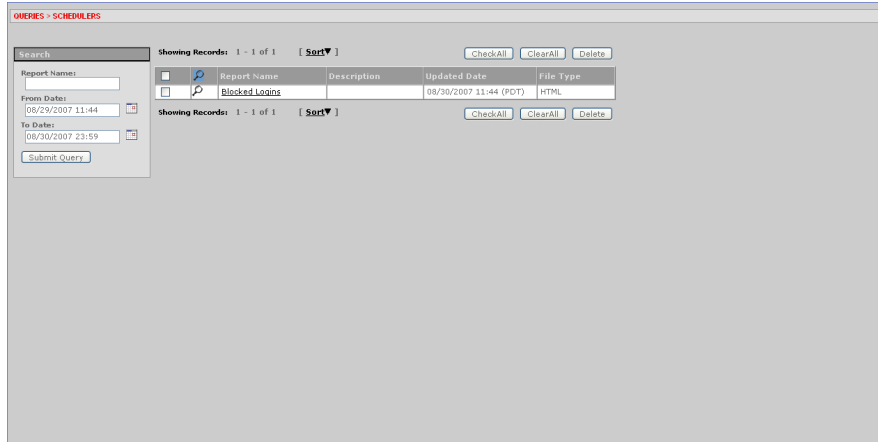
Viewing a List of Schedulers

You can view a list of all schedulers that have been created to run reports by date and time or by interval.

To view a list of schedulers

- 1. Click Schedulers on the Queries menu.**

The Schedulers page appears listing all existing schedulers.



- 2. To locate the schedulers you want, click the calendar icons and select the From and To dates you want.**
- 3. Click the scheduler to view the schedule parameters.**

The schedule parameters appear.
- 4. You may edit and re-save schedulers.**

Glossary

Action – A response that is triggered by a rule, such as forcing a challenge question after x login attempts within x period of time.

Alert – A graded and customizable message triggered by a rule..

Device – A Computer, PDA, cell phone, kiosk, etc.

Group – A collection of users, locations, devices, actions, or alerts.

Location – A city, state, country, IPs, or IP range.

Model – A set of rules that, when linked to a group, are used by Oracle Adaptive Access Manager to evaluate the group member's activity.

Rule – A configurable evaluator of system traffic that can trigger alerts, actions and generate a risk score.