keynote

DeviceAnywhere

The #1 Mobile Testing Platform

DeviceAnywhere Enterprise Monitoring

Portal Guide

Release 6.0

DeviceAnywhere Enterprise Monitoring 6.0

June 2013

Copyright Notice

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY EXPRESS REPRESENTATIONS OF WARRANTIES. IN ADDITION, KEYNOTE DISCLAIMS ALL IMPLIED REPRESENTATIONS AND WARRANTIES, INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

Please forward any comments or suggestions regarding this document to Keynote Support.

Keynote Systems, Inc.
777 Mariners Island Blvd.
San Mateo, CA 94404

Contents

About This Document

This document describes how to view and interpret monitoring data uploaded from Keynote's DeviceAnywhere Enterprise Monitoring (DAE Monitoring) to the DAE Monitoring Portal.

DAE Monitoring is an enterprise-class service for monitoring mobile network and application availability and performance on smart devices. With DAE Monitoring, production support teams can easily write/record monitor scripts and schedule them at any frequency on real, live devices. You can define custom thresholds for acceptable performance and the alerts that are triggered when policies are violated. Alert responses include customizable, instant email or SNMP notifications (with up to three escalation paths) and adjusted monitor frequency.

The DAE Monitoring Portal provides a real-time dashboard view of currently running monitors and live device screens as scripts are executed on them. Users can also view historical monitor data such as a list of all monitor executions, success rates for individual monitors, error reports, trend charts, and detailed results for individual script runs complete with device screenshots. All standard reports can be customized for display using filters and date ranges. Users with permissions can exclude specific runs from some reports. Additionally, users can save customized report criteria and set up schedules for periodic generation and delivery of reports. Monitor reporting data aids immediate incident tracking and management as well as mid- to long-term trend analysis for the purposes of product improvement and performance benchmarking.

This document introduces DAE Monitoring reporting concepts and describes how to access and interpret data, share and export results, generate graphs, and save/export reports.

Document Outline

This document assumes that you are familiar with DeviceAnywhere Enterprise Monitoring concepts and with creating and scheduling monitor scripts in the DeviceAnywhere Studio client application. Please refer to the *DAE Automation User Guide* for detailed instructions on working in the visual scripting environment.

In this document:

Getting Started describes how to access the DAE Monitoring portal and contains brief descriptions of important concepts and an overview of its various sections.

Dashboard describes how to interpret latest run information in the dashboard, including monitor status and result icons and trend graphics. You can also read about viewing a live device during monitor runs.

Execution Report describes the detailed list of every monitor run over a specified date range in your DAE Monitoring system.

Monitors describes the monitor summary and list of monitor incidents available in the **Monitors** view of the DAE Monitoring Portal. Links to access more detailed reports are also discussed.

Transactions describes the transaction summary and list of transaction incidents available in the **Transactions** view of the DAE Monitoring Portal. Links to access more detailed reports are also discussed.

Detailed Reports describes monitor and transaction details, incident reports, and detailed run results, which are accessible at several points in the DAE Monitoring Portal.

Charts describes the types of charts available in the DAE Monitoring Portal and explains standard chart types with examples.

Saving Reports and Criteria describes how to save reports and criteria, and how to generate reports from saved criteria.

Typographical Conventions

The table below describes the typographical conventions used in Keynote DeviceAnywhere documentation.

Style	Element	Examples
Blue	Links and email addresses	http://www.keynotedeviceanywhere.com The Document Outline section describes the structure of this manual.
Bold	User interface elements such as menu items	Click **My Devices** in DeviceAnywhere Studio.
`Monospace`	Commands, code output, filenames, directories	Right-click the project's `test cases` directory.
`Monospace bold`	User input	In a command window, type **`adb devices`**.
Italic	Document titles and emphasis	Refer to the *DeviceAnywhere Enterprise Automation User Guide* to learn how to script.

Contacting Support

If you have any comments or suggestions regarding this document, contact Keynote Support. For inquiries about DeviceAnywhere product demonstrations and consulting services, contact your Keynote Solutions Consultant.

Customers can find additional support information at http://support.keynote.com or 1-888-KEY-SYST (539-7978).

Additional Documentation

You can find additional information at http://www.keynotedeviceanywhere.com/monitoring-documentation.html. This includes the following documents:

- *DAE Monitoring Release Notes*
- *DAE Monitoring Best Practice Workflow*

You can also find these documents on interacting with devices and working in the visual scripting environment in DeviceAnywhere Studio:

- *DAE Automation User Guide*—refer to chapters on Projects, Working with Commands, Actions, States, Test Cases, and the Command Reference.

  NOTE This manual deals primarily with using DeviceAnywhere Enterprise Automation for pre-deployment testing of mobile applications, services, and devices.

- *DAE Interactive User Guide*—learn about device interaction and process improvement and collaboration tools available in DeviceAnywhere Studio.

You can also access documentation from the **Help** menu in DeviceAnywhere Studio.

1 Getting Started

Keynote's DeviceAnywhere Enterprise Monitoring Portal is certified on the following browsers:

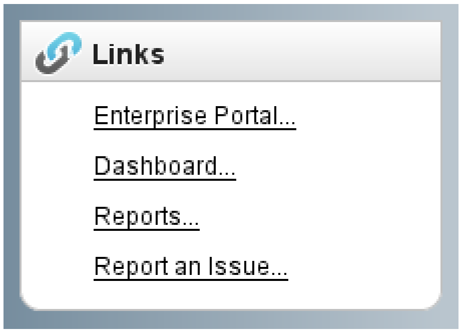
- Mozilla Firefox 11 or higher
- Windows Internet Explorer 8, 9, and 10 with Document Mode set to Internet Explorer 9
- Safari 5.0 or higher
- Chrome 16 or higher

1.1 Log In to the Portal and Launch DeviceAnywhere Studio

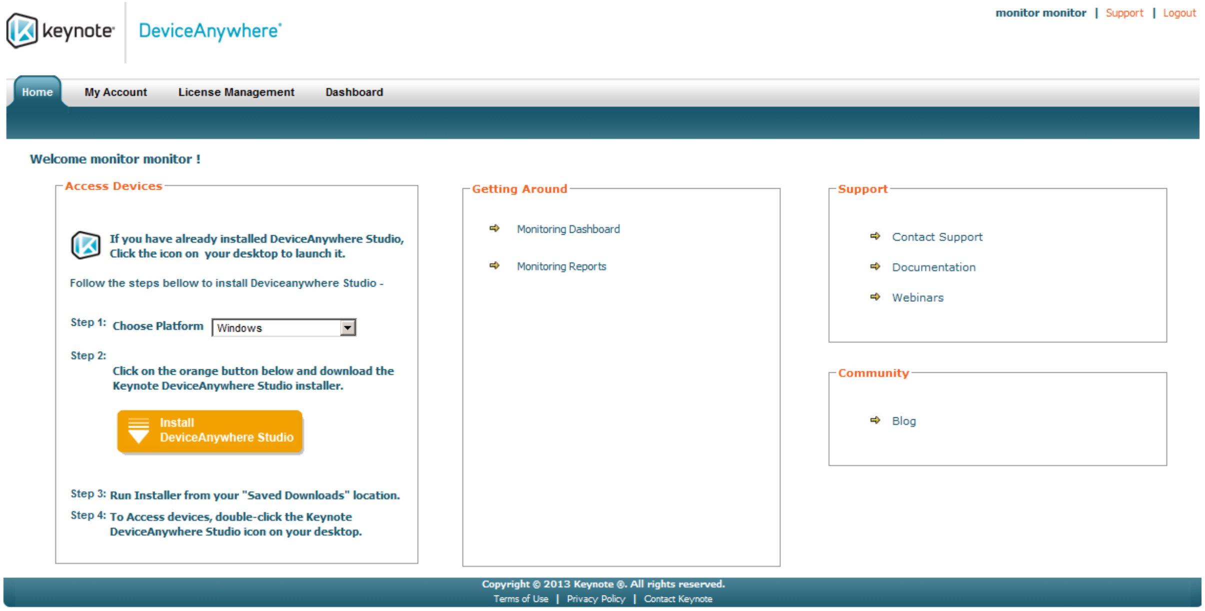
To begin using the DAE Monitoring Portal, you must:

1 Launch and log in to DeviceAnywhere Studio.

2 Select **Enterprise Portal** from the Links view in the sidebar.



You are directed to the landing page of the DAE Monitoring Portal.


keynote
DeviceAnywhere
monitor monitor | Support | Logout
Home
My Account
License Management
Dashboard
Install DeviceAnywhere Studio

Welcome monitor monitor !

Access Devices

If you have already installed DeviceAnywhere Studio, Click the icon on your desktop to launch it.

Follow the steps bellow to install Deviceanywhere Studio -

Step 1: Choose Platform Windows

Step 2: Click on the orange button below and download the Keynote DeviceAnywhere Studio installer.

Step 3: Run Installer from your "Saved Downloads" location.

Step 4: To Access devices, double-click the Keynote DeviceAnywhere Studio icon on your desktop.

Getting Around

- Monitoring Dashboard
- Monitoring Reports

Support

- Contact Support
- Documentation
- Webinars

Community

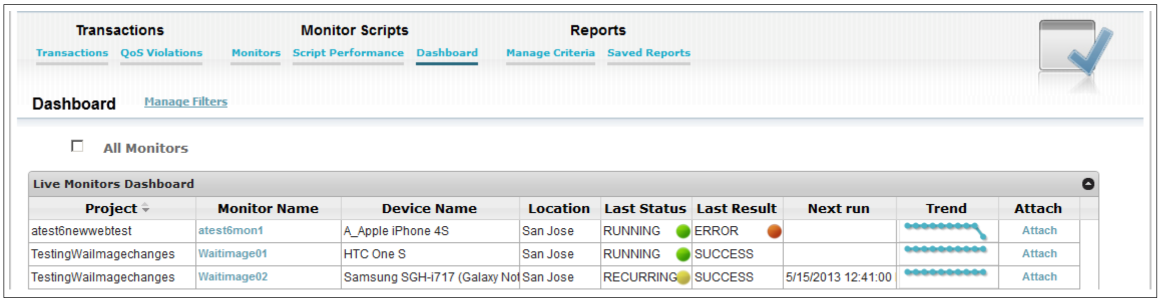
- Blog

Copyright © 2013 Keynote ®. All rights reserved.
Terms of Use | Privacy Policy | Contact Keynote

NOTE You can also log in directly to the portal at `<Server_address>/Login.aspx`, where `<Server_address>` is the machine hosting the DAE Monitoring Portal.

3 Select a link in the Getting Around section to access monitoring data:

- **Monitoring Dashboard** takes you to the dashboard view of currently executing monitors (**Dashboard** tab). This is briefly described in DAE Monitoring Portal Overview and discussed in detail in Dashboard.



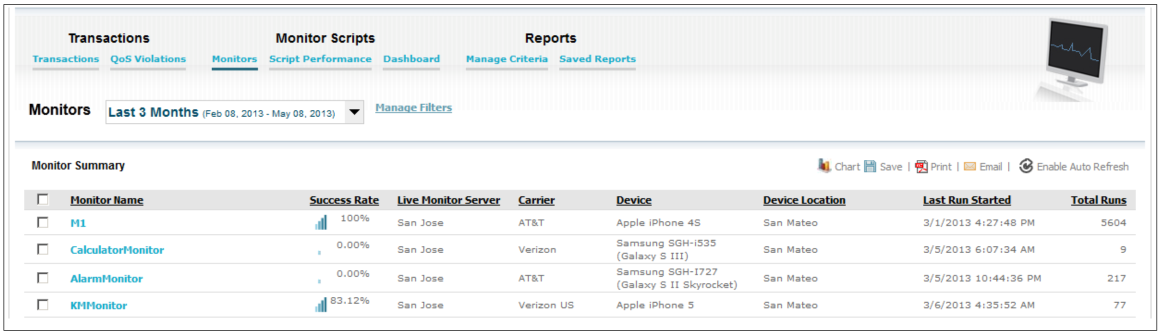
Dashboard Manage Filters

□ All Monitors

Live Monitors Dashboard

Project	Monitor Name	Device Name	Location	Last Status	Last Result	Next run	Trend	Attach
atest6newwebtest	atest6mon1	A_Apple iPhone 4S	San Jose	RUNNING ●	ERROR ●			Attach
TestingWaiImagechanges	Waitimage01	HTC One S	San Jose	RUNNING ●	SUCCESS			Attach
TestingWaiImagechanges	Waitimage02	Samsung SGH-i717 (Galaxy Not	San Jose	RECURRING●	SUCCESS	5/15/2013 12:41:00		Attach

- **Monitoring Reports** shows success rates and total number of runs for your monitors (**Monitors** tab). This is briefly described in DAE Monitoring Portal Overview and discussed in detail in Monitors.



Monitors Last 3 Months (Feb 08, 2013 - May 08, 2013) Manage Filters

Monitor Summary

□	Monitor Name	Success Rate	Live Monitor Server	Carrier	Device	Device Location	Last Run Started	Total Runs
□	M1	100%	San Jose	AT&T	Apple iPhone 4S	San Mateo	3/1/2013 4:27:48 PM	5604
□	CalculatorMonitor	0.00%	San Jose	Verizon	Samsung SGH-i535 (Galaxy S III)	San Mateo	3/5/2013 6:07:34 AM	9
□	AlarmMonitor	0.00%	San Jose	AT&T	Samsung SGH-I727 (Galaxy S II Skyrocket)	San Mateo	3/5/2013 10:44:36 PM	217
□	KMMonitor	83.12%	San Jose	Verizon US	Apple iPhone 5	San Mateo	3/6/2013 4:35:52 AM	77

NOTE You can also access this page by clicking **Reports** in the DeviceAnywhere Studio sidebar.

1.2 DAE Monitoring Concepts

This section briefly describes important monitor scripting concepts and reporting concepts that are foundational to understanding and interpreting data in the DAE Monitoring Portal.

1.2.1 Monitor Scripting Concepts

Users create monitor scripts, performance criteria, and schedules in the DeviceAnywhere Studio client software. Scripting and scheduling tools enable users to measure the overall performance of a monitor script as well as key portions of a script, called transactions.

Monitor

In the DAE Monitoring scripting architecture, a *test case* is the broad process that represents the monitoring scenario for your mobile application, content, or device. For example, a test case might consist of logging in to and checking balances in a mobile banking application, or searching for flights based on search criteria entered in a mobile browser. Test cases are comprised of one or more *actions*, the discrete procedures that make up the larger process that is the test case.

A test case scheduled to run at a specified frequency on a monitor server and on a specified device (or multiple devices for a multi-device test case) is a monitor.

Transaction

Named transactions are used within monitor scripts (in test cases and/or constituent actions) to delimit crucial interactions with your application or service that you would like to track the performance of. For example, in a monitor script for a banking application, you might want to use a transaction to track logging in. In a monitor for a mobile airline website, you might want to track receiving results after entering search criteria for flights. You would not, for instance, use a transaction to track resetting a device to the home screen—these types of interactions are necessary in a monitor script to set up service measurements, but their success or failure has no bearing on the performance of your mobile application or service.

You can track transaction completion times as compared to an acceptable threshold as well as the failure of a transaction to be completed as expected.

Transactions can be used in multiple monitors, enabling you to compare the same set of interactions across different monitors, e.g., the time taken to log in to an application on three different devices.

1.2.2 Reporting Concepts

This section provides brief definitions and descriptions of DAE Monitoring Portal elements, reporting data, report types, and information on where to find them.

Dashboard

The dashboard (Dashboard tab) provides the ability to view the status of most recently executed monitor runs, upcoming scheduled runs, and live device screens as monitor scripts are being executed on them. Monitors runs during an alert suppression window also show up in the dashboard. Icons provide a quick visual indication of run result (success or failure) and monitor status (running, disabled, etc.). A link next to each monitor allows you to view the device screen as the monitor script is being executed on it.

Execution Report

The execution report (Execution Report link) is the exhaustive list of every single monitor run in your system, excluding runs during an alert suppression window. By default, runs are arranged most recent first, with information on device, carrier, run result, and a link to view screen-by-screen results for failed runs. Users with permissions can exclude specific runs from the execution report, which also excludes them from all other reports in the DAE Monitoring Portal.

Monitor Summary Report

The monitor summary in the Monitor Scripts view displays the overall success rate and total number of runs for every monitor in your system over a specified date range. Each monitor has a link to view monitor details, which include errors encountered, transaction run times, and incidents. You can select monitors to be displayed in a comparative chart of transaction times (monitor performance) or a visual representation of monitor success or failure (monitor availability) over a period of time.

Monitor Details

The monitor details report, which opens up when you click the name of a monitor anywhere in the DAE Monitoring Portal, displays the total number of runs, success rate, a graphic representation of the success rate and failures (by error type), transaction times, and a list of incidents and their violation levels. There are also links to view detailed incident reports and screen-by-screen results for failed runs.

Transaction Summary Report

The transaction summary in the Transactions view displays the success rate and total number of transaction runs over a specified date range for every transaction in your system. Transaction details can be viewed by clicking a transaction name.

You can select transactions to be displayed in a comparative chart of transaction times (transaction performance) or a visual representation of transaction success or failure (transaction availability) over a period of time.

Transaction Details Report

The transaction details report opens up when you click the name of a transaction. It displays the total number of transaction runs with the success rate and its graphic representation. It lists the monitors, devices, and locations from which the transaction has been executed and also lists total number of transaction incidents and escalations at each level.

Excluding Runs

Users with the Account Admin role can exclude specific runs from calculations in the monitor details report and from the execution report. Other users can view a list of all, excluded, or included runs as well as click links for detailed results of failed runs.

Incident and Incident Summaries

The first run that violates a transaction or monitor policy generates an incident. An incident begins at the lowest escalation level and is tracked through up to two further levels until it is resolved. Incidents may be resolved at any escalation level.

The most recent monitor incidents and their current status are displayed in the Script Performance tab. The most recent transaction incidents are displayed in the QoS Violations tab. Click an **Incident Start Time** to view a detailed incident report.

Incident Report

An incident report displays a run-by-run analysis of an incident, from the first level of escalation when alerts were sent out to incident resolution. It also displays a graph transaction success rate based on the runs contributing to the incident.

Availability Chart

Availability charts visually represent the success or failure of a transaction or monitor over a period of time. A value of 100 represents a success while 0 represents a failure. However, when viewing availability over a long period of time, data may be aggregated and then averaged over smaller intervals.

Performance Chart

You can select monitors to be displayed in a comparative chart of transaction completion times over a selected date range. A performance chart for transactions shows the completion times of each transaction selected over the date range chosen.

Candlestick Chart

A candlestick chart shows the maximum, minimum, and average run time for a transaction at different points in the day over the date range chosen.

Report Criteria

Report criteria are the various headings of information for which data points are gathered, analyzed, and displayed in the various report types on the DAE Monitoring Portal. For example, the report criteria for the monitor summary report include the list of monitors executed over a date range, their success rate, and the number of runs. These criteria (including any custom filters applied) can be customized, saved and scheduled for periodic data gathering and generation of reports. Saved criteria are listed in the Manage Criteria tab.

Saving Reports

At various points in the DAE Monitoring portal, you can save one-time, ad hoc reports (i.e., graphs and raw or aggregated data) or you can save report criteria in order to schedule reports for periodic generation. Saved reports are listed in the Saved Reports tab. Saved criteria are listed in Manage Criteria.

Detailed Results for Failed Runs

At various points in the DAE Monitoring Portal, you can click links for detailed results for script runs that encountered a monitor failure, transaction violation, or a system error. The detailed results page contains a clickable script command tree and screenshots of actual vs. expected results. Click any node of the command tree to view any nested commands and detailed results.

Vuser Chart

The Vuser chart shows the number of Vuser licenses used at any minute in your system over a specified period of time. If you have 2 Vuser licenses, you might still be able to execute 4 monitors a minute using 2 licenses for 25 seconds at a time. The image below shows Vuser license usage for two LiveMonitor Server locations (in green and yellow). Hover over a point to see the associated number of Vuser licenses.

Sorting and Filtering

The lists of runs, monitors, and transactions in most tabs of the DAE Monitoring Portal can be sorted by column. Data can be filtered by date range and other criteria. For instance, the list of transaction incidents in the **QoS Violations** tab can be filtered by project so that only incidents pertaining to transactions in a particular project (in DeviceAnywhere Studio) are displayed.

Exporting Reports

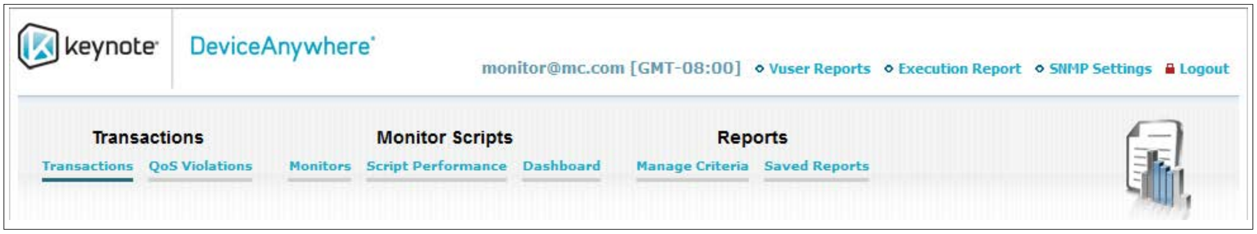
You can **Print** or **Email** PDF reports. Report emails can be sent to users in your DAE Monitoring environment or to other write-in addresses. You can also **Download** aggregated or raw report data in Excel format.

NOTE Raw data is not available for date ranges over 5 days.

1.3 DAE Monitoring Portal Overview

This section describes the information to be found in each of the main views of the DAE Monitoring Portal.

Figure 1-1 Main Portal Links



Dashboard

The **Dashboard** provides a view of the most recent run/status of monitors over a specific date range (the default date range is the current day). You can also view live device screens and a log of script commands as monitors are being executed.

Monitor Scripts View

The Monitor Scripts view displays information pertaining to entire monitor script runs and monitor incidents (see DAE Monitoring Concepts for definitions of monitors and transactions).

- The **Monitors** tab displays the success rate and total number of runs of each monitor in your system over a given period of time.
- The **Script Performance** tab displays monitor incidents, defined as the violations of monitor policies set up by the user.

Transactions View

DAE Monitoring enables you to measure the overall performance of a script as well as for portions of your script, called transactions. Transactions enable you to track the performance of crucial aspects of your application or service, e.g., the time taken for a site to load (see DAE Monitoring Concepts for definitions of monitors and transactions). Delineating transactions enables you to distinguish between service/application issues and device/script issues, which do not indicate a service issue.

- The **Transactions** tab displays the success rate, i.e., the percentage of runs in which performance criteria were met, of each transaction in your system over a given period of time.
- The **QoS Violations** tab tracks transaction incidents.

Reports View

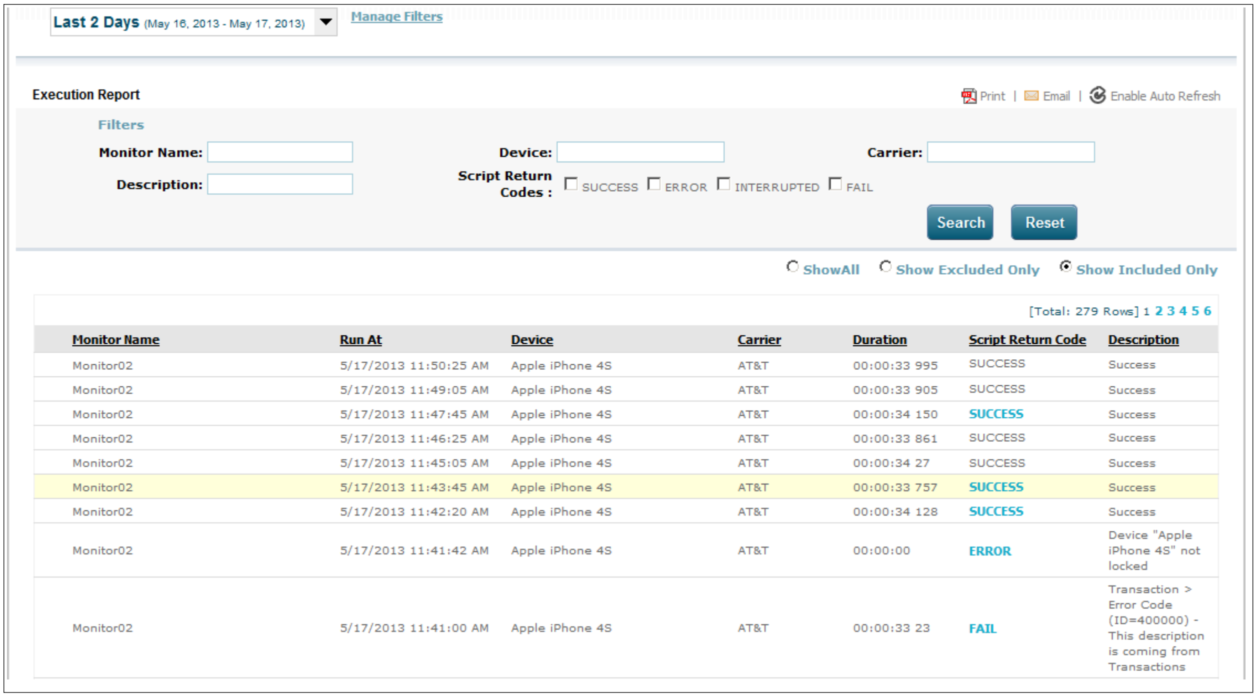
At various points in the DAE Monitoring Portal, you can save one-time, ad hoc reports or you can save customized report criteria.

- The **Saved Reports** tab displays one-time reports that you have saved.
- The **Manage Criteria** tab displays report criteria you have saved. In this tab, you can manage criteria and schedule criteria for periodic report generation.

Execution Report

Clicking the **Execution Report** link at the top-right corner of the window displays a list of all monitor runs for a given date range. The default range is the current day. Runs are displayed with information on monitor name, time the run began, length of run, device, carrier, and run outcome.

Figure 1-2 Execution Report



Last 2 Days (May 16, 2013 - May 17, 2013)
Manage Filters
Print | Email | Enable Auto Refresh
Search
Reset

Execution Report

Filters

Monitor Name:

Description:

Device:

Script Return Codes : □ SUCCESS □ ERROR □ INTERRUPTED □ FAIL

Carrier:

○ ShowAll ○ Show Excluded Only ● Show Included Only

[Total: 279 Rows] 1 2 3 4 5 6

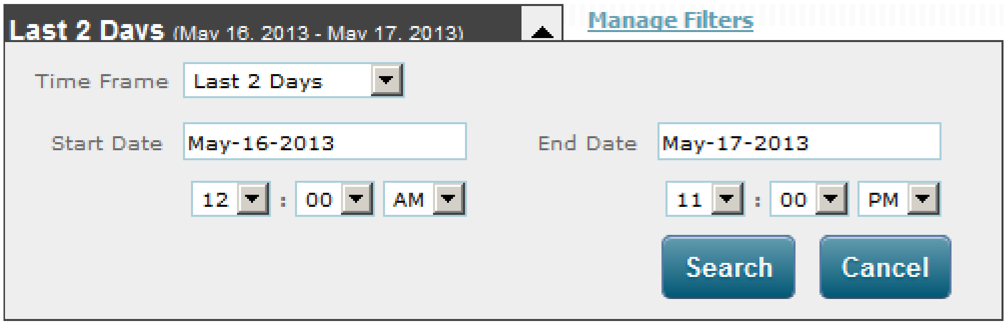
Monitor Name	Run At	Device	Carrier	Duration	Script Return Code	Description
Monitor02	5/17/2013 11:50:25 AM	Apple iPhone 4S	AT&T	00:00:33 995	SUCCESS	Success
Monitor02	5/17/2013 11:49:05 AM	Apple iPhone 4S	AT&T	00:00:33 905	SUCCESS	Success
Monitor02	5/17/2013 11:47:45 AM	Apple iPhone 4S	AT&T	00:00:34 150	SUCCESS	Success
Monitor02	5/17/2013 11:46:25 AM	Apple iPhone 4S	AT&T	00:00:33 861	SUCCESS	Success
Monitor02	5/17/2013 11:45:05 AM	Apple iPhone 4S	AT&T	00:00:34 27	SUCCESS	Success
Monitor02	5/17/2013 11:43:45 AM	Apple iPhone 4S	AT&T	00:00:33 757	SUCCESS	Success
Monitor02	5/17/2013 11:42:20 AM	Apple iPhone 4S	AT&T	00:00:34 128	SUCCESS	Success
Monitor02	5/17/2013 11:41:42 AM	Apple iPhone 4S	AT&T	00:00:00	ERROR	Device "Apple iPhone 4S" not locked
Monitor02	5/17/2013 11:41:00 AM	Apple iPhone 4S	AT&T	00:00:33 23	FAIL	Transaction > Error Code (ID=400000) - This description is coming from Transactions

1.4 Standard Operations in the Portal

All data displayed in the Portal can be filtered by date range (additional filter criteria are covered in discussions of the various reports they are available for).

To change the date range for a report, click the arrow next to the date range field at the top left of the page.

Figure 1-3 Changing the Date Range



Time Frame: Last 2 Days

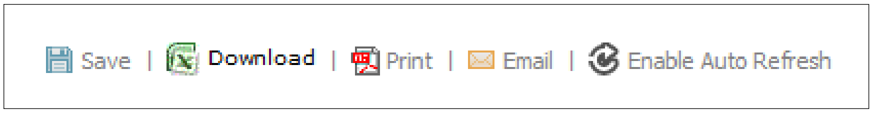
Start Date: May-16-2013 12 : 00 AM

End Date: May-17-2013 11 : 00 PM

Select a predefined **Time Frame**, or to define your own window, choose **Custom Dates**. Then select a **Start Date** and time as well as an **End Date** and time. Click **Search** to apply your date range.

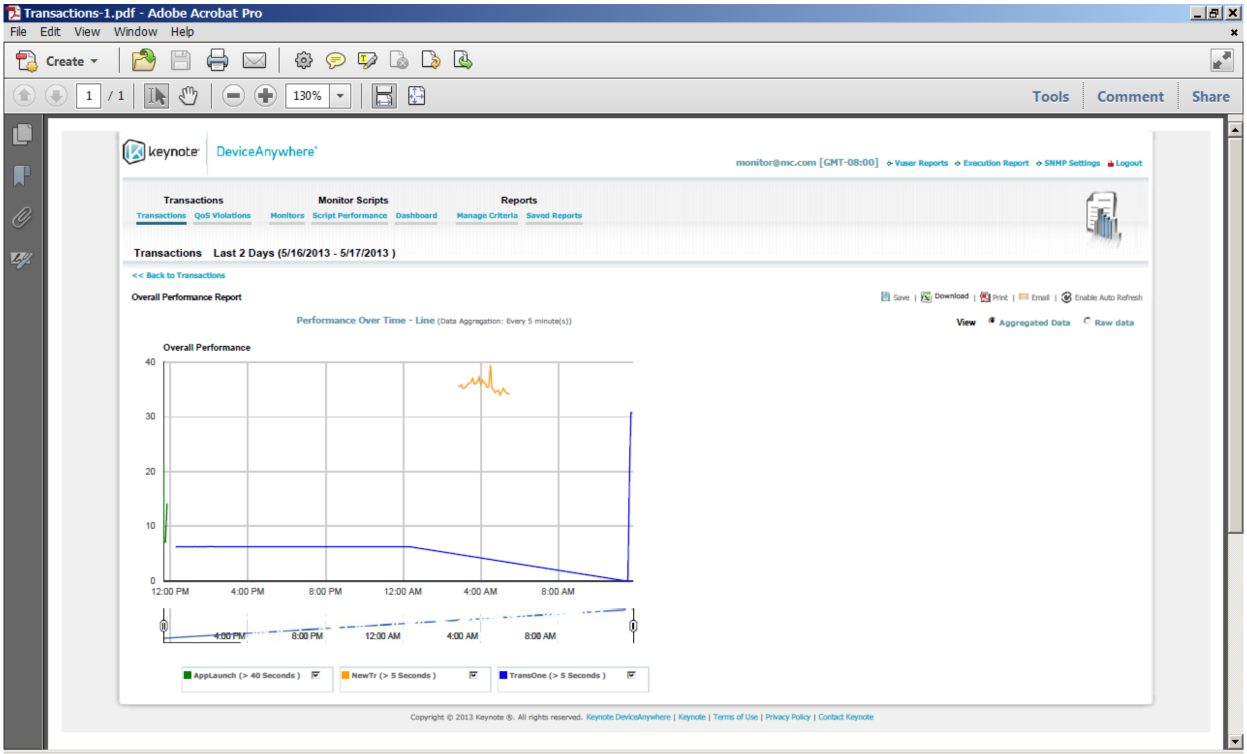
You can **Print** or **Email** reports (i.e., the pages displayed as you drill down through the various tabs in the DAE Monitoring Portal) as PDF files. Links to print and email reports can be found at the top-right corner of Portal pages. (The **Chart** and **Save** links are discussed in Charts and Saving Reports and Criteria, respectively.)

Figure 1-4 Print or Email a Report



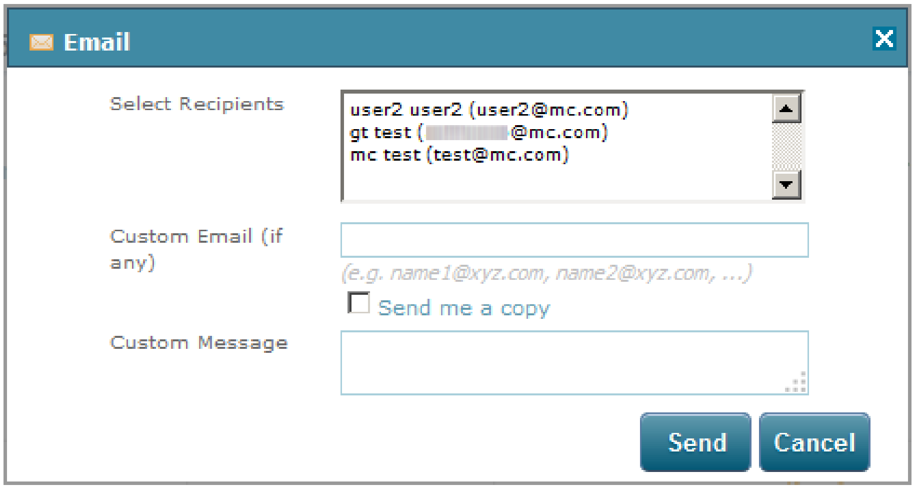
When you select **Print**, the current page is saved as a PDF file that can be downloaded to your file system. The image below shows a PDF file generated from a transaction performance chart.

Figure 1-5 Print to PDF


Transactions-1.pdf - Adobe Acrobat Pro
File Edit View Window Help
Create
1 / 1
130%
Tools Comment Share
keynote DeviceAnywhere
monitor@mc.com [GMT-08:00] Vuser Reports Execution Report SNMP Settings Logout
Transactions Monitor Scripts Reports
Transactions QoS Violations Monitors Script Performance Dashboard Manage Criteria Saved Reports
Transactions Last 2 Days (5/16/2013 - 5/17/2013)
<< Back to Transactions
Overall Performance Report
Save | Download | Print | Email | Enable Auto Refresh
Performance Over Time - Line (Data Aggregation: Every 5 minute(s))
View ● Aggregated Data ○ Raw data
Overall Performance
40
30
20
10
0
12:00 PM
4:00 PM
8:00 PM
12:00 AM
4:00 AM
8:00 AM
4:00 PM
8:00 PM
12:00 AM
4:00 AM
8:00 AM
🟩 AppLaunch (> 40 Seconds)
🟧 NewTr (> 5 Seconds)
🟦 TransOne (> 5 Seconds)
Copyright © 2013 Keynote ®. All rights reserved. Keynote DeviceAnywhere | Keynote | Terms of Use | Privacy Policy | Contact Keynote

Report emails can be sent to users in your DAE Monitoring environment or to other write-in addresses. Email recipients receive a PDF file of the report.

Figure 1-6 Emailing a Report



Select Recipients

user2 user2 (user2@mc.com)
gt test ([redacted]@mc.com)
mc test (test@mc.com)

Custom Email (if any)

(e.g. name1@xyz.com, name2@xyz.com, ...)

□ Send me a copy

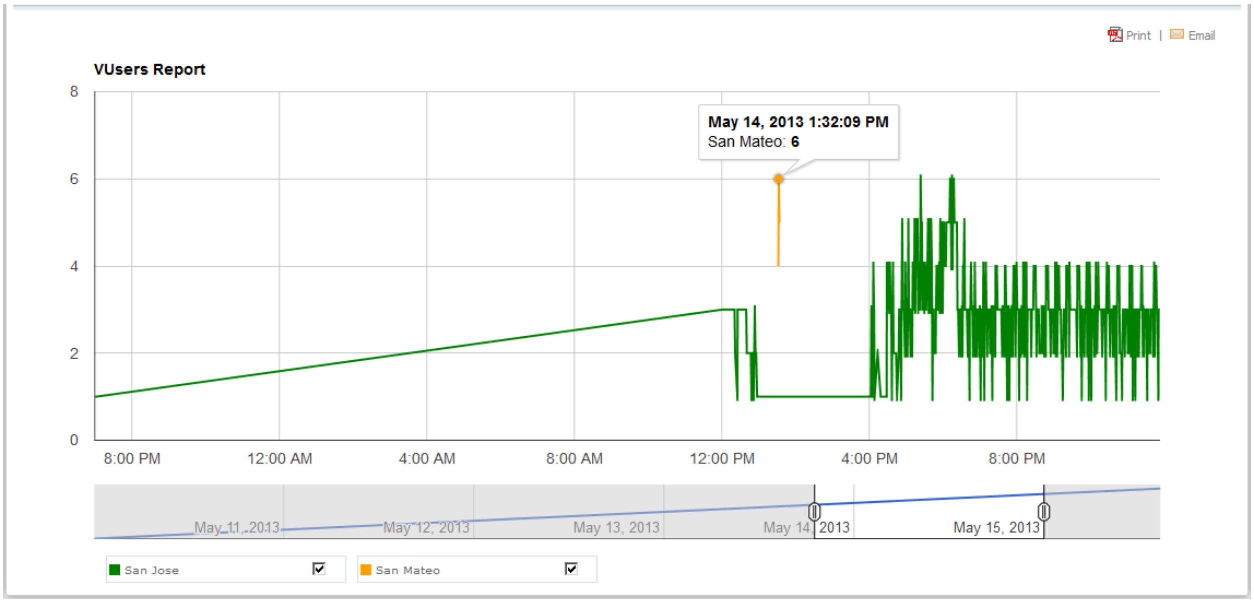
Custom Message

Finally, Enable Auto Refresh automatically refreshes the monitor/transaction summary pages or any chart you run with new data from ongoing runs. Pages are refreshed every 10 seconds by default.

1.4.1 Vuser Chart

The Vuser chart shows the number of Vuser licenses used at any minute in your system over a specified period of time. If you have 2 Vuser licenses, you might still be able to execute 4 monitors a minute using 2 licenses for 25 seconds at a time. The image below shows Vuser license usage for two LiveMonitor Server locations (in green and yellow). Hover over a point to see the associated number of Vuser licenses.

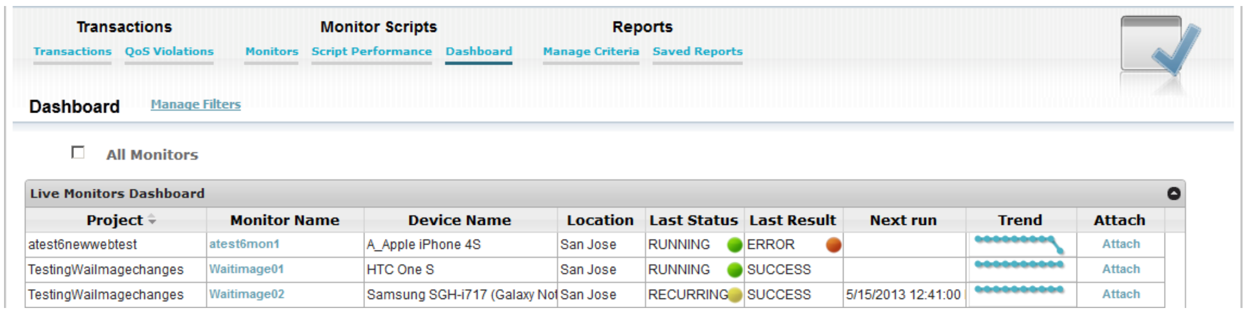
Figure 1-7 Vuser Chart



2 Dashboard

The dashboard can be accessed by clicking the **Monitoring Dashboard** link when you log in to the DeviceAnywhere Enterprise Monitoring Portal. This takes you to the **Dashboard** tab of the Monitor Scripts view.

Figure 2-1 Dashboard



Live Monitors Dashboard

Project	Monitor Name	Device Name	Location	Last Status	Last Result	Next run	Trend	Attach
atest6newwebtest	atest6mon1	A_Apple iPhone 4S	San Jose	RUNNING ●	ERROR ●			Attach
TestingWaiImagechanges	Waitimage01	HTC One S	San Jose	RUNNING ●	SUCCESS			Attach
TestingWaiImagechanges	Waitimage02	Samsung SGH-i717 (Galaxy Not	San Jose	RECURRING ●	SUCCESS	5/15/2013 12:41:00		Attach

Monitors in the dashboard are listed with the following information:

- DeviceAnywhere Studio **Project** that the monitor was created in
- **Monitor Name** with a link to open the monitor details report
- **Device Name** that the monitor is scheduled to run on
- **Location** of the LiveMonitor server that the script is being executed on
- Last Status—status as of most recent run
- Last Result—result of most recent run
- **Next run** (displayed only for monitors with **Recurring** status)
- Trend graphic showing a visual representation of the success or failure of the ten most recent runs
- Link to **Attach** and view a device screen as a monitor script is being executed on it

2.1 Monitor Status and Run Result

Each monitor is displayed in the dashboard with the status as of the most recent run. Statuses can be identified by colored icons. The table below describes monitor statuses and their icons:

Table 2-1 Monitor Status Descriptions

Status and Icon	Description
○ PENDING	Displayed when a monitor is enabled, before the first run in the monitor schedule.
● RUNNING	Displayed when a monitor script is currently being executed on the chosen device.
● RECURRING	Displayed between scheduled runs of a monitor. The next scheduled run time is also displayed.
● COMPLETE	Displayed when a monitor has completed all scheduled runs.

The result displayed in the dashboard indicates whether the most recent monitor run was a success or failure in terms of script completion and any errors encountered. Monitor run failures due to system errors are also noted. An icon identifies failed runs.

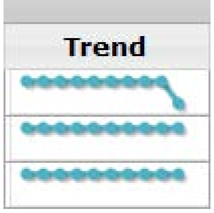
Table 2-2 Monitor Result Descriptions

Status and Icon	Description
SUCCESS (no icon)	Displayed when the most recent monitor run has been completed successfully. **NOTE** A successful monitor run does not necessarily imply that transactions contained in the monitor are also successful.
● FAIL	Displayed when the most recent monitor run is a failure because it encountered an error as defined in script logic. **NOTE** A monitor failure might still be within the tolerance levels set in the monitor policy and, therefore, does not necessarily generate an incident alert.
● ERROR	Displayed when the monitor fails for reasons other than script logic, e.g., when the monitor cannot run as scheduled because the device is being used by another monitor.

2.2 Trend Graphic

The blue trend graphic displayed for a monitor at the right is a visual representation of the success or failure of the last ten runs. A node at the top indicates success while a node at the bottom indicates failure. In the image below, the first graphic represents a monitor with nine successful runs and one failed run, the second a monitor with ten consecutive successful runs.

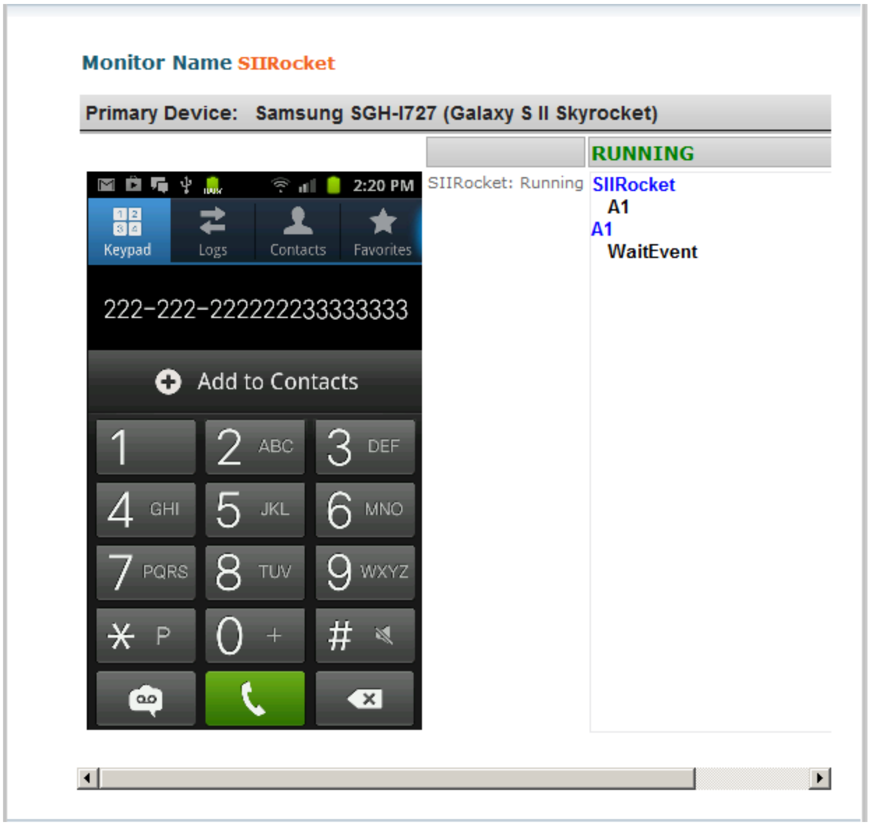
Figure 2-2 Trend Graphics



2.3 Viewing a Live Device

Click **Attach** next to a monitor to view the live device screen as the monitor script is being executed on it. The monitor must currently be running so you can view device screen updates and a log of script commands as they are being executed. The current monitor status is also displayed.

Figure 2-3 Viewing Monitor Execution Live



Monitor Name SIIRocket

Primary Device: Samsung SGH-I727 (Galaxy S II Skyrocket)

RUNNING

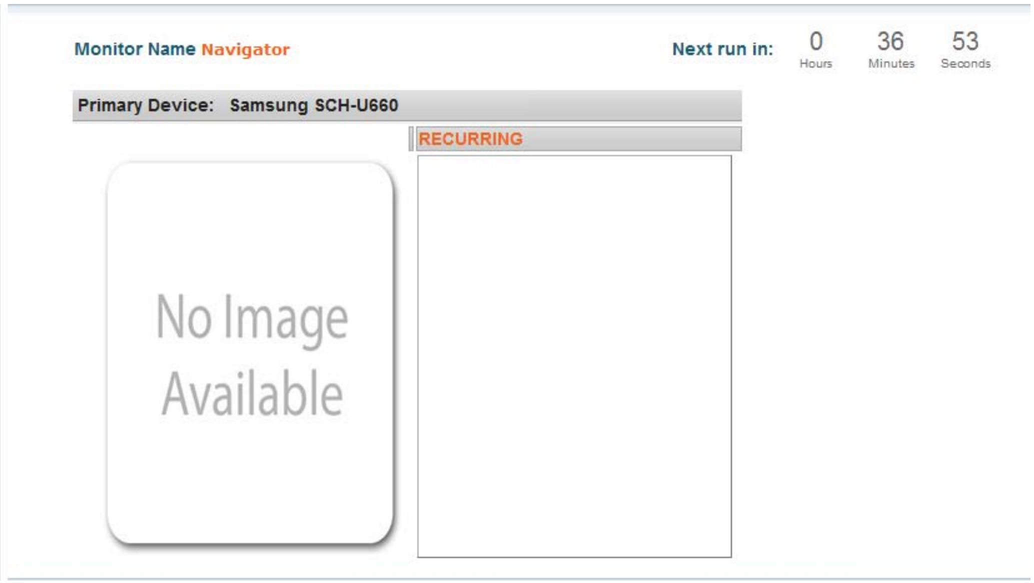
SIIRocket: Running

SIIRocket
  A1
A1
  WaitEvent

When the script is completed, the display changes from streaming video to an image of the last screen of script execution.

If you click **Attach** when the monitor is between scheduled runs, you will not see a device image. The current monitor status (e.g., Recurring) and wait time for the next run are displayed.

Figure 2-4 Viewing Device Screen between Script Runs



Monitor Name Navigator

Next run in: 0 Hours 36 Minutes 53 Seconds

Primary Device: Samsung SCH-U660

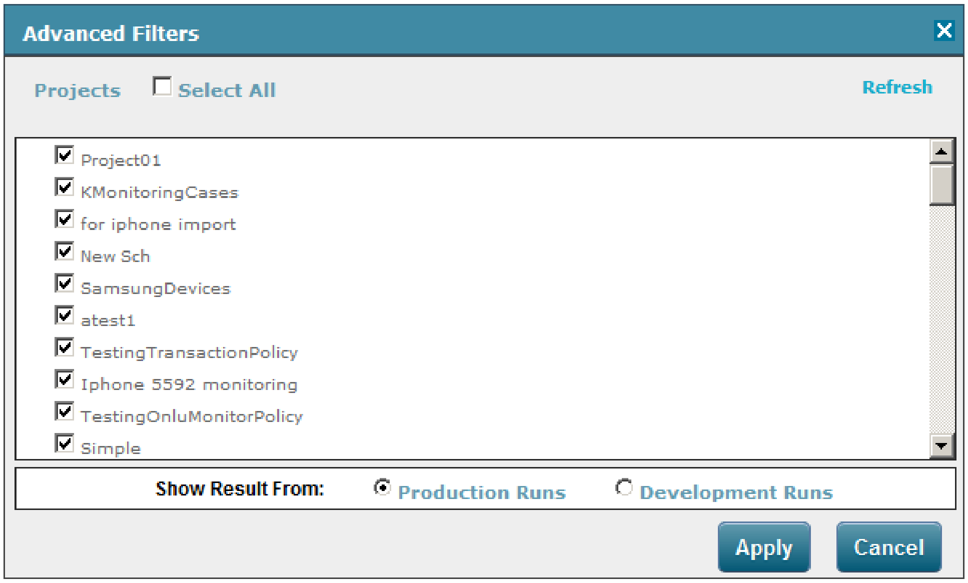
RECURRING

2.4 Sorting and Filtering the Dashboard

The dashboard can be sorted by any column header.

Click **Manage Filters** above the dashboard to filter monitors displayed. You can opt to view monitors contained in selected **Projects** and based on whether they are production or development runs.

Figure 2-5 Dashboard Filter



Projects ☐ Select All

☑ Project01
☑ KMonitoringCases
☑ for iphone import
☑ New Sch
☑ SamsungDevices
☑ atest1
☑ TestingTransactionPolicy
☑ Iphone 5592 monitoring
☑ TestingOnluMonitorPolicy
☑ Simple

Show Result From: ● Production Runs ○ Development Runs

Apply your filter criteria.

2.5 Using the Dashboard

The dashboard should be your first point of reference when you have just deployed/enabled your monitor. You will want to make sure that your monitor is listed in the dashboard and displays the correct status and start time.

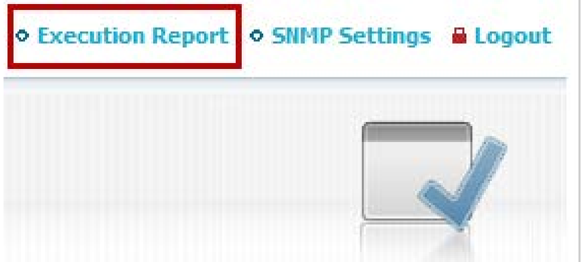
The dashboard icons and trend graphic also provide a quick reference for current and recent monitor results. For details, you should look at the monitor details report; check the execution report for a specific run.

Viewing the live device screen during monitor execution can also be a quick diagnostic tool to check on your monitor or service if any alerts are generated.

3 Execution Report

The execution report is the exhaustive list of all monitor runs in a DeviceAnywhere Enterprise Monitoring system. Click **Execution Report** at the top-right corner of the DAE Monitoring Portal (highlighted in the image below) to view the run list for the current day, which is the default date range.

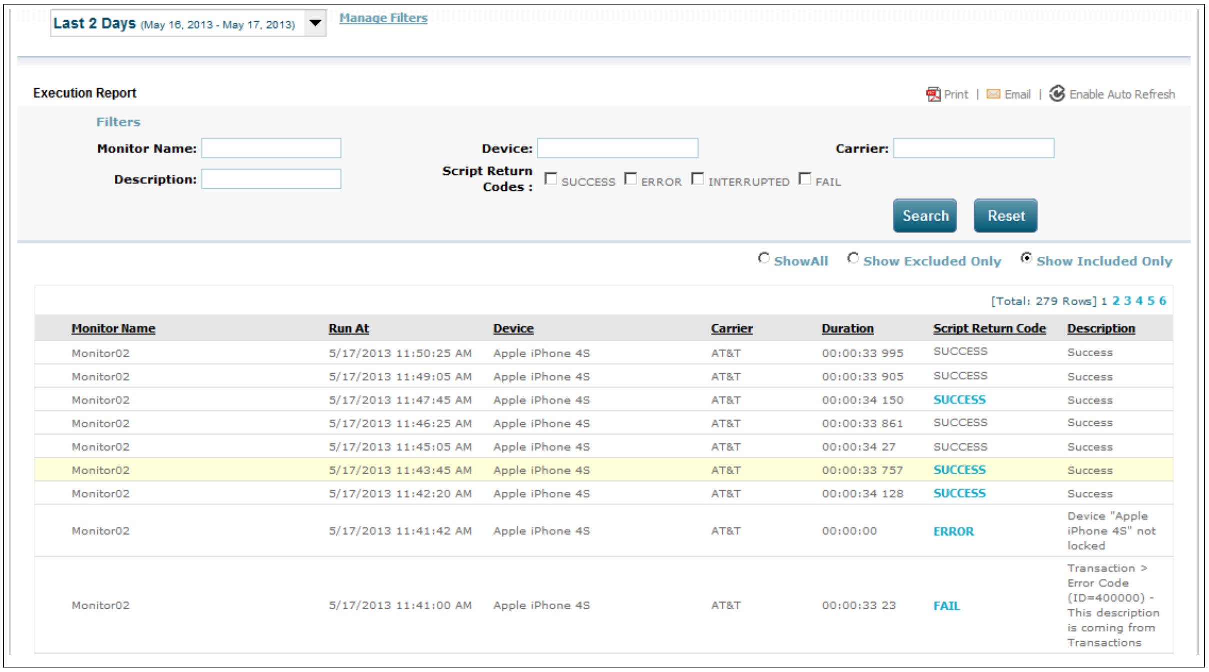
Figure 3-1 Accessing the Execution Report



Runs are displayed most recent first with information on:

- **Monitor Name**
- Time the run began (**Run At**)
- **Device**
- **Carrier**
- **Duration** of run
- Run result (**Script Return Code**)
- **Description** of run result—if an error is encountered, this displays the error description

Figure 3-2 Execution Report


Last 2 Days (May 16, 2013 - May 17, 2013)
Manage Filters
Execution Report
Print | Email | Enable Auto Refresh
Filters
Monitor Name:
Device:
Carrier:
Description:
Script Return Codes :
□ SUCCESS □ ERROR □ INTERRUPTED □ FAIL
Search
Reset
○ ShowAll ○ Show Excluded Only ● Show Included Only

[Total: 279 Rows] 1 2 3 4 5 6

Monitor Name	Run At	Device	Carrier	Duration	Script Return Code	Description
Monitor02	5/17/2013 11:50:25 AM	Apple iPhone 4S	AT&T	00:00:33 995	SUCCESS	Success
Monitor02	5/17/2013 11:49:05 AM	Apple iPhone 4S	AT&T	00:00:33 905	SUCCESS	Success
Monitor02	5/17/2013 11:47:45 AM	Apple iPhone 4S	AT&T	00:00:34 150	SUCCESS	Success
Monitor02	5/17/2013 11:46:25 AM	Apple iPhone 4S	AT&T	00:00:33 861	SUCCESS	Success
Monitor02	5/17/2013 11:45:05 AM	Apple iPhone 4S	AT&T	00:00:34 27	SUCCESS	Success
Monitor02	5/17/2013 11:43:45 AM	Apple iPhone 4S	AT&T	00:00:33 757	SUCCESS	Success
Monitor02	5/17/2013 11:42:20 AM	Apple iPhone 4S	AT&T	00:00:34 128	SUCCESS	Success
Monitor02	5/17/2013 11:41:42 AM	Apple iPhone 4S	AT&T	00:00:00	ERROR	Device "Apple iPhone 4S" not locked
Monitor02	5/17/2013 11:41:00 AM	Apple iPhone 4S	AT&T	00:00:33 23	FAIL	Transaction > Error Code (ID=400000) - This description is coming from Transactions

3.1 Links for Detailed Results

Runs for which detailed results are available are highlighted in the execution report. Check the **Script Return Code** column for a **Fail**, **Success**, or **Error** hyperlink.

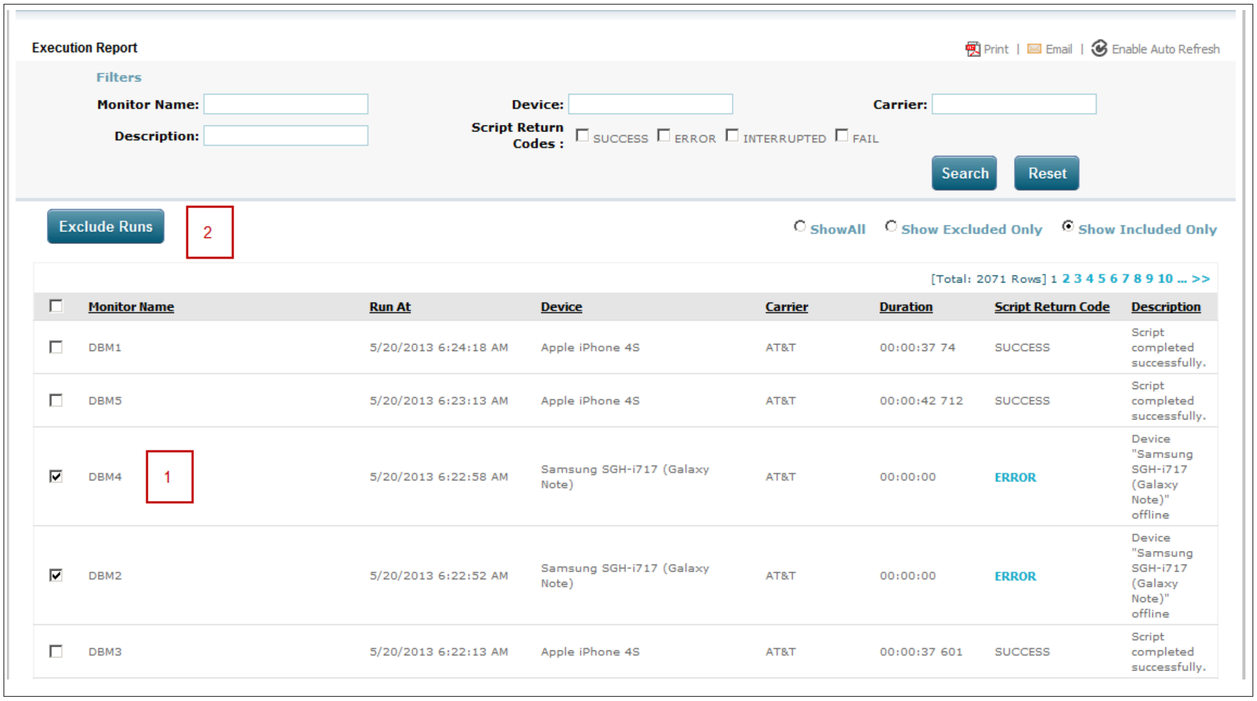
- **Fail** indicates a monitor run that failed because it encountered a customer-defined error. Failed runs always have links for detailed results.
- A hyperlinked **Success** result indicates a completed monitor run but one in which transactions failed or exceeded acceptable run times.
- **Error** indicates a script that was not completed due to system errors such as the device going offline. Runs with system errors always have links for detailed results.

See also Monitor Status and Run Result above for a discussion of run results. See Detailed Run Results for a description of command-by-command run results.

3.2 Excluding Runs

Users with the Account Admin role can exclude specific runs from the execution report—these excluded runs are not counted in any reports in the Portal. A check box appears next to each run in the execution report for users with the Account Admin role. To exclude a run, check the corresponding box and click **Exclude Runs**.

Figure 3-3 Excluding Runs from the Execution Report



□	Monitor Name	Run At	Device	Carrier	Duration	Script Return Code	Description
□	DBM1	5/20/2013 6:24:18 AM	Apple iPhone 4S	AT&T	00:00:37 74	SUCCESS	Script completed successfully.
□	DBM5	5/20/2013 6:23:13 AM	Apple iPhone 4S	AT&T	00:00:42 712	SUCCESS	Script completed successfully.
☑	DBM4	5/20/2013 6:22:58 AM	Samsung SGH-i717 (Galaxy Note)	AT&T	00:00:00	ERROR	Device "Samsung SGH-i717 (Galaxy Note)" offline
☑	DBM2	5/20/2013 6:22:52 AM	Samsung SGH-i717 (Galaxy Note)	AT&T	00:00:00	ERROR	Device "Samsung SGH-i717 (Galaxy Note)" offline
□	DBM3	5/20/2013 6:22:13 AM	Apple iPhone 4S	AT&T	00:00:37 601	SUCCESS	Script completed successfully.

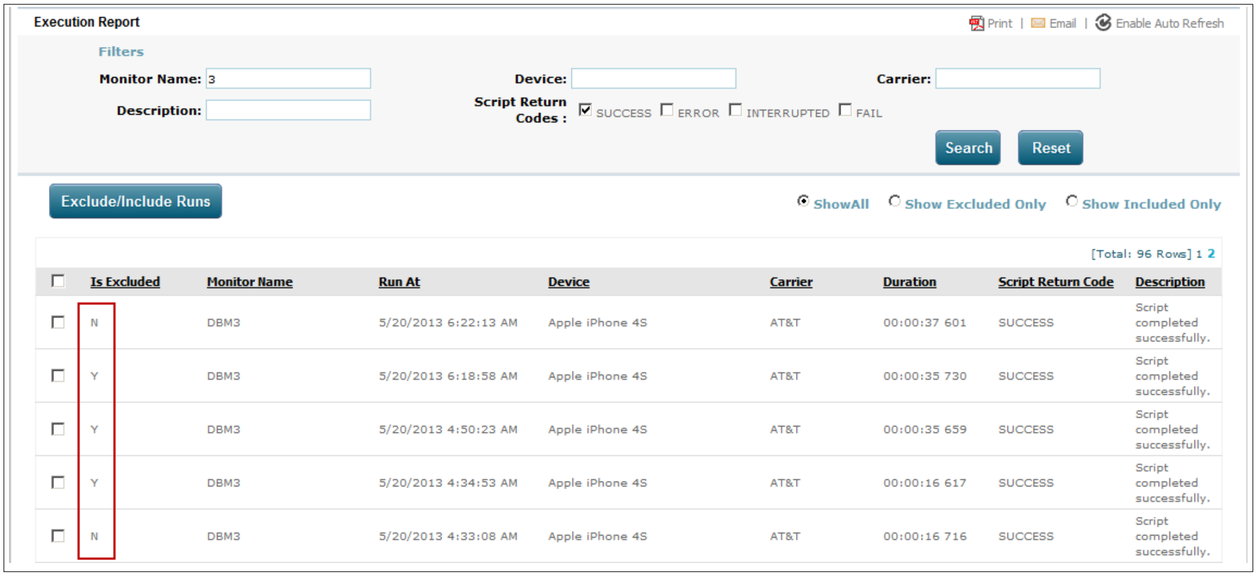
NOTE Other users do not have permission to select runs to be excluded. However, they can view a list of all, excluded, or included runs (see Sorting and Filtering the Execution Report below).

To include an excluded run, select the **Show All** radio button. Then check the box next to the excluded run and click **Exclude/Include Runs**.

Use the radio buttons above the execution list to the right to view runs excluded from the execution report by an account administrator. **Show Included Only** is selected by default; this option does not display excluded runs. Select **Show Excluded Only** to view excluded runs.

Select **Show All** to view both included and excluded runs. There is an indication next to each run in the **Is Excluded** column whether a run has been excluded by the administrator (**Y**) or not (**N**).

Figure 3-4 Viewing Excluded as Well as Included Runs in the Execution Report



Monitor Name: 3

Device:

Carrier:

Description:

Script Return Codes : ☑ SUCCESS □ ERROR □ INTERRUPTED □ FAIL

● ShowAll ○ Show Excluded Only ○ Show Included Only

[Total: 96 Rows] 1 2

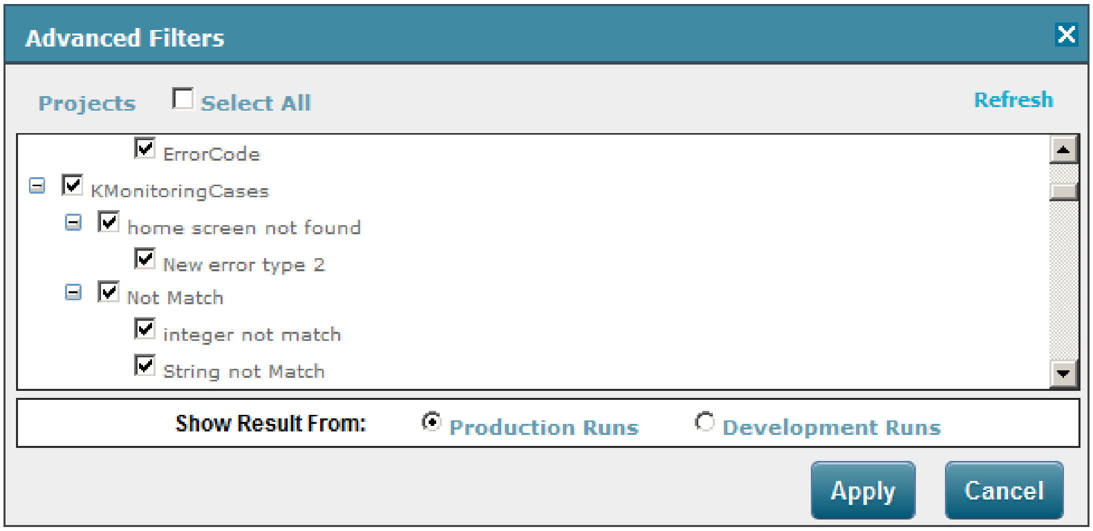
□	Is Excluded	Monitor Name	Run At	Device	Carrier	Duration	Script Return Code	Description
□	N	DBM3	5/20/2013 6:22:13 AM	Apple iPhone 4S	AT&T	00:00:37 601	SUCCESS	Script completed successfully.
□	Y	DBM3	5/20/2013 6:18:58 AM	Apple iPhone 4S	AT&T	00:00:35 730	SUCCESS	Script completed successfully.
□	Y	DBM3	5/20/2013 4:50:23 AM	Apple iPhone 4S	AT&T	00:00:35 659	SUCCESS	Script completed successfully.
□	Y	DBM3	5/20/2013 4:34:53 AM	Apple iPhone 4S	AT&T	00:00:16 617	SUCCESS	Script completed successfully.
□	N	DBM3	5/20/2013 4:33:08 AM	Apple iPhone 4S	AT&T	00:00:16 716	SUCCESS	Script completed successfully.

3.3 Sorting and Filtering the Execution Report

The execution report can be sorted by any column header.

Click **Manage Filters** near the date range to filter the execution report by increasingly granular criteria: projects, error categories within projects, and/or error types within error categories. If you deselect a project, any runs for monitors in that project are filtered out. Likewise, if you deselect an error category, any monitor runs that triggered errors in the category are filtered out.

Figure 3-5 Execution Report Filter Criteria



□ Select All

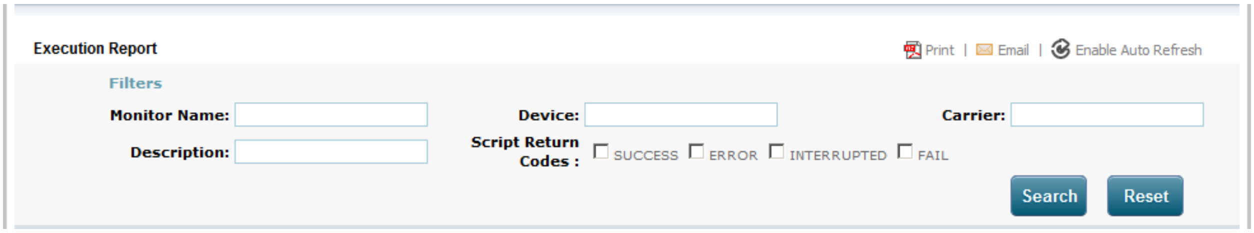
- ☑ ErrorCode
- ⊟ ☑ KMonitoringCases
  - ⊟ ☑ home screen not found
    - ☑ New error type 2
  - ⊟ ☑ Not Match
    - ☑ integer not match
    - ☑ String not Match

Show Result From: ● Production Runs ○ Development Runs

You can also filter by the name of any item in a column of the execution report. In the search area, enter a string in the field next to a column name, e.g., enter part of or a full **Monitor Name**. Click **Search**. (You can **Reset** search criteria at any time.)

You can also search by a string from the run **Description**, **Device**, or **Carrier** and filter runs by **Script Return Codes**. You can combine multiple filter criteria.

Figure 3-6 Filtering by an Item in a Column



3.4 Using the Execution Report

The execution report is a good place to track down a specific run, especially if the run did not contribute to an incident and therefore, cannot be found in an incident report. You can use the powerful filters in the execution report to find the run you are looking for, click the run result link to view detailed results, and then diagnose a failure.

4 Monitors

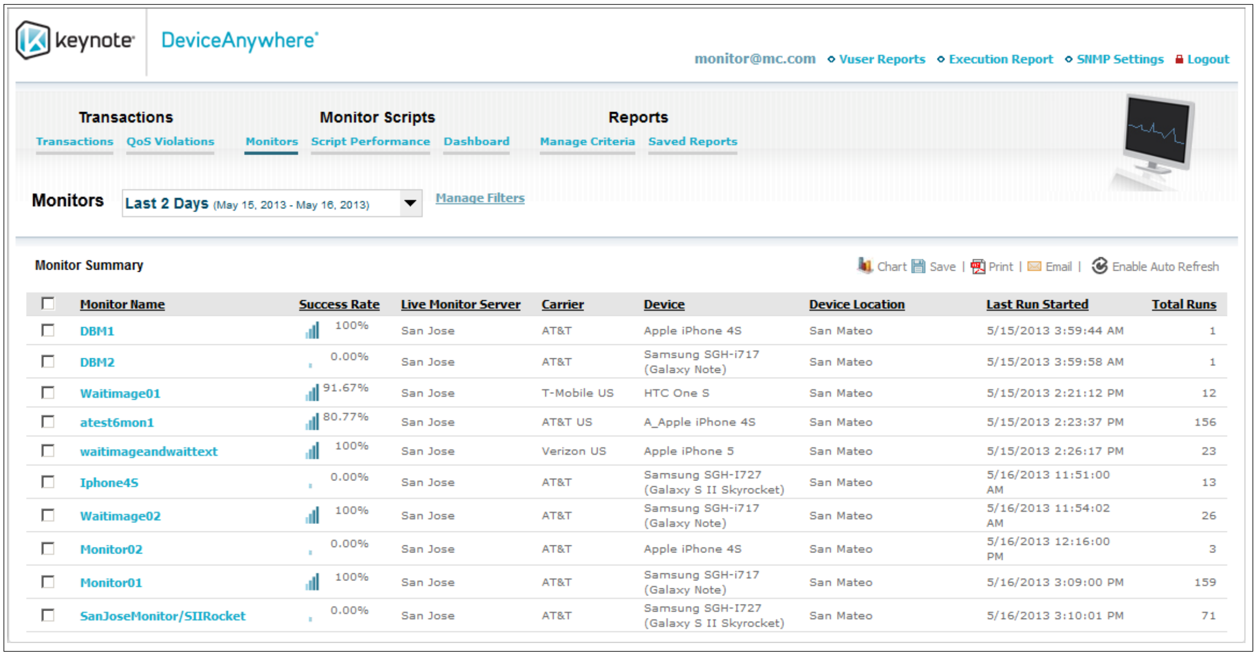
This chapter describes summary reports accessible from the Monitor Scripts view of the DeviceAnywhere Enterprise Monitoring Portal. The monitor summary is displayed in the **Monitors** tab and the list of monitor incidents in the **Script Performance** tab. The monitor details report is accessible from the monitor summary and by clicking the name of a monitor anywhere else in the TCE Monitoring Portal.

NOTE The monitor details report and monitor incident reports are covered in Detailed Reports. Charting monitors is covered in Charts. Saving monitor reports is covered in Saving Reports and Criteria.

4.1 Monitors Tab

The monitor summary displays the success rate and total number of runs for every monitor in your system over a specified date range. The date range defaults to the current day.

Figure 4-1 Monitor Summary



Monitors Last 2 Days (May 15, 2013 - May 16, 2013)

Monitor Summary

□	Monitor Name	Success Rate	Live Monitor Server	Carrier	Device	Device Location	Last Run Started	Total Runs
□	DBM1	100%	San Jose	AT&T	Apple iPhone 4S	San Mateo	5/15/2013 3:59:44 AM	1
□	DBM2	0.00%	San Jose	AT&T	Samsung SGH-i717 (Galaxy Note)	San Mateo	5/15/2013 3:59:58 AM	1
□	Waitimage01	91.67%	San Jose	T-Mobile US	HTC One S	San Mateo	5/15/2013 2:21:12 PM	12
□	atest6mon1	80.77%	San Jose	AT&T US	A_Apple iPhone 4S	San Mateo	5/15/2013 2:23:37 PM	156
□	waitimageandwaittext	100%	San Jose	Verizon US	Apple iPhone 5	San Mateo	5/15/2013 2:26:17 PM	23
□	Iphone4S	0.00%	San Jose	AT&T	Samsung SGH-I727 (Galaxy S II Skyrocket)	San Mateo	5/16/2013 11:51:00 AM	13
□	Waitimage02	100%	San Jose	AT&T	Samsung SGH-i717 (Galaxy Note)	San Mateo	5/16/2013 11:54:02 AM	26
□	Monitor02	0.00%	San Jose	AT&T	Apple iPhone 4S	San Mateo	5/16/2013 12:16:00 PM	3
□	Monitor01	100%	San Jose	AT&T	Samsung SGH-i717 (Galaxy Note)	San Mateo	5/16/2013 3:09:00 PM	159
□	SanJoseMonitor/SIIRocket	0.00%	San Jose	AT&T	Samsung SGH-I727 (Galaxy S II Skyrocket)	San Mateo	5/16/2013 3:10:01 PM	71

Monitors in the summary are listed with the following information:

- **Monitor Name** with a link to open the monitor details report
- **Success Rate**, calculated over the **Total Runs** in the time period selected
- **LiveMonitor Server**—location of the monitor server
- **Carrier**
- **Device**
- **Device Location**—location of the Ensemble Server to which device is connected
- **Last Run Started**—start time of the most recent run
- **Total Runs** over the date range selected

Click on a monitor name to view monitor details, including script and system errors encountered, transaction run times, and monitor incidents. From the monitor summary, you can select monitors to be displayed in a comparative chart of transaction times (monitor performance) or a visual representation of monitor success or failure (monitor availability) over a period of time. This is covered in detail in Charts.

You can also **Save** the report (as displayed once filters have been applied). Saved reports are available in the Reports view.

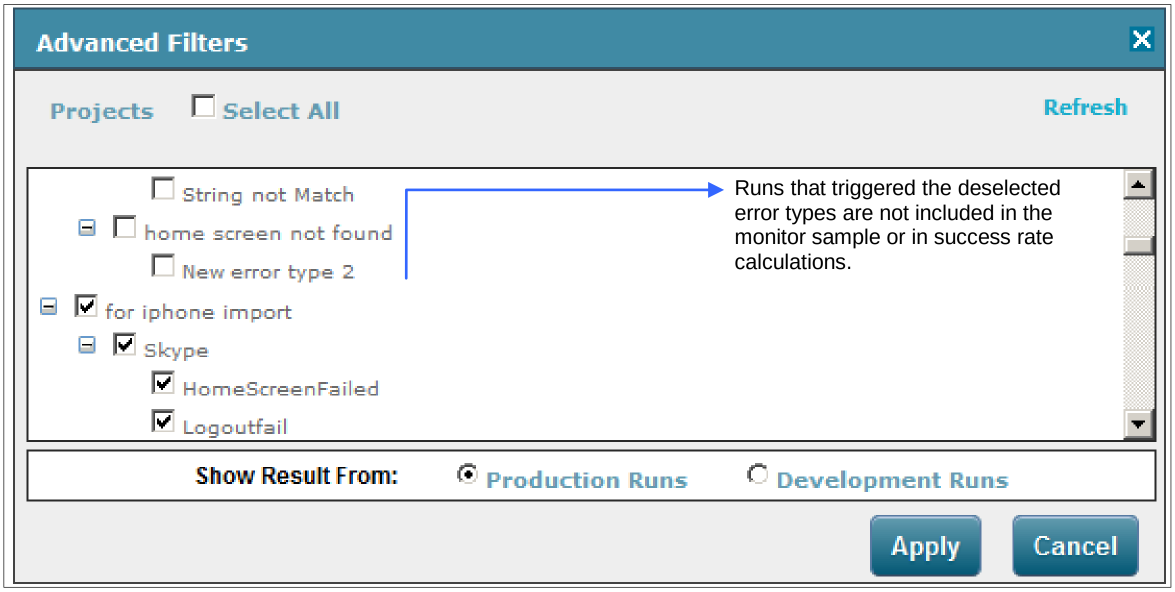
4.1.1 Sorting and Filtering the Monitor Summary

The monitor summary report can be sorted by any column header.

Click **Manage Filters** near the date range to filter the monitor report and recalculate the success rate. If you deselect a project, any monitors in that project are filtered out of the monitor summary.

If you deselect an error category, monitor runs that triggered errors from that category are filtered out. The monitor success rate is recalculated based on the remaining runs. The corresponding monitor details report also reflects the recalculated sample size and success rate of the monitor.

Figure 4-2 Filtering the Monitor Summary



Runs that triggered the deselected error types are not included in the monitor sample or in success rate calculations.

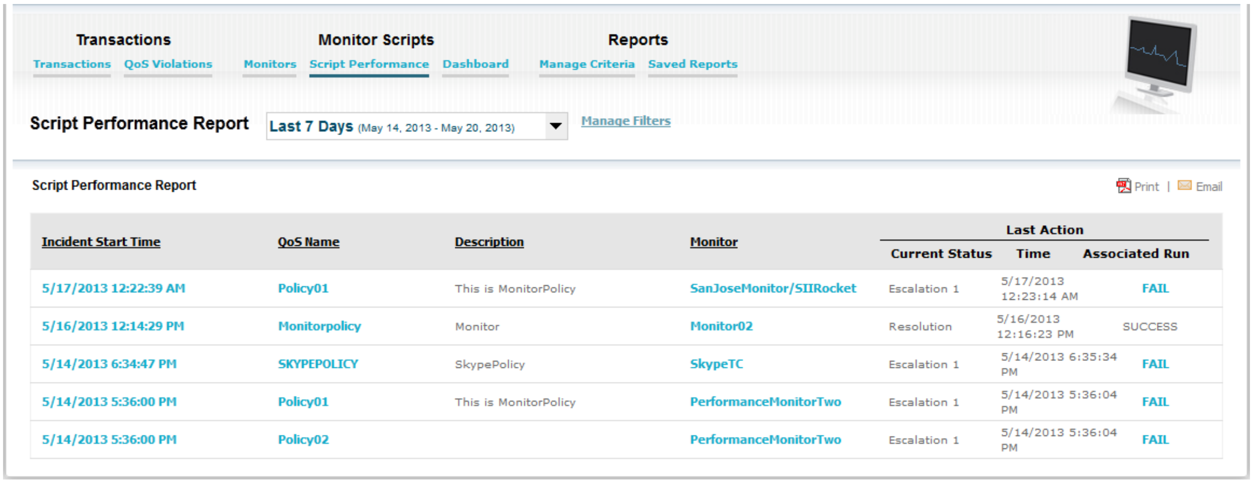
4.1.2 Using the Monitor Summary

Use the monitor summary report for a quick glimpse, aided by graphics, of the success rate of your monitors over a date range. You can quickly change the date range or error types triggered to see how the success rate varies. You can drill down to monitor details reports from this page.

4.2 Script Performance Tab

The *most recent incidents and their current status for each monitor policy-monitor combination* in your system are displayed in the **Script Performance** tab. Incidents are listed most recent first. The date range defaults to the current day.

Figure 4-3 Script Performance—Most Recent Monitor Incidents



Script Performance Report

Last 7 Days (May 14, 2013 - May 20, 2013)

Script Performance Report

Incident Start Time	QoS Name	Description	Monitor	Last Action		
				Current Status	Time	Associated Run
5/17/2013 12:22:39 AM	Policy01	This is MonitorPolicy	SanJoseMonitor/SIIRocket	Escalation 1	5/17/2013 12:23:14 AM	FAIL
5/16/2013 12:14:29 PM	Monitorpolicy	Monitor	Monitor02	Resolution	5/16/2013 12:16:23 PM	SUCCESS
5/14/2013 6:34:47 PM	SKYPEPOLICY	SkypePolicy	SkypeTC	Escalation 1	5/14/2013 6:35:34 PM	FAIL
5/14/2013 5:36:00 PM	Policy01	This is MonitorPolicy	PerformanceMonitorTwo	Escalation 1	5/14/2013 5:36:04 PM	FAIL
5/14/2013 5:36:00 PM	Policy02		PerformanceMonitorTwo	Escalation 1	5/14/2013 5:36:04 PM	FAIL

Monitor incidents are listed with the following information:

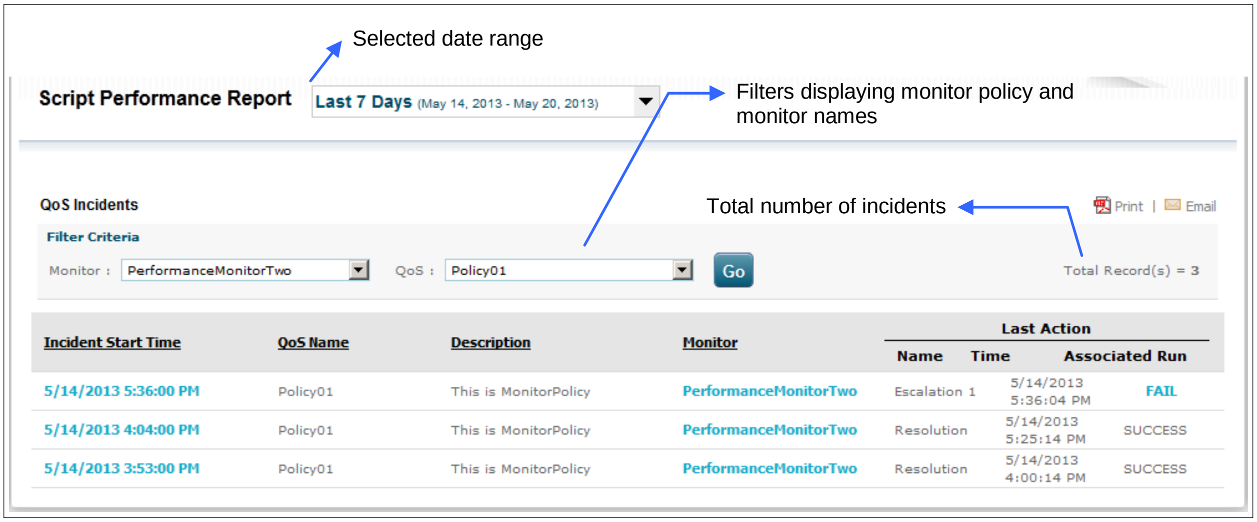
- **Incident Start Time**—start time of the run generating the first level 1 escalation
- **QoS Name**—name of monitor policy violated
- **Description** of the monitor policy violated
- **Monitor** name
- **Last Action**—time and current escalation/resolution status of the incident
  - **Current Status**—current escalation level or resolution status
  - **Time** of the run that triggered the current escalation or resolution alert
  - **Associated Run**—run result (link to view detailed results available for failed runs causing an escalation)

4.2.1 Links from the Script Performance Report

You can drill down from the script performance report to view several detailed reports:

- Click an **Incident Start Time** to view a detailed incident report. This is the most recent incident for the monitor policy-monitor combination in the entry.
- Click the **Monitor** name to view the monitor details report
- Click an available link for a run result, e.g., **FAIL** in the **Associated Run** column, to view detailed run results (available for failed runs causing an escalation).
- Click the **QoS Name** (monitor policy) to view a history of violations of the policy in the **Monitor** over your selected date range. You will see a list of incidents filtered by the policy and the monitor (see Figure 4-4 below).

Figure 4-4 History of Incidents for Monitor Policy-Monitor Combination



Selected date range

Script Performance Report Last 7 Days (May 14, 2013 - May 20, 2013)

Filters displaying monitor policy and monitor names

QoS Incidents

Total number of incidents

Filter Criteria

Monitor : PerformanceMonitorTwo QoS : Policy01 Go

Total Record(s) = 3

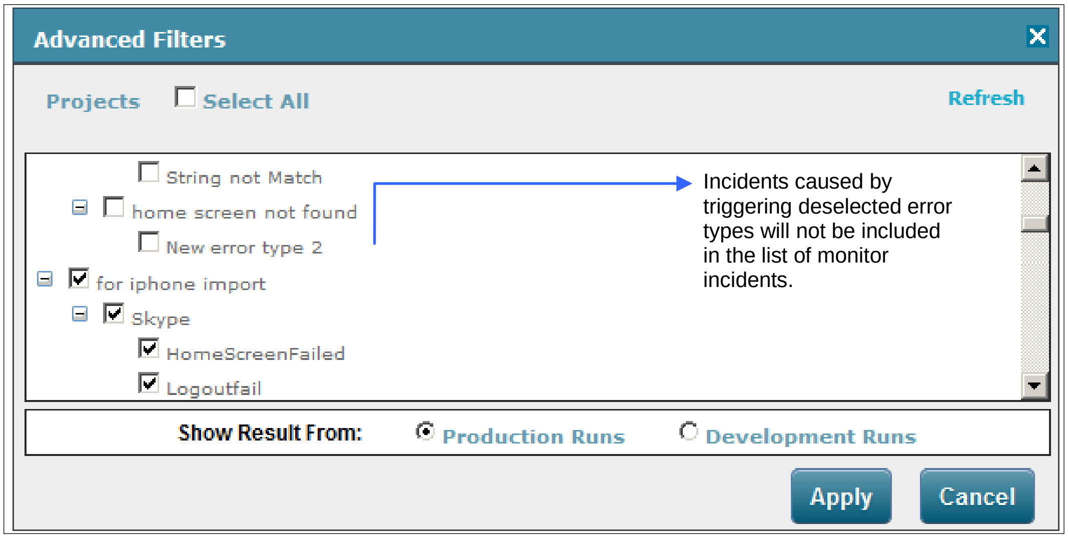
Incident Start Time	QoS Name	Description	Monitor	Last Action		
				Name	Time	Associated Run
5/14/2013 5:36:00 PM	Policy01	This is MonitorPolicy	PerformanceMonitorTwo	Escalation 1	5/14/2013 5:36:04 PM	FAIL
5/14/2013 4:04:00 PM	Policy01	This is MonitorPolicy	PerformanceMonitorTwo	Resolution	5/14/2013 5:25:14 PM	SUCCESS
5/14/2013 3:53:00 PM	Policy01	This is MonitorPolicy	PerformanceMonitorTwo	Resolution	5/14/2013 4:00:14 PM	SUCCESS

4.2.2 Sorting and Filtering the Script Performance Report

The script performance report can be sorted by incident start time, monitor policy name, policy description, or monitor name.

Click **Manage Filters** near the date range to filter the script performance report. As with the monitor summary, you can select/deselect projects, error categories, or error types as filter criteria. If you deselect a project, incidents for monitors in that project are filtered out. If you deselect an error category, incidents caused by triggering errors in that category are filtered out. If you deselect an error type, incidents caused by triggering that error type are filtered out.

Figure 4-5 Filtering the Script Performance Report



Advanced Filters

Projects □ Select All Refresh

- □ String not Match
- ⊟ □ home screen not found
  - □ New error type 2
- ⊟ ☑ for iphone import
  - ⊟ ☑ Skype
    - ☑ HomeScreenFailed
    - ☑ Logoutfail

Incidents caused by triggering deselected error types will not be included in the list of monitor incidents.

Show Result From: ● Production Runs ○ Development Runs

4.2.3 Using the Script Performance Report

The script performance report provides a summary of the current health of your monitors by displaying recent incidents. When you receive an alert for a monitor violation, the script performance report gives you a quick idea of the current status of the incident before you drill down to incident details.

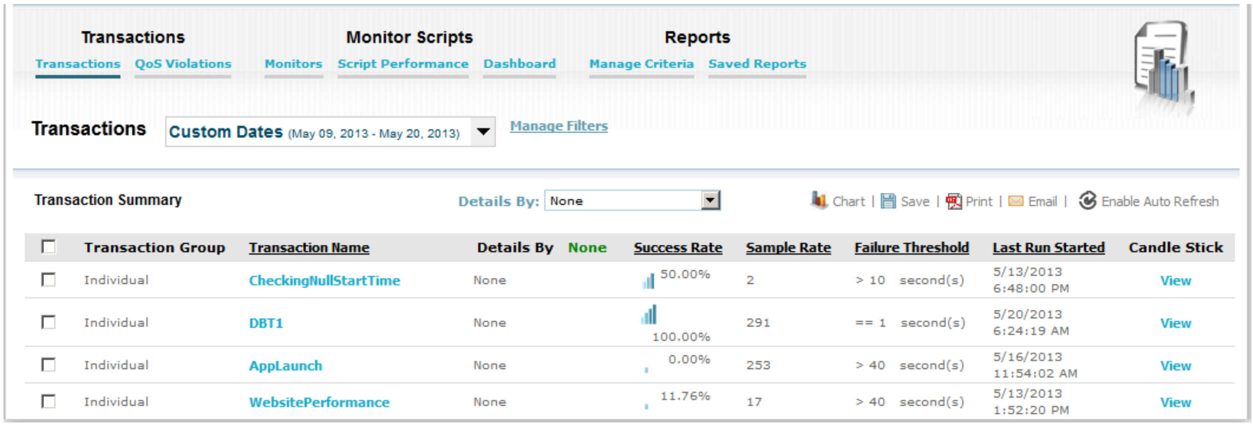
5 Transactions

This chapter describes the transaction summary report and the list of most recent transaction incidents accessible from the Transactions view of the DeviceAnywhere Enterprise Monitoring Portal. The transaction summary is displayed in the **Transactions** tab and the list of transaction incidents in the **QoS Violations** tab.

5.1 Transactions Tab

The transaction summary displays the success rate and total number of runs for every transaction in your system over a specified date range. The date range defaults to the current day.

Figure 5-1 Transaction Summary



Transactions Custom Dates (May 09, 2013 - May 20, 2013) Manage Filters

Transaction Summary Details By: None

Chart | Save | Print | Email | Enable Auto Refresh

□	Transaction Group	Transaction Name	Details By None	Success Rate	Sample Rate	Failure Threshold	Last Run Started	Candle Stick
□	Individual	CheckingNullStartTime	None	50.00%	2	> 10 second(s)	5/13/2013 6:48:00 PM	View
□	Individual	DBT1	None	100.00%	291	== 1 second(s)	5/20/2013 6:24:19 AM	View
□	Individual	AppLaunch	None	0.00%	253	> 40 second(s)	5/16/2013 11:54:02 AM	View
□	Individual	WebsitePerformance	None	11.76%	17	> 40 second(s)	5/13/2013 1:52:20 PM	View

Transactions in the summary are listed with the following information:

- **Transaction Group**, if any (Ungrouped transactions are listed as Individual.)
- **Transaction Name**
- **Details By**—lists the criterion by which transaction information is split out and displayed—see Transaction Summary Display Controls.
- **Success Rate**, calculated over the **Sample Size** in the time period selected
- **Sample Size**—number of transaction runs over the date range selected
- **Failure Threshold** of the transaction—e.g., a failure threshold of > 30 means that transaction run times greater than 30 seconds are considered failures.

  NOTE Besides violating the expected run time, transactions can also fail because they are not completed as expected, e.g., in a script branch in which the Toggle Transaction command is set to **Fail** to indicate failure.

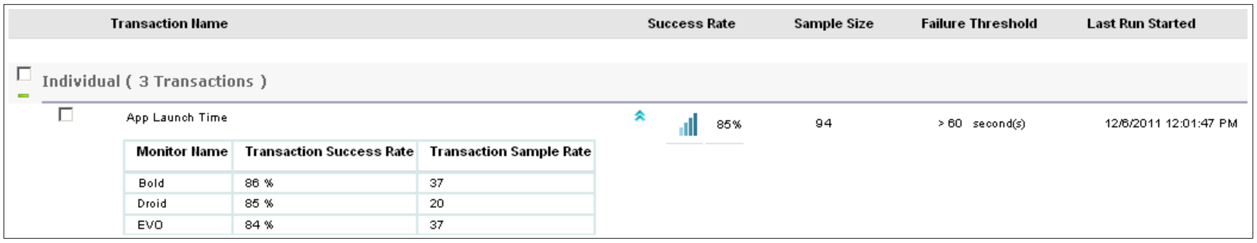
- Time the most recent run began (**Last Run Started**)
- **Candlestick** – Click **View** to generate a candlestick graph.

Transactions have as many entries in the transaction summary as the failure thresholds they have been associated with. For example, if you have changed the failure threshold of a transaction once, it will have two entries in the transaction summary, one for run evaluations against each threshold.

Transactions in groups are listed under the group name (see “test12 txngrp1” in the image above).

Click the expand button next to a success rate graphic to view transaction details.

Figure 5-2 Transaction Details



Transaction Name	Success Rate	Sample Size	Failure Threshold	Last Run Started
□ Individual (3 Transactions)				
□ App Launch Time	85%	94	> 60 second(s)	12/6/2011 12:01:47 PM

Monitor Name	Transaction Success Rate	Transaction Sample Rate
Bold	86 %	37
Droid	85 %	20
EVO	84 %	37

A table displays the success rate and number of transaction runs by each monitor it is used in.

You can select transactions to be displayed in a comparative chart of transaction times (transaction performance) or a visual representation of transaction success or failure (transaction availability) over a period of time. This is covered in detail in Charts.

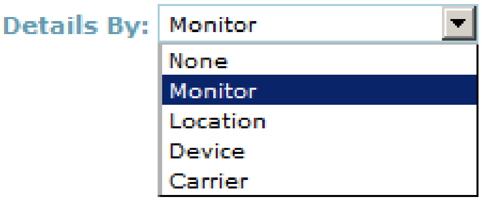
You can save transaction charts or the summary report (as displayed once filters have been applied). Saved reports are available in the Reports view.

5.1.1 Transaction Summary Display Controls

Transaction information can be split out and displayed by various criteria. For example, if you have used a transaction in multiple monitors, you can display a separate entry for each monitor in the transaction summary.

Select a criterion from the **Details By** drop-down list above the transaction summary. You can display separate entries for a transaction by **Monitor**, **Location**, **Device**, or **Carrier**.

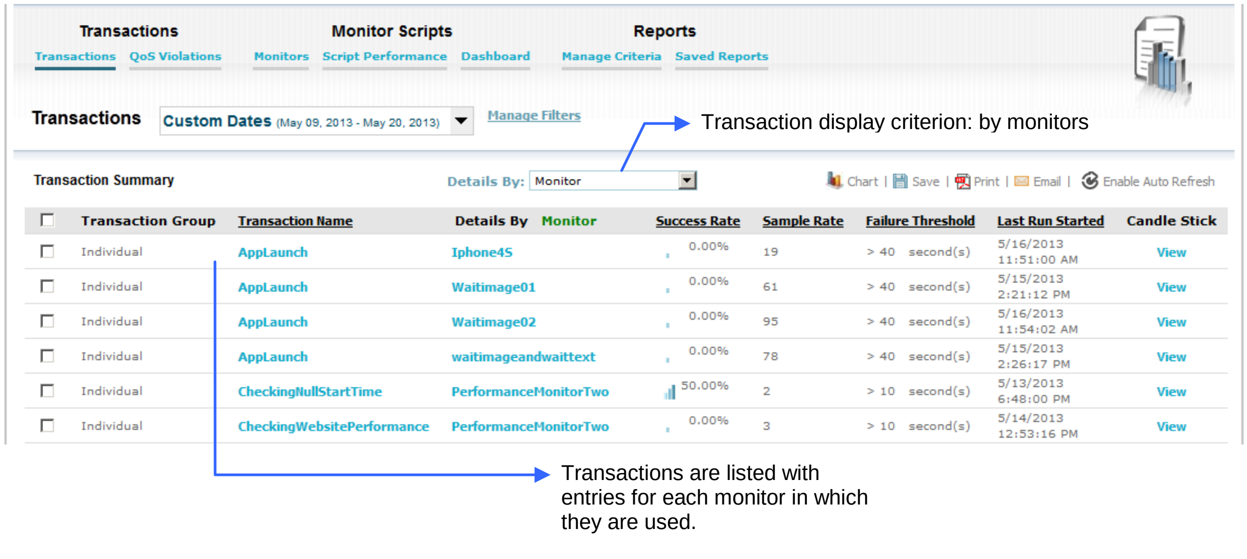
Figure 5-3 Controls to View Transaction Summary



Details By: Monitor

Where available, a transaction is listed with separate entries for the chosen criterion.

Figure 5-4 Viewing Transaction Summary by a Criterion



Transactions: Custom Dates (May 09, 2013 - May 20, 2013)

Transaction display criterion: by monitors

Transaction Summary

Details By: Monitor

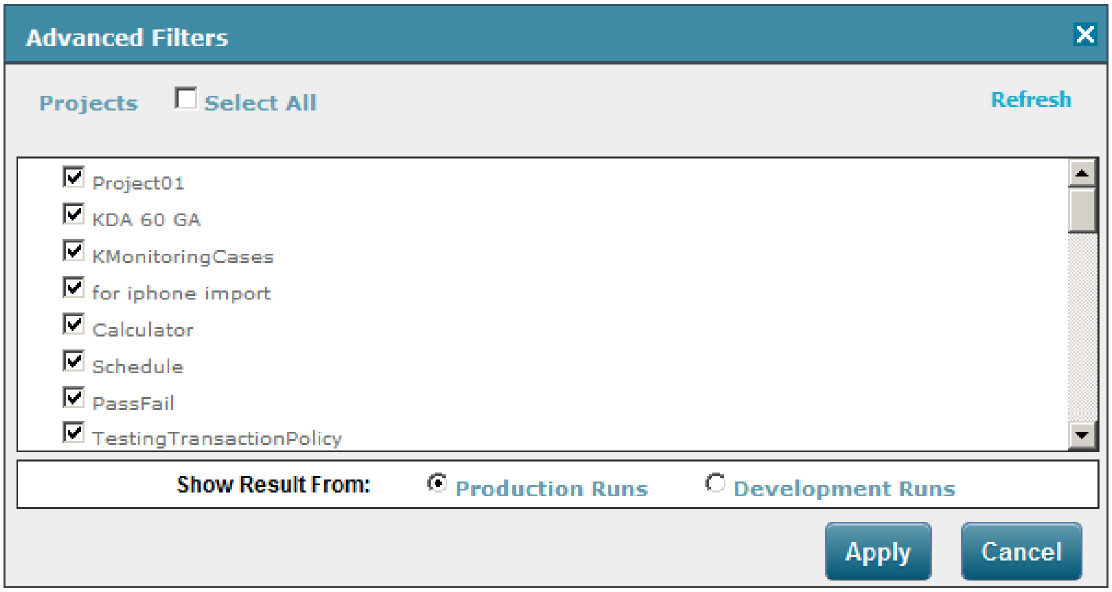
□	Transaction Group	Transaction Name	Details By Monitor	Success Rate	Sample Rate	Failure Threshold	Last Run Started	Candle Stick
□	Individual	AppLaunch	Iphone4S	0.00%	19	> 40 second(s)	5/16/2013 11:51:00 AM	View
□	Individual	AppLaunch	Waitimage01	0.00%	61	> 40 second(s)	5/15/2013 2:21:12 PM	View
□	Individual	AppLaunch	Waitimage02	0.00%	95	> 40 second(s)	5/16/2013 11:54:02 AM	View
□	Individual	AppLaunch	waitimageandwaittext	0.00%	78	> 40 second(s)	5/15/2013 2:26:17 PM	View
□	Individual	CheckingNullStartTime	PerformanceMonitorTwo	50.00%	2	> 10 second(s)	5/13/2013 6:48:00 PM	View
□	Individual	CheckingWebsitePerformance	PerformanceMonitorTwo	0.00%	3	> 10 second(s)	5/14/2013 12:53:16 PM	View

Transactions are listed with entries for each monitor in which they are used.

The transaction summary can be sorted by transaction name, success rate, sample size, failure threshold, and start time of most recent run.

Besides choosing a date range for which to view transaction runs, you can also filter the transaction summary by project.

Figure 5-5 Transaction Summary Filter



□ Select All

☑ Project01
☑ KDA 60 GA
☑ KMonitoringCases
☑ for iphone import
☑ Calculator
☑ Schedule
☑ PassFail
☑ TestingTransactionPolicy

Show Result From: ● Production Runs ○ Development Runs

If you deselect a project, transactions used in monitor scripts in that project are not displayed.

5.1.2 Using the Transaction Summary

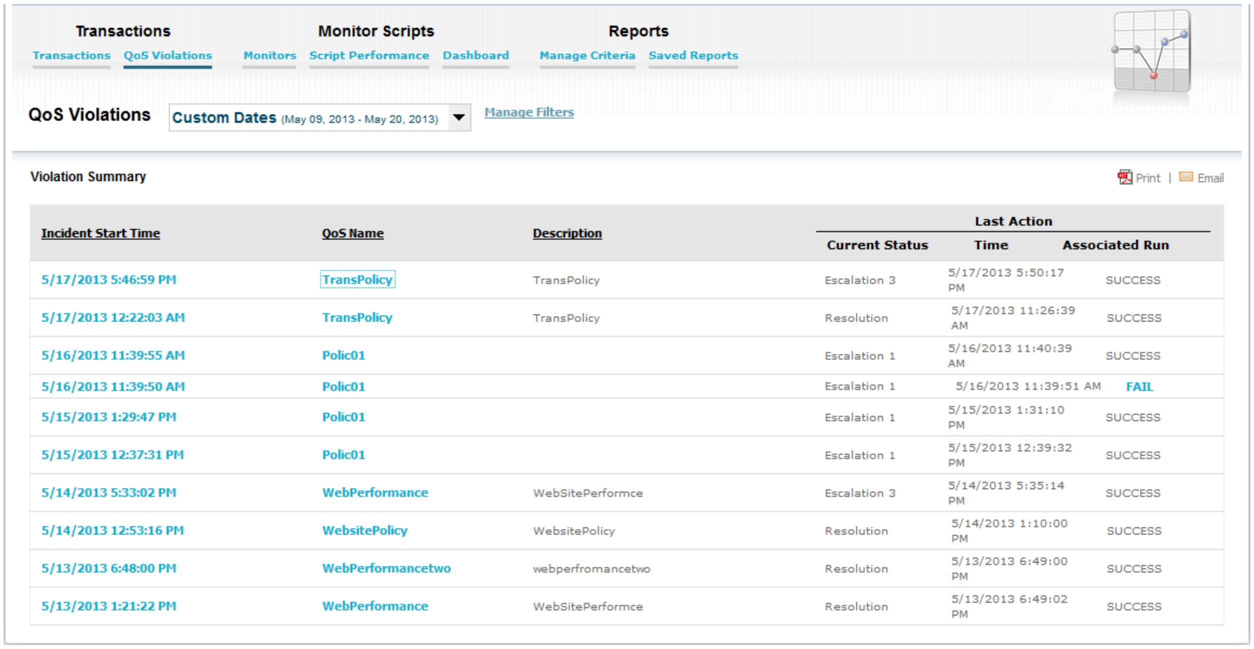
Use the transaction summary report for a quick glimpse, aided by graphics, of the success rate of your transactions over a date range. You can quickly change the date range to see how the success rate varies.

5.2 QoS Violations Tab

The *most recent incidents and their current status for each transaction policy-monitor combination* in your system are displayed in the **QoS Violations** tab. So if there are transaction incidents pertaining to the same policy in two separate monitors, there will be two entries in this report.

Incidents are listed most recent first. The date range defaults to the current day.

Figure 5-6 QoS Violations—Most Recent Transaction Incidents



Violation Summary

Incident Start Time	QoS Name	Description	Last Action		
			Current Status	Time	Associated Run
5/17/2013 5:46:59 PM	TransPolicy	TransPolicy	Escalation 3	5/17/2013 5:50:17 PM	SUCCESS
5/17/2013 12:22:03 AM	TransPolicy	TransPolicy	Resolution	5/17/2013 11:26:39 AM	SUCCESS
5/16/2013 11:39:55 AM	Polic01		Escalation 1	5/16/2013 11:40:39 AM	SUCCESS
5/16/2013 11:39:50 AM	Polic01		Escalation 1	5/16/2013 11:39:51 AM	FAIL
5/15/2013 1:29:47 PM	Polic01		Escalation 1	5/15/2013 1:31:10 PM	SUCCESS
5/15/2013 12:37:31 PM	Polic01		Escalation 1	5/15/2013 12:39:32 PM	SUCCESS
5/14/2013 5:33:02 PM	WebPerformance	WebSitePerformce	Escalation 3	5/14/2013 5:35:14 PM	SUCCESS
5/14/2013 12:53:16 PM	WebsitePolicy	WebsitePolicy	Resolution	5/14/2013 1:10:00 PM	SUCCESS
5/13/2013 6:48:00 PM	WebPerformancetwo	webperfromancetwo	Resolution	5/13/2013 6:49:00 PM	SUCCESS
5/13/2013 1:21:22 PM	WebPerformance	WebSitePerformce	Resolution	5/13/2013 6:49:02 PM	SUCCESS

Transaction incidents are listed with the following information:

- **Incident Start Time**—start time of the run that triggered the first incident alert
- **QoS Name**—name of transaction policy violated
- **Description** of the transaction policy violated
- **Last Action**—time and current escalation/resolution status of the incident
  - **Current Status**—current escalation level or resolution status
  - **Time** of the run that triggered the current escalation or resolution alert
  - **Associated Run**—run result (link to view detailed results available for failed runs causing an escalation)

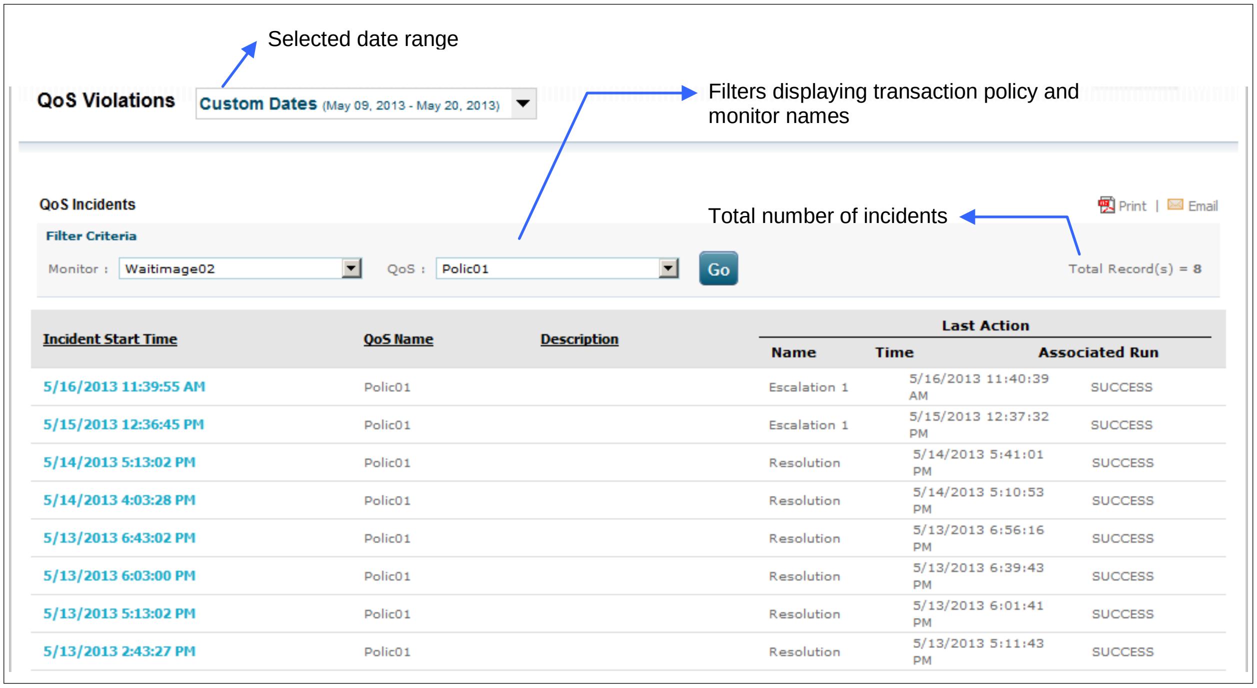
5.2.1 Links from the QoS Violations Report

You can drill down from the transaction incidents report to view several detailed reports:

- Click an **Incident Start Time** to view a detailed incident report. This is the most recent incident for the transaction policy-monitor combination in the entry.
- Click an available link for a run result, e.g., **FAIL** in the **Associated Run** column, to view detailed run results (available for failed runs causing an escalation).

- Click the **QoS Name** (transaction policy) to view a history of violations of the policy in the monitor over your selected date range. You will see a list of incidents filtered by the policy and monitor name (see Figure 5-7 below).

Figure 5-7 History of Incidents for Transaction Policy-Monitor Combination



Selected date range

Filters displaying transaction policy and monitor names

Total number of incidents

QoS Violations

Custom Dates (May 09, 2013 - May 20, 2013)

QoS Incidents

Print | Email

Filter Criteria

Monitor : Waitimage02 QoS : Polic01 Go

Total Record(s) = 8

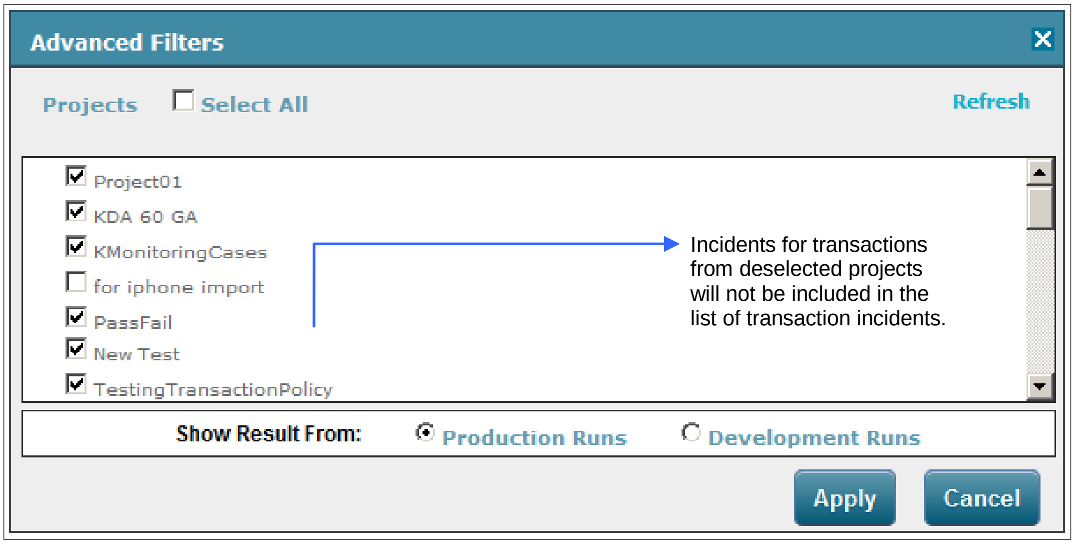
Incident Start Time	QoS Name	Description	Last Action		
			Name	Time	Associated Run
5/16/2013 11:39:55 AM	Polic01		Escalation 1	5/16/2013 11:40:39 AM	SUCCESS
5/15/2013 12:36:45 PM	Polic01		Escalation 1	5/15/2013 12:37:32 PM	SUCCESS
5/14/2013 5:13:02 PM	Polic01		Resolution	5/14/2013 5:41:01 PM	SUCCESS
5/14/2013 4:03:28 PM	Polic01		Resolution	5/14/2013 5:10:53 PM	SUCCESS
5/13/2013 6:43:02 PM	Polic01		Resolution	5/13/2013 6:56:16 PM	SUCCESS
5/13/2013 6:03:00 PM	Polic01		Resolution	5/13/2013 6:39:43 PM	SUCCESS
5/13/2013 5:13:02 PM	Polic01		Resolution	5/13/2013 6:01:41 PM	SUCCESS
5/13/2013 2:43:27 PM	Polic01		Resolution	5/13/2013 5:11:43 PM	SUCCESS

5.2.2 Sorting and Filtering the QoS Violations Report

The QoS violations report can be sorted by incident start time, transaction policy name, or policy description.

Click **Manage Filters** near the date range to filter the QoS violations report by project. If you deselect a project, incidents for transactions in that project are not displayed.

Figure 5-8 Filtering the QoS Violations Report



□ Select All

☑ Project01
☑ KDA 60 GA
☑ KMonitoringCases
□ for iphone import
☑ PassFail
☑ New Test
☑ TestingTransactionPolicy

Show Result From: ● Production Runs ○ Development Runs

Incidents for transactions from deselected projects will not be included in the list of transaction incidents.

5.2.3 Using the QoS Violations Report

The QoS violations report provides a summary of the current health of your transactions by displaying recent incidents. When you receive an alert for a transaction violation, the QoS violations report gives you a quick idea of the current status of the incident before you drill down to incident details.

6 Detailed Reports

This chapter discusses the following detailed reports that can be accessed from various points in the DeviceAnywhere Enterprise Monitoring Portal:

- Monitor details report
- Transaction details report
- Incident report for transaction or monitor policy violations
- Detailed run results

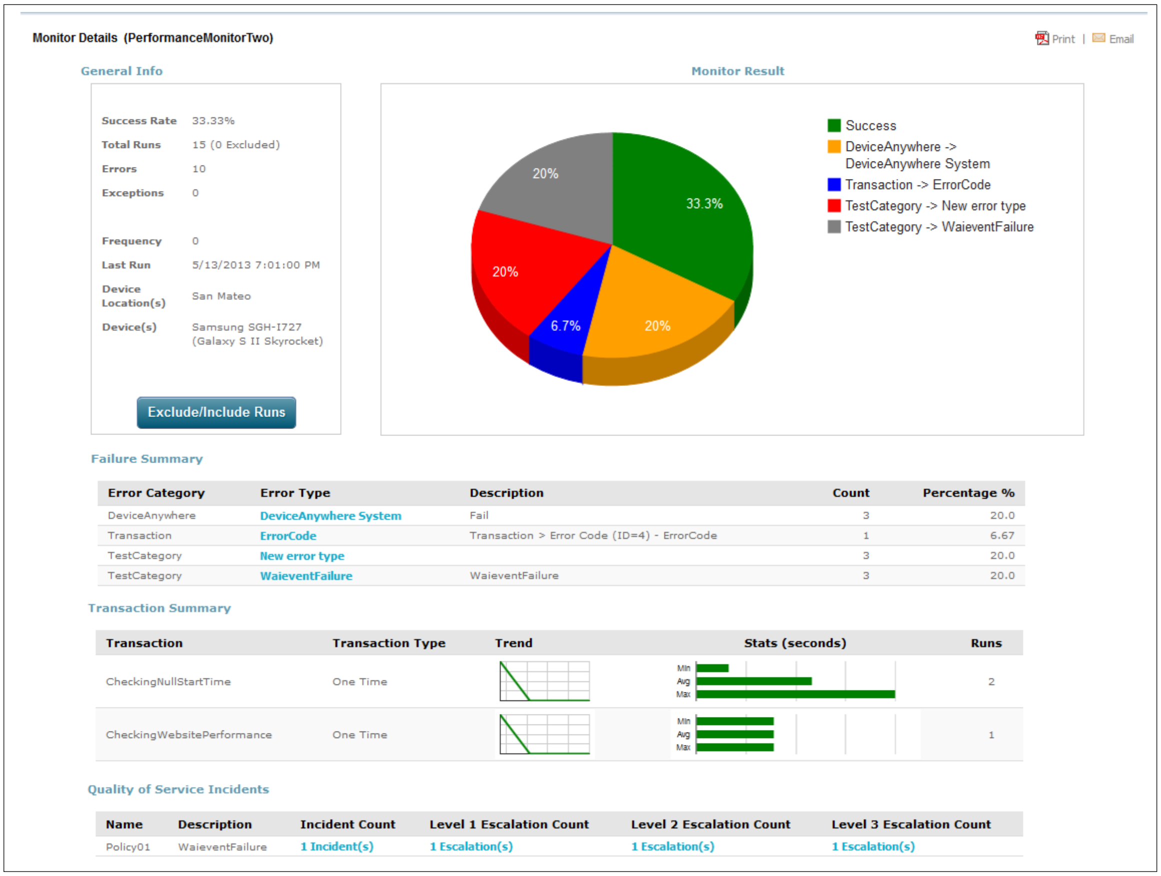
6.1 Monitor Details Report

Click on a monitor name anywhere in the DAE Monitoring Portal, most easily in the dashboard or monitor summary, to view monitor details. The monitor details report displays the success rate and rate of errors in a pie chart. You can use filters to recalculate the success rate by changing the date range, filtering out failed runs for an error type, or by excluding failed runs (requires permission).

The monitor details report also contains details of errors triggered with links to view results for failed runs, transaction times, and a list of monitor incidents with links to view incident reports.

Each section of the report is discussed in detail below.

Figure 6-1 Monitor Details


Print | Email
Monitor Result
20%
33.3%
20%
6.7%
20%
🟩 Success
🟧 DeviceAnywhere -> DeviceAnywhere System
🟦 Transaction -> ErrorCode
🟥 TestCategory -> New error type
⬛ TestCategory -> WaieventFailure
Exclude/Include Runs
Min
Avg
Max
Min
Avg
Max

Monitor Details (PerformanceMonitorTwo)

General Info

Success Rate	33.33%
Total Runs	15 (0 Excluded)
Errors	10
Exceptions	0
Frequency	0
Last Run	5/13/2013 7:01:00 PM
Device Location(s)	San Mateo
Device(s)	Samsung SGH-I727 (Galaxy S II Skyrocket)

Failure Summary

Error Category	Error Type	Description	Count	Percentage %
DeviceAnywhere	DeviceAnywhere System	Fail	3	20.0
Transaction	ErrorCode	Transaction > Error Code (ID=4) - ErrorCode	1	6.67
TestCategory	New error type		3	20.0
TestCategory	WaieventFailure	WaieventFailure	3	20.0

Transaction Summary

Transaction	Transaction Type	Trend	Stats (seconds)	Runs
CheckingNullStartTime	One Time			2
CheckingWebsitePerformance	One Time			1

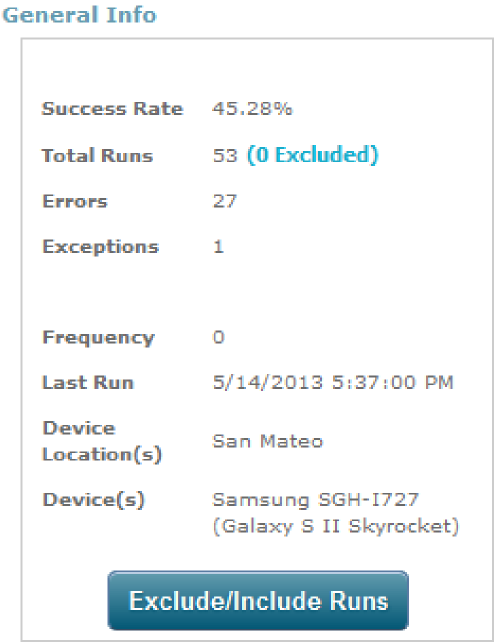
Quality of Service Incidents

Name	Description	Incident Count	Level 1 Escalation Count	Level 2 Escalation Count	Level 3 Escalation Count
Policy01	WaieventFailure	1 Incident(s)	1 Escalation(s)	1 Escalation(s)	1 Escalation(s)

6.1.1 General Info

This section displays statistics on the total number of runs, failed runs, and success rate for a selected date range. The statistics are recalculated when you use filters to change the date range or exclude runs from analysis.

Figure 6-2 Monitor Statistics



General Info

Success Rate	45.28%
Total Runs	53 (0 Excluded)
Errors	27
Exceptions	1
Frequency	0
Last Run	5/14/2013 5:37:00 PM
Device Location(s)	San Mateo
Device(s)	Samsung SGH-I727 (Galaxy S II Skyrocket)

The summary number of **Errors** equals the total number of errors reported in the Failure Summary.

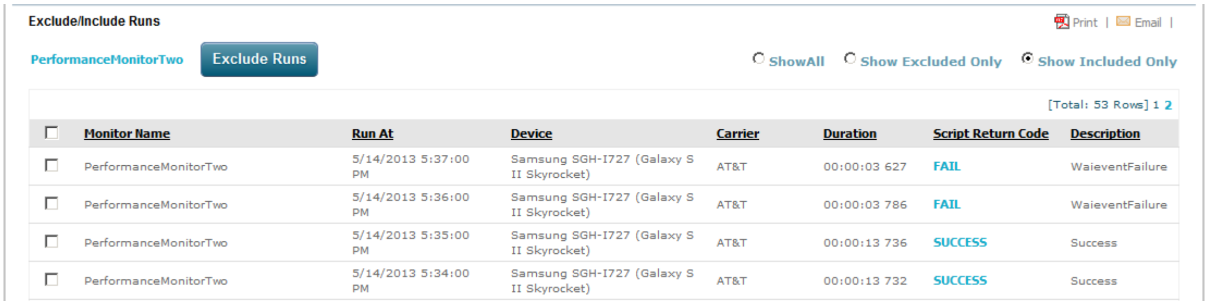
6.1.2 Filtering the Monitor Details Report

You can filter the monitor details report and recalculate error and success rates by changing the date range for which monitor runs are analyzed, or by excluding specific runs from the analysis. Changing the time frame is discussed in Standard Operations in the Portal.

Users with the Account Admin role can exclude runs:

1 Click **Exclude/Include Runs** in the General Info section of the monitor details report.

A list of all monitor runs for the given date range is displayed.



Exclude/Include Runs

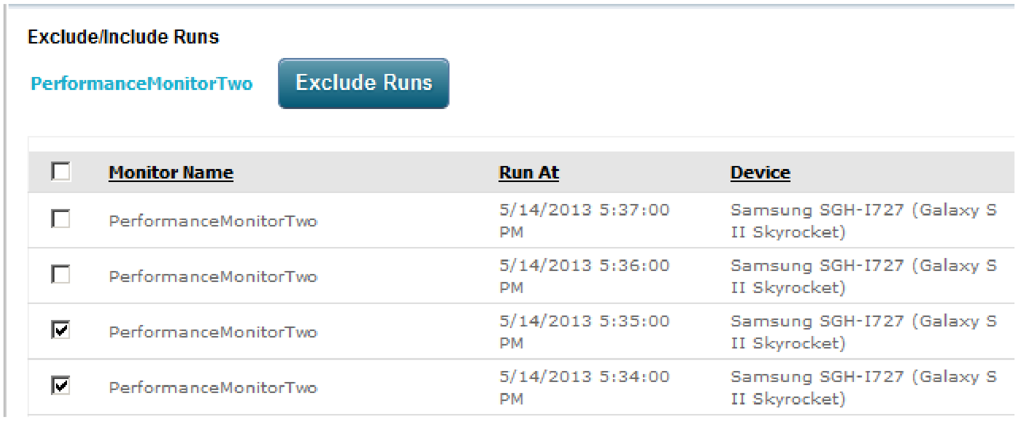
PerformanceMonitorTwo

○ ShowAll ○ Show Excluded Only ● Show Included Only

[Total: 53 Rows] 1 2

□	Monitor Name	Run At	Device	Carrier	Duration	Script Return Code	Description
□	PerformanceMonitorTwo	5/14/2013 5:37:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)	AT&T	00:00:03 627	FAIL	WaieventFailure
□	PerformanceMonitorTwo	5/14/2013 5:36:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)	AT&T	00:00:03 786	FAIL	WaieventFailure
□	PerformanceMonitorTwo	5/14/2013 5:35:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)	AT&T	00:00:13 736	SUCCESS	Success
□	PerformanceMonitorTwo	5/14/2013 5:34:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)	AT&T	00:00:13 732	SUCCESS	Success

2 Check the box next to a run to select it, and then click **Exclude Runs**.

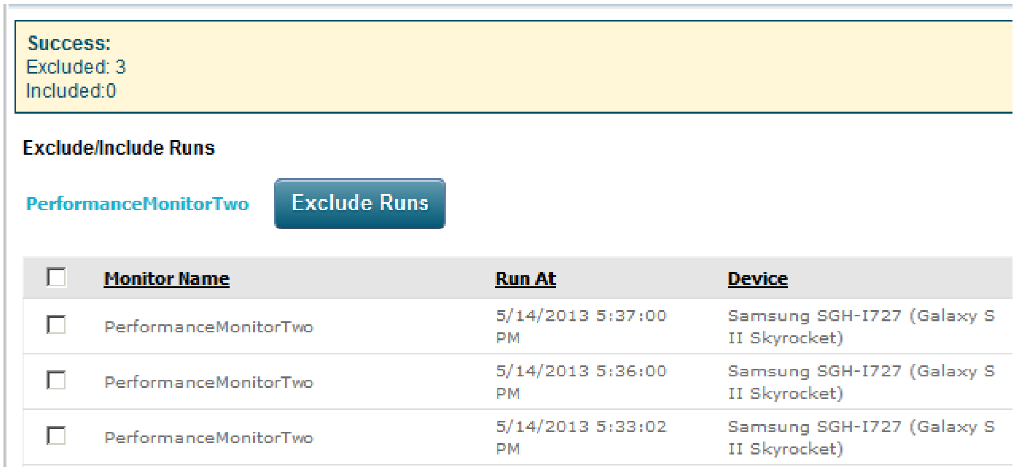


Exclude/Include Runs

PerformanceMonitorTwo

☐	Monitor Name	Run At	Device
☐	PerformanceMonitorTwo	5/14/2013 5:37:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)
☐	PerformanceMonitorTwo	5/14/2013 5:36:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)
☑	PerformanceMonitorTwo	5/14/2013 5:35:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)
☑	PerformanceMonitorTwo	5/14/2013 5:34:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)

A message at the top of the list confirms the operation.



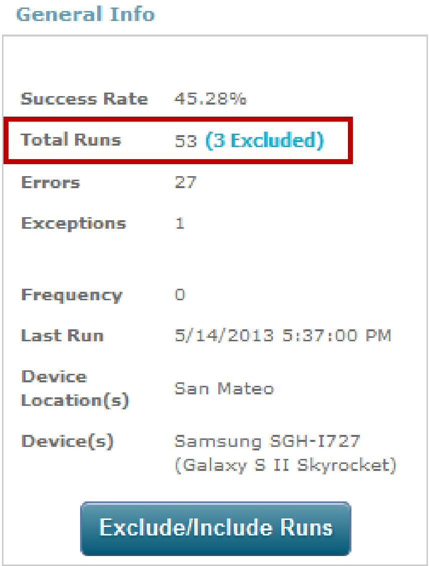
Success:
Excluded: 3
Included:0

Exclude/Include Runs

PerformanceMonitorTwo

☐	Monitor Name	Run At	Device
☐	PerformanceMonitorTwo	5/14/2013 5:37:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)
☐	PerformanceMonitorTwo	5/14/2013 5:36:00 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)
☐	PerformanceMonitorTwo	5/14/2013 5:33:02 PM	Samsung SGH-I727 (Galaxy S II Skyrocket)

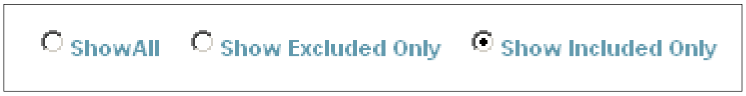
3 Click the highlighted monitor name to return to the monitor details report. The total number of runs displayed indicates that some runs have been excluded.



General Info

Success Rate	45.28%
Total Runs	53 (3 Excluded)
Errors	27
Exceptions	1
Frequency	0
Last Run	5/14/2013 5:37:00 PM
Device Location(s)	San Mateo
Device(s)	Samsung SGH-I727 (Galaxy S II Skyrocket)

4 Any user can click **Exclude/Include Runs** button to view the list of all monitor runs. Users can opt to view line items for excluded, included, or all runs.

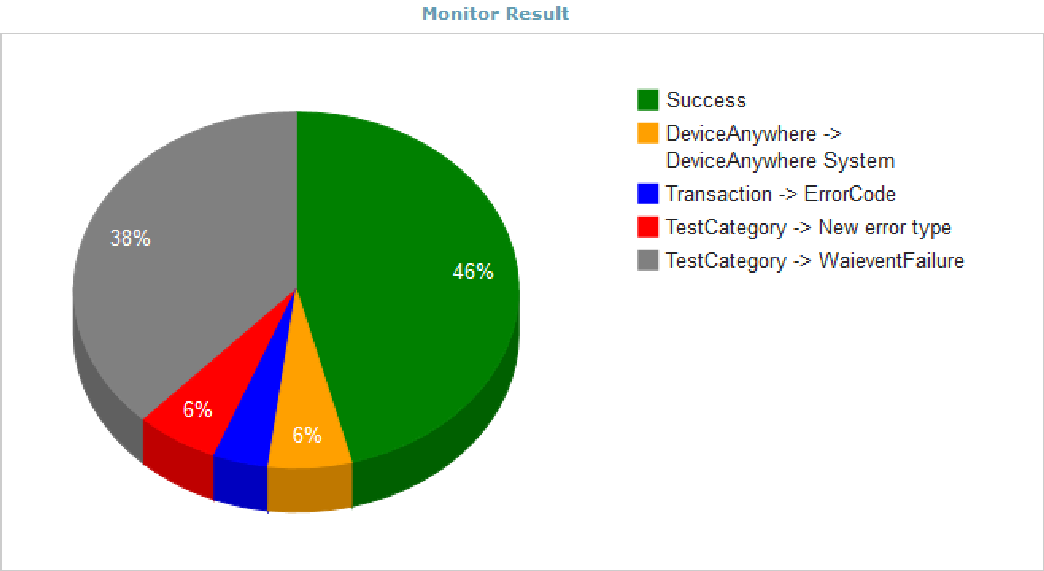


○ ShowAll ○ Show Excluded Only ● Show Included Only

6.1.3 Monitor Result

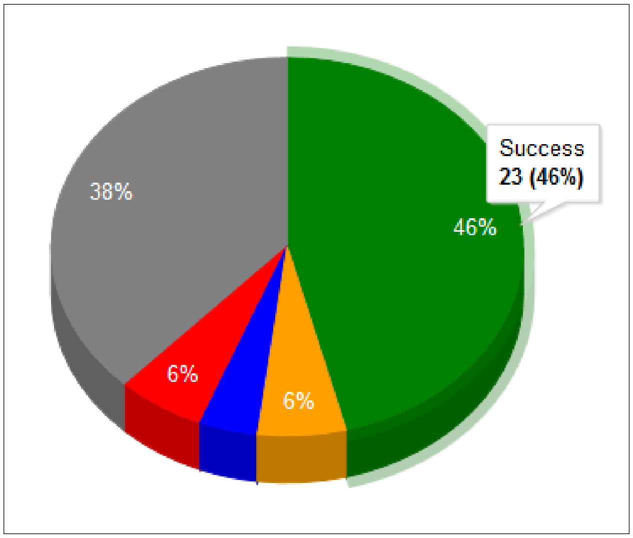
This section displays success and error rates for the time period selected in a pie chart.

Figure 6-3 Monitor Error and Success Rates



Hover over any section of the pie chart to view statistics (count and percentage) for that category.

Figure 6-4 Viewing Statistics for Successful/Failed Runs in the Pie Chart



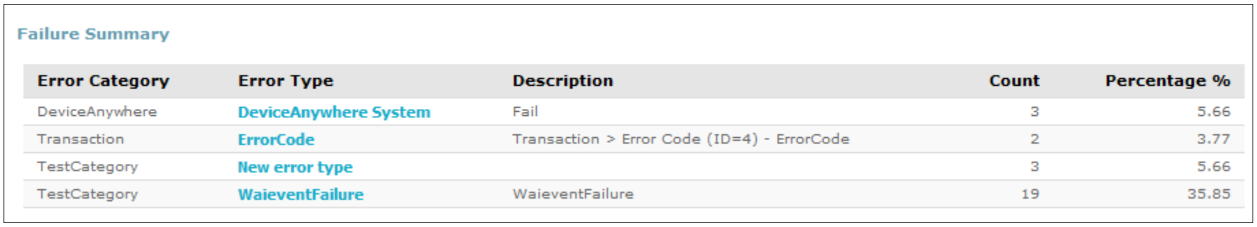
The total number of runs matches the number in General Info, and the count of failed runs matches the error breakdown in the Failure Summary.

6.1.4 Failure Summary

The failure summary displays details of failed runs, with the number of runs and percentage of total runs for each error encountered.

NOTE Not all errors encountered contribute to monitor incidents, however, as only some of them might have been associated with the monitor policy applied to the monitor.

Figure 6-5 Details of Failed Monitor Runs

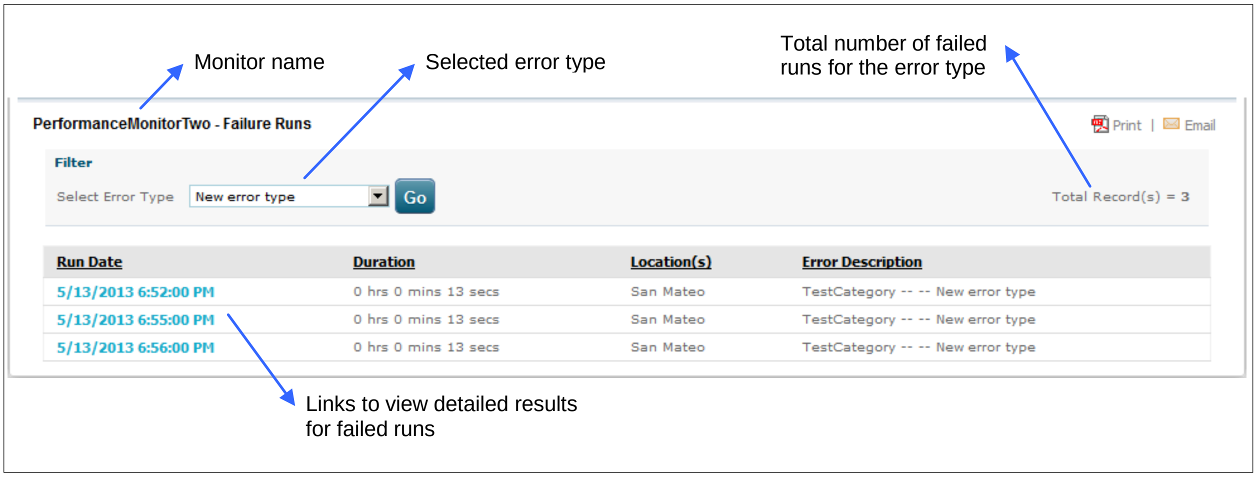


Failure Summary

Error Category	Error Type	Description	Count	Percentage %
DeviceAnywhere	DeviceAnywhere System	Fail	3	5.66
Transaction	ErrorCode	Transaction > Error Code (ID=4) - ErrorCode	2	3.77
TestCategory	New error type		3	5.66
TestCategory	WaieventFailure	WaieventFailure	19	35.85

Click a highlighted **Error Type** to view a log of all failed monitor runs for that particular error.

Figure 6-6 Failed Monitor Runs for an Error Type



Monitor name

Selected error type

Total number of failed runs for the error type

PerformanceMonitorTwo - Failure Runs

Filter

Select Error Type: New error type

Total Record(s) = 3

Run Date	Duration	Location(s)	Error Description
5/13/2013 6:52:00 PM	0 hrs 0 mins 13 secs	San Mateo	TestCategory -- -- New error type
5/13/2013 6:55:00 PM	0 hrs 0 mins 13 secs	San Mateo	TestCategory -- -- New error type
5/13/2013 6:56:00 PM	0 hrs 0 mins 13 secs	San Mateo	TestCategory -- -- New error type

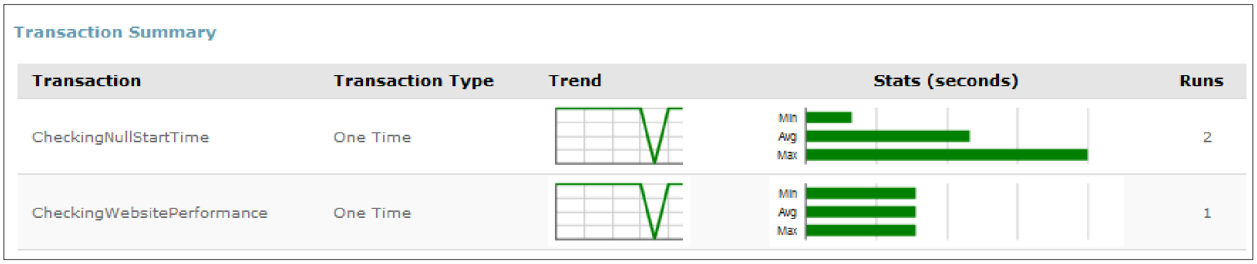
Links to view detailed results for failed runs

Click a highlighted **Run Date** to view detailed, screen-by-screen results for a run.

6.1.5 Transaction Summary

The transaction summary section of the monitor details report shows a list of all transaction runs in the monitor over the selected date range. Minimum, maximum, and average runs times are displayed. The trend graphic visually represents the success or failure of the transaction over the last ten runs.

Figure 6-7 Transaction Availability Graphs in Monitor Details



Transaction Summary

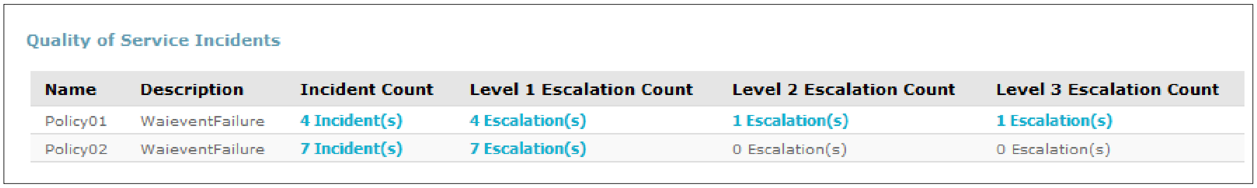
Transaction	Transaction Type	Trend	Stats (seconds)	Runs
CheckingNullStartTime	One Time		Min Avg Max	2
CheckingWebsitePerformance	One Time		Min Avg Max	1

NOTE The total number of transaction runs might exceed the number of monitor runs as a monitor might have several instances each of multiple transactions.

6.1.6 Quality of Service Incidents

This section lists monitor policy violation incidents for the date range chosen. If there are no incidents, you will see the message “No QoS Thresholds.”

Figure 6-8 Monitor Incidents



Quality of Service Incidents

Name	Description	Incident Count	Level 1 Escalation Count	Level 2 Escalation Count	Level 3 Escalation Count
Policy01	WaieventFailure	4 Incident(s)	4 Escalation(s)	1 Escalation(s)	1 Escalation(s)
Policy02	WaieventFailure	7 Incident(s)	7 Escalation(s)	0 Escalation(s)	0 Escalation(s)

For each monitor policy, the number of incidents and escalations at various levels are reported:

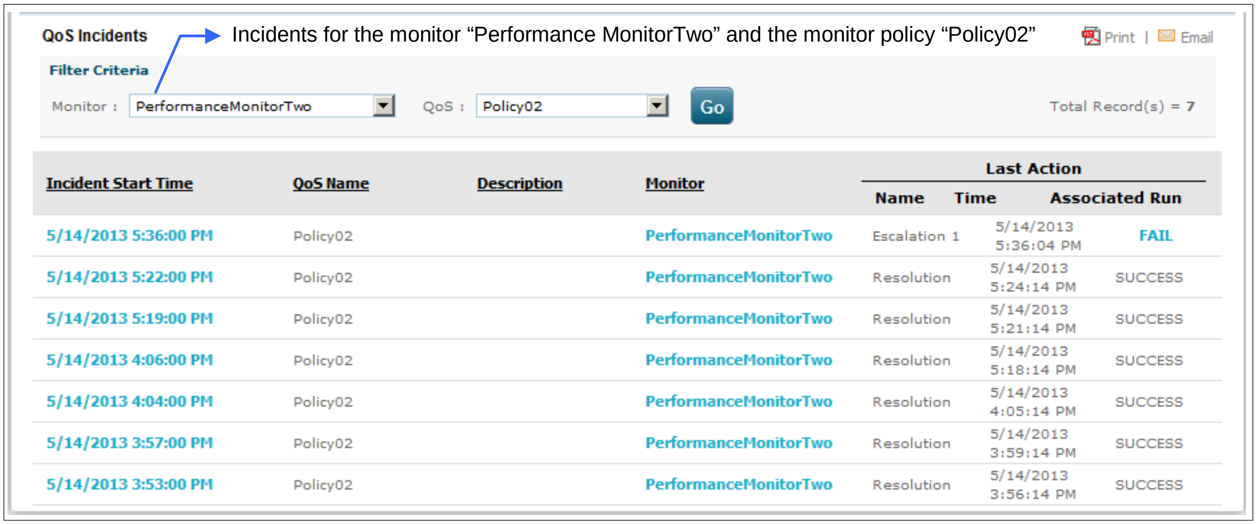
- **Name** of monitor policy
- **Description** of the policy
- **Incident Count**—the number of incidents of violation of the policy
- **Level 1 Escalation Count**—number of times a violation of the policy was escalated to level 1
- **Level 2 Escalation Count**—number of times a violation of the policy was escalated to level 2
- **Level 3 Escalation Count**—number of times a violation of the policy was escalated to level 3

NOTE Not all incidents are escalated to level 2 or 3 as they can be resolved at any level.

6.1.6.1 Accessing the Incident Lists for a Policy

Click an **Incident Count** to view the list of incidents for the given policy. The list of incidents you see is filtered by policy and monitor name. You are directed to the Script Performance tab.

Figure 6-9 List of Incidents Accessible from the Monitor Details Report



Incidents for the monitor “Performance MonitorTwo” and the monitor policy “Policy02”

Monitor : PerformanceMonitorTwo QoS : Policy02

Total Record(s) = 7

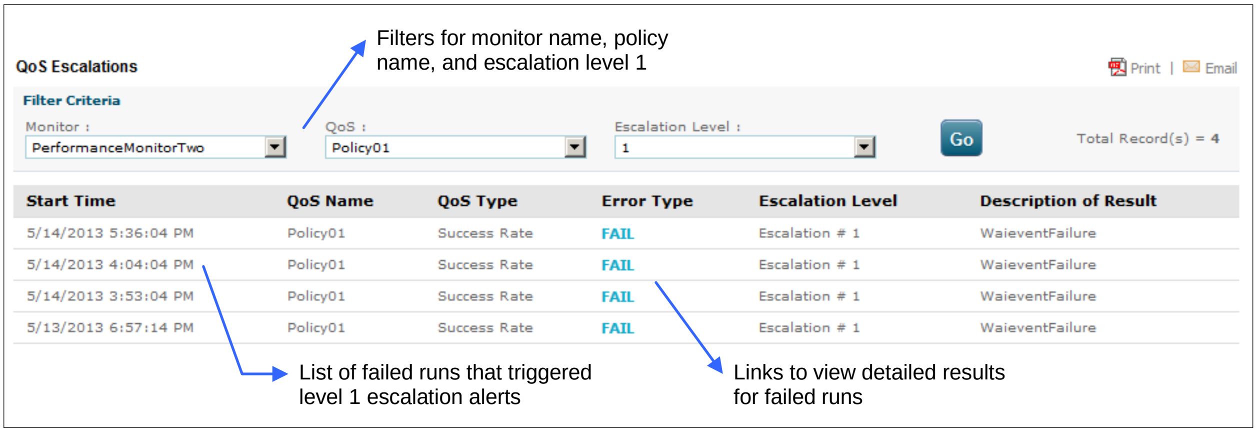
Incident Start Time	QoS Name	Description	Monitor	Last Action		
				Name	Time	Associated Run
5/14/2013 5:36:00 PM	Policy02		PerformanceMonitorTwo	Escalation 1	5/14/2013 5:36:04 PM	FAIL
5/14/2013 5:22:00 PM	Policy02		PerformanceMonitorTwo	Resolution	5/14/2013 5:24:14 PM	SUCCESS
5/14/2013 5:19:00 PM	Policy02		PerformanceMonitorTwo	Resolution	5/14/2013 5:21:14 PM	SUCCESS
5/14/2013 4:06:00 PM	Policy02		PerformanceMonitorTwo	Resolution	5/14/2013 5:18:14 PM	SUCCESS
5/14/2013 4:04:00 PM	Policy02		PerformanceMonitorTwo	Resolution	5/14/2013 4:05:14 PM	SUCCESS
5/14/2013 3:57:00 PM	Policy02		PerformanceMonitorTwo	Resolution	5/14/2013 3:59:14 PM	SUCCESS
5/14/2013 3:53:00 PM	Policy02		PerformanceMonitorTwo	Resolution	5/14/2013 3:56:14 PM	SUCCESS

Click the start time of an incident to view the detailed incident report. From this page, you can also click an available link for a run result to view detailed results.

6.1.6.2 Accessing Failed Runs for an Escalation Level

In the monitor details report, click the number of level 1, level 2, or level 3 escalations for a policy to see the list of failed runs that caused the escalations. For example, if you click the link for four level 1 escalations, you will see the list of four failed runs that triggered level 1 escalations. The image below shows the four runs that triggered a level 1 alert at different times for violation of a monitor policy.

Figure 6-10 Failed Runs that Triggered Escalation 1 Alerts



Filters for monitor name, policy name, and escalation level 1

QoS Escalations

Filter Criteria

Monitor : PerformanceMonitorTwo

QoS : Policy01

Escalation Level : 1

Total Record(s) = 4

Start Time	QoS Name	QoS Type	Error Type	Escalation Level	Description of Result
5/14/2013 5:36:04 PM	Policy01	Success Rate	FAIL	Escalation # 1	WaieventFailure
5/14/2013 4:04:04 PM	Policy01	Success Rate	FAIL	Escalation # 1	WaieventFailure
5/14/2013 3:53:04 PM	Policy01	Success Rate	FAIL	Escalation # 1	WaieventFailure
5/13/2013 6:57:14 PM	Policy01	Success Rate	FAIL	Escalation # 1	WaieventFailure

List of failed runs that triggered level 1 escalation alerts

Links to view detailed results for failed runs

From here, you can view detailed run results.

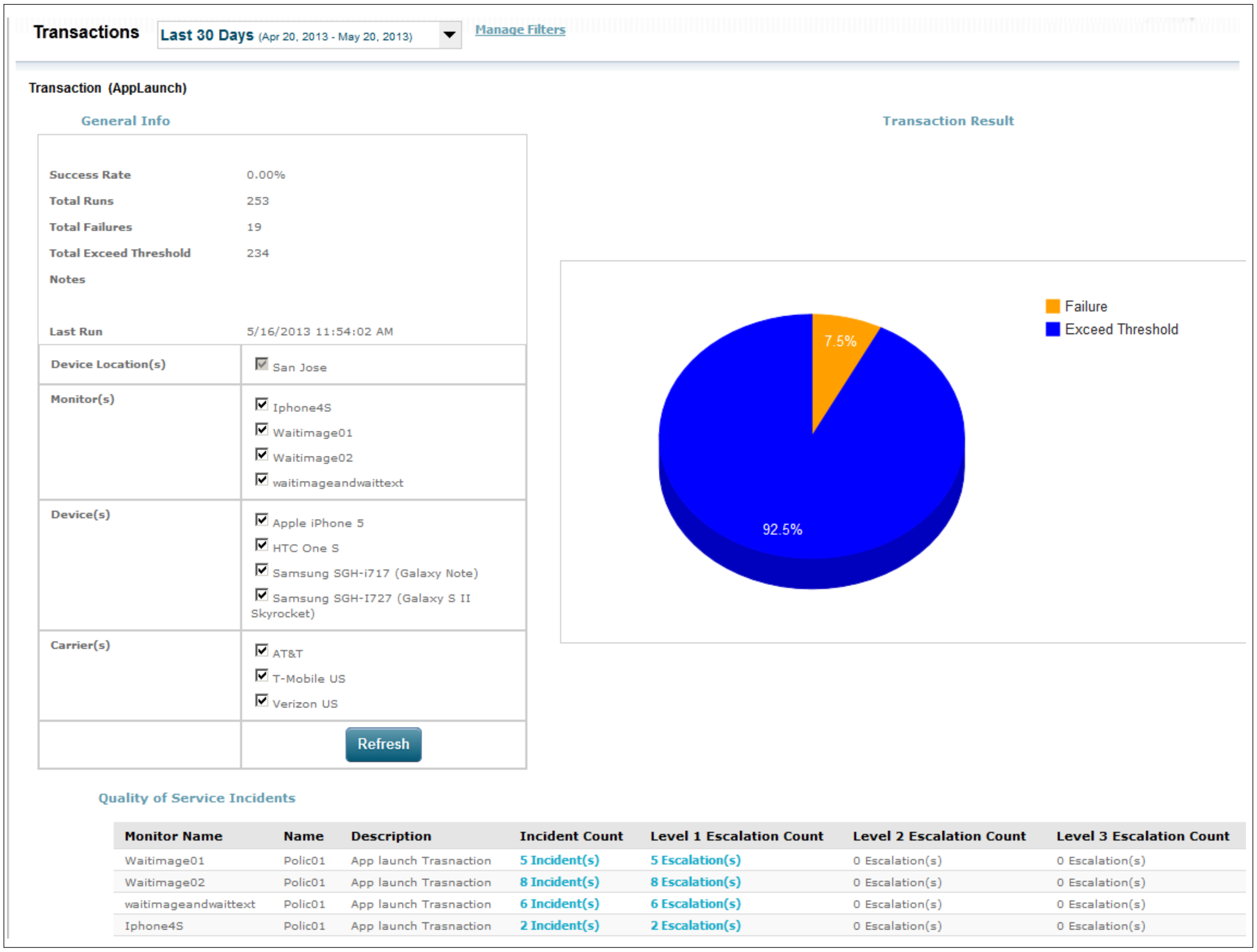
6.2 Transaction Details Report

The transaction details report opens up when you click the name of a transaction (in the Transactions tab). It displays the total number of transaction runs with the success rate and its graphic representation.

It lists the monitors, devices, and locations from which the transaction has been executed. You can recalculate the success rate by changing the date range or filtering out runs on a specific monitor, device, or carrier. The transaction details report also lists total number of transaction incidents and escalations at each level.

Each section of the report is discussed in detail below.

Figure 6-11 Transaction Details



Transactions Last 30 Days (Apr 20, 2013 - May 20, 2013) ▾ Manage Filters

Transaction (AppLaunch)

General Info

Success Rate	0.00%
Total Runs	253
Total Failures	19
Total Exceed Threshold	234
Notes	
Last Run	5/16/2013 11:54:02 AM
Device Location(s)	☑ San Jose
Monitor(s)	☑ Iphone4S ☑ Waitimage01 ☑ Waitimage02 ☑ waitimageandwaittext
Device(s)	☑ Apple iPhone 5 ☑ HTC One S ☑ Samsung SGH-i717 (Galaxy Note) ☑ Samsung SGH-I727 (Galaxy S II Skyrocket)
Carrier(s)	☑ AT&T ☑ T-Mobile US ☑ Verizon US
	Refresh

Transaction Result

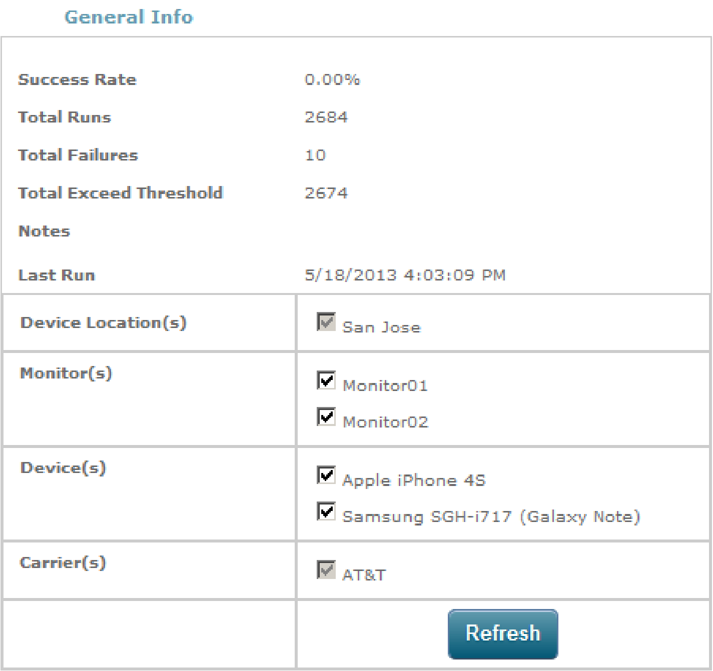
Quality of Service Incidents

Monitor Name	Name	Description	Incident Count	Level 1 Escalation Count	Level 2 Escalation Count	Level 3 Escalation Count
Waitimage01	Polic01	App launch Trasnaction	5 Incident(s)	5 Escalation(s)	0 Escalation(s)	0 Escalation(s)
Waitimage02	Polic01	App launch Trasnaction	8 Incident(s)	8 Escalation(s)	0 Escalation(s)	0 Escalation(s)
waitimageandwaittext	Polic01	App launch Trasnaction	6 Incident(s)	6 Escalation(s)	0 Escalation(s)	0 Escalation(s)
Iphone4S	Polic01	App launch Trasnaction	2 Incident(s)	2 Escalation(s)	0 Escalation(s)	0 Escalation(s)

6.2.1 General Info

This section displays statistics on the total number of runs, runs exceeding the threshold, outright failures, and success percentage for a selected date range. The statistics and incidents are recalculated when you change the date range or filter out certain monitors, devices, or carriers.

Figure 6-12 Transaction Statistics



General Info

Success Rate	0.00%
Total Runs	2684
Total Failures	10
Total Exceed Threshold	2674
Notes	
Last Run	5/18/2013 4:03:09 PM
Device Location(s)	☑ San Jose
Monitor(s)	☑ Monitor01 ☑ Monitor02
Device(s)	☑ Apple iPhone 4S ☑ Samsung SGH-i717 (Galaxy Note)
Carrier(s)	☑ AT&T
	Refresh

In the example above, the transaction has a 0% **Success Rate** largely attributable to runs exceeding the threshold (**Total Exceed Threshold**) and some outright transaction failures (**Total Failures**)

The transaction has been deployed on several monitors and devices. Uncheck a monitor or device to recalculate the transaction statistics.

6.2.2 Transaction Result

This section displays transaction success and failure rates, broken down by runs exceeding the threshold and outright transaction failures.

Figure 6-13 Transaction Failure and Success Rates (No Success)

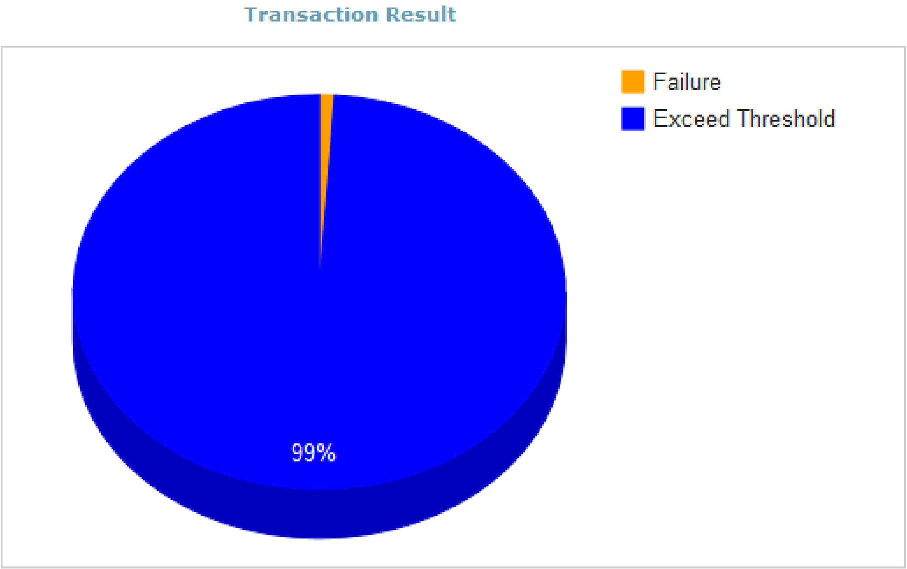
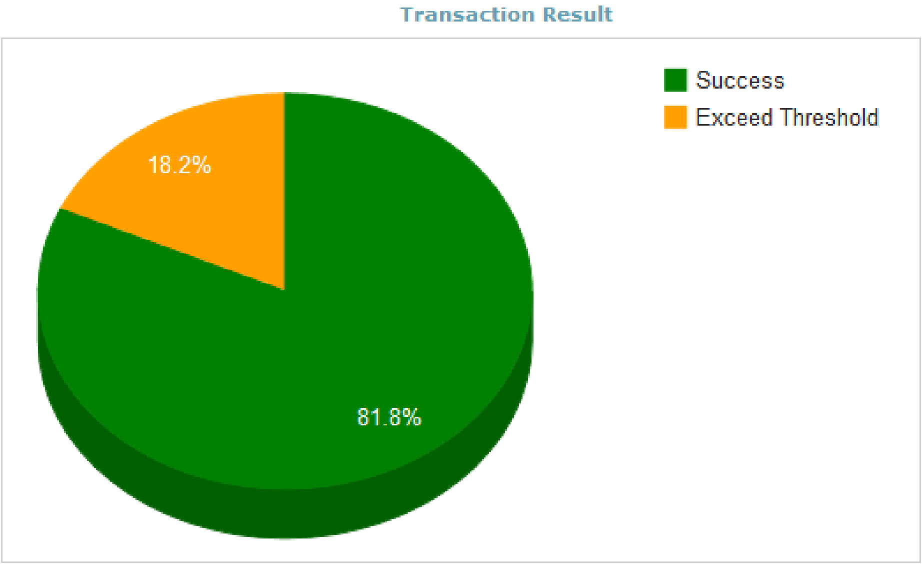
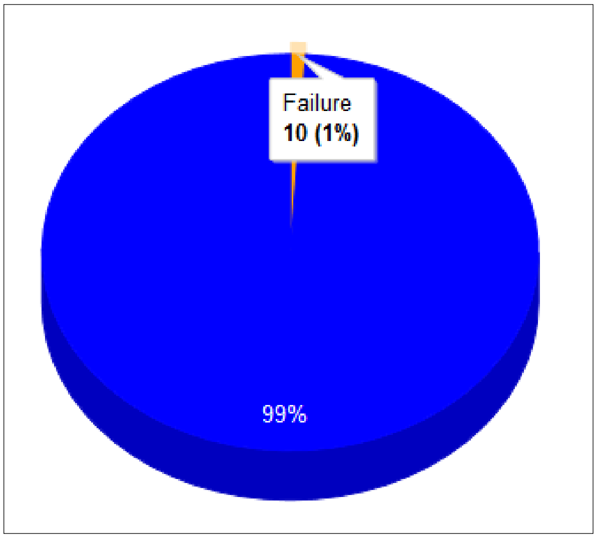


Figure 6-14 Transaction Success Rate



Hover over any section of the pie chart to view statistics (count and percentage) for that category.

Figure 6-15 Viewing Statistics for Successful/Failed Transaction Runs

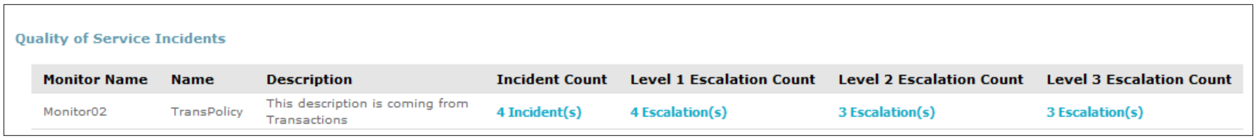


The total number of runs matches the number in General Info.

6.2.3 Quality of Service Incidents

This section lists transaction policy violation incidents for the date range chosen. If there are no incidents, you will see the message "No QoS Thresholds."

Figure 6-16 Transaction Incidents



Quality of Service Incidents

Monitor Name	Name	Description	Incident Count	Level 1 Escalation Count	Level 2 Escalation Count	Level 3 Escalation Count
Monitor02	TransPolicy	This description is coming from Transactions	4 Incident(s)	4 Escalation(s)	3 Escalation(s)	3 Escalation(s)

For each transaction policy, the number of incidents and escalations at various levels are reported:

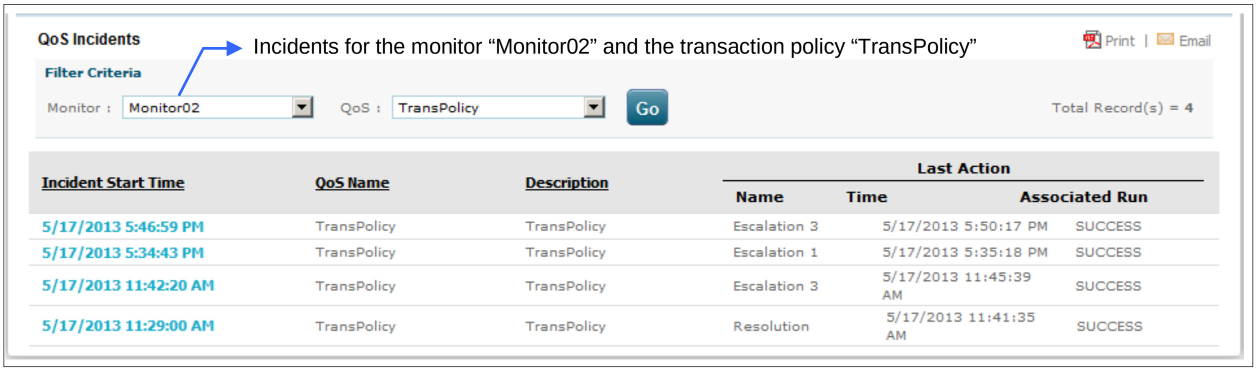
- **Monitor Name**—monitor in which transaction was used
- **Name** of transaction policy
- **Description** of the policy
- **Incident Count**—the number of incidents of violation of the policy
- **Level 1 Escalation Count**—number of times a violation of the policy was escalated to level 1
- **Level 2 Escalation Count**—number of times a violation of the policy was escalated to level 2
- **Level 3 Escalation Count**—number of times a violation of the policy was escalated to level 3

NOTE Not all incidents are escalated to level 2 or 3 as they can be resolved at any level.

6.2.3.1 Accessing the Incident Lists for a Policy

Click an **Incident Count** to view the list of incidents for the transaction policy. The list of incidents is filtered by policy and monitor name. You are directed to the QoS Violations tab.

Figure 6-17 List of Incidents Accessible from the Transaction Details Report



QoS Incidents

Incidents for the monitor "Monitor02" and the transaction policy "TransPolicy"

Filter Criteria

Monitor : Monitor02 QoS : TransPolicy

Total Record(s) = 4

Incident Start Time	QoS Name	Description	Last Action		
			Name	Time	Associated Run
5/17/2013 5:46:59 PM	TransPolicy	TransPolicy	Escalation 3	5/17/2013 5:50:17 PM	SUCCESS
5/17/2013 5:34:43 PM	TransPolicy	TransPolicy	Escalation 1	5/17/2013 5:35:18 PM	SUCCESS
5/17/2013 11:42:20 AM	TransPolicy	TransPolicy	Escalation 3	5/17/2013 11:45:39 AM	SUCCESS
5/17/2013 11:29:00 AM	TransPolicy	TransPolicy	Resolution	5/17/2013 11:41:35 AM	SUCCESS

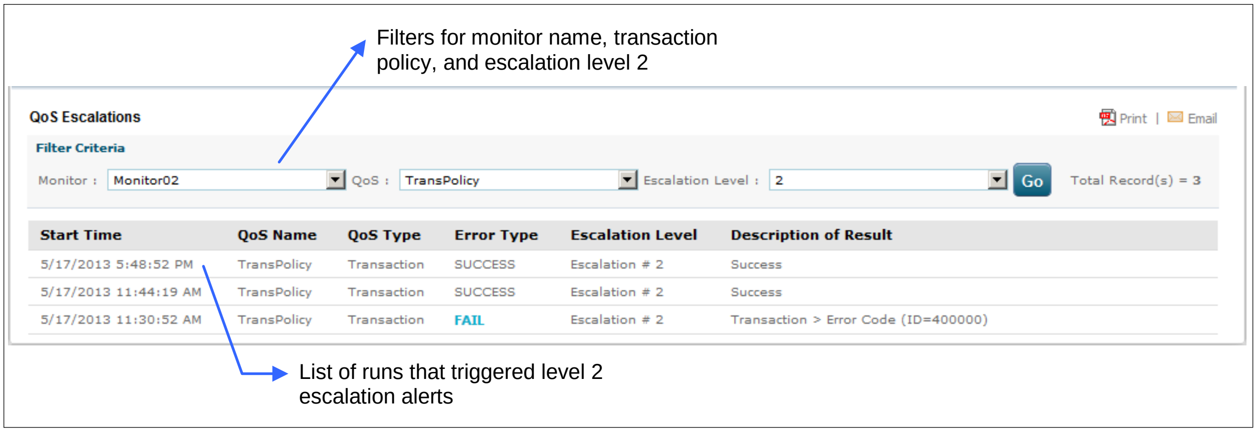
Click an incident start time to view the detailed incident report. From this page, you can also click an available link for a run result to view detailed results.

6.2.3.2 Accessing Failed Runs for an Escalation Level

In the transaction details report, click the number of level 1, level 2, or level 3 escalations for a policy to see the list of runs that caused the escalations. For example, if you click the link for three level 2 escalations, you will see the list of three runs that triggered level 2 escalations. The image below shows the three runs that triggered a level 2 alert at different times for violation of a transaction policy.

NOTE A run can be successful and trigger a transaction alert if the transaction exceeded acceptable run times.

Figure 6-18 Failed Runs that Triggered Escalation 1 Alerts



Filters for monitor name, transaction policy, and escalation level 2

QoS Escalations

Filter Criteria

Monitor : Monitor02 QoS : TransPolicy Escalation Level : 2 Go Total Record(s) = 3

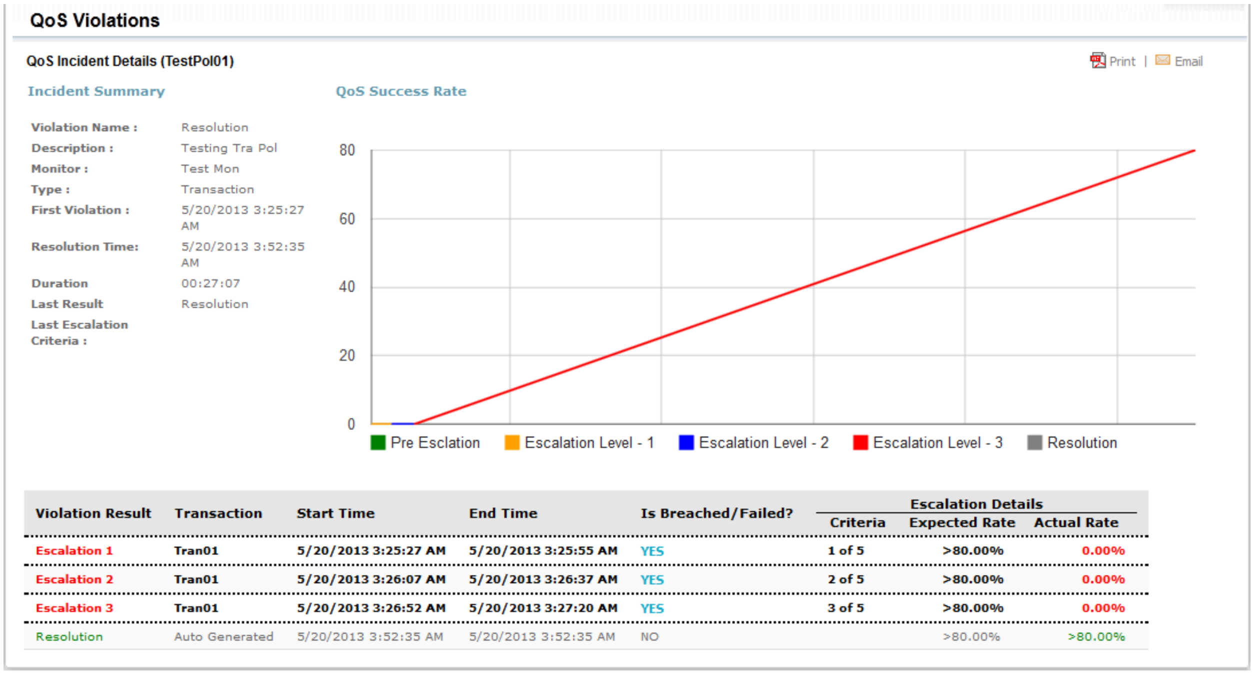
Start Time	QoS Name	QoS Type	Error Type	Escalation Level	Description of Result
5/17/2013 5:48:52 PM	TransPolicy	Transaction	SUCCESS	Escalation # 2	Success
5/17/2013 11:44:19 AM	TransPolicy	Transaction	SUCCESS	Escalation # 2	Success
5/17/2013 11:30:52 AM	TransPolicy	Transaction	FAIL	Escalation # 2	Transaction > Error Code (ID=400000)

List of runs that triggered level 2 escalation alerts

6.3 Incident Report

An incident report tracks a particular incident in violation of a transaction or monitor policy, tracking runs from the lowest escalation level through resolution. You can access an incident report by clicking an incident start time in the Script Performance tab (for monitor incidents) or the QoS Violations tab (for transaction incidents). You can also access an incident report by drilling down through the Quality of Service Incidents sections of a monitor details or transaction details report.

Figure 6-19 Incident Report for a Transaction



QoS Violations

QoS Incident Details (TestPol01)

Incident Summary

Violation Name :	Resolution
Description :	Testing Tra Pol
Monitor :	Test Mon
Type :	Transaction
First Violation :	5/20/2013 3:25:27 AM
Resolution Time:	5/20/2013 3:52:35 AM
Duration	00:27:07
Last Result	Resolution
Last Escalation Criteria :	

QoS Success Rate

Violation Result	Transaction	Start Time	End Time	Is Breached/Failed?	Escalation Details		
					Criteria	Expected Rate	Actual Rate
Escalation 1	Tran01	5/20/2013 3:25:27 AM	5/20/2013 3:25:55 AM	YES	1 of 5	>80.00%	0.00%
Escalation 2	Tran01	5/20/2013 3:26:07 AM	5/20/2013 3:26:37 AM	YES	2 of 5	>80.00%	0.00%
Escalation 3	Tran01	5/20/2013 3:26:52 AM	5/20/2013 3:27:20 AM	YES	3 of 5	>80.00%	0.00%
Resolution	Auto Generated	5/20/2013 3:52:35 AM	5/20/2013 3:52:35 AM	NO		>80.00%	>80.00%

Among other things, the incident report summary lists the current escalation or resolution status of the incident and the time the incident began. The summary includes:

- **Violation Result**—escalation level (or resolution) associated with the run, if the run contributes to an escalation/resolution
- **Description** of the policy violated

- **Monitor** name
- **Type** of policy (monitor or transaction)
- **First Violation**—start time of the run that triggered the level 1 escalation alert
- **Resolution Time**—start time of the run that triggered the resolution alert
- **Duration**—time between runs that triggered the first escalation and resolution alerts
- **Last Result**—current escalation or resolution status of the incident
- **Last Escalation Criteria**—criterion for the current escalation or resolution status (e.g., 5 out 5 successful runs constitute a resolution)

The run summary at the bottom contains line items for the run that kicked off the incident and each run after through to resolution. If a run contributes to an escalation, it is highlighted and the associated escalation level is displayed. Links are displayed for detailed results of failed runs.

- **Violation Name**—current escalation level (or resolution)
- **Transaction** name
- **Start Time** of run
- **End Time** of run
- **Is Breached/Failed?**—whether the transaction exceeded the threshold or failed outright
- **Escalation Details**
    - **Criteria**—number of failed runs out of a given number that trigger the operative escalation
    - **Expected Rate**—desired success rate based on the Criteria leading to a level 1 escalation, e.g., if 1 of 5 failed runs lead to escalation level 1, then the desired success rate is at least 80%.
    - **Actual Rate**—actual success rate

The incident graph shows the success rate of the transaction and plots the graph based on the runs that cause escalations/resolution. The runs associated with different escalation levels are graphed in different colors. Hover over a node to see the run's associated escalation level and success rate.

Figure 6-20 Incident Graph for a Transaction

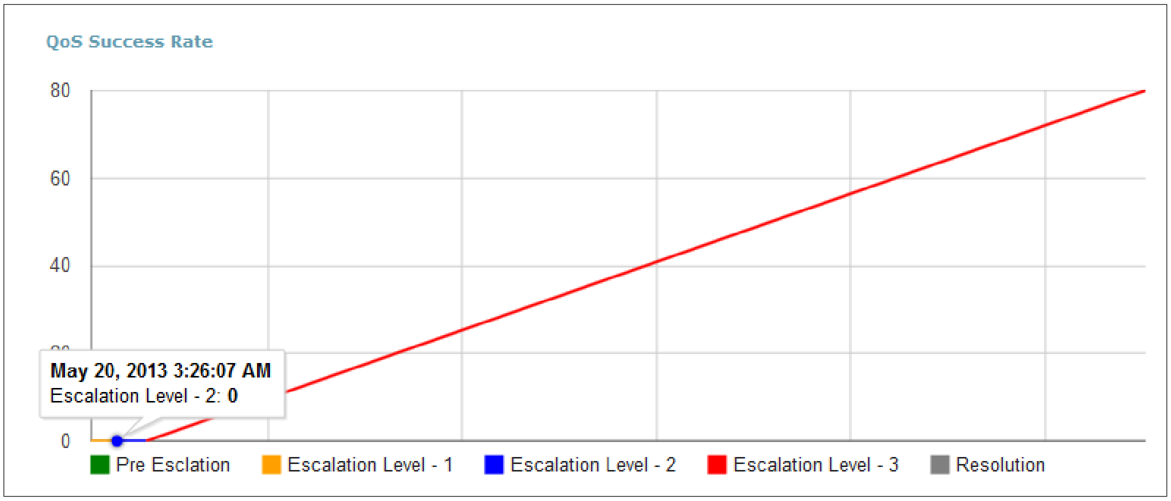


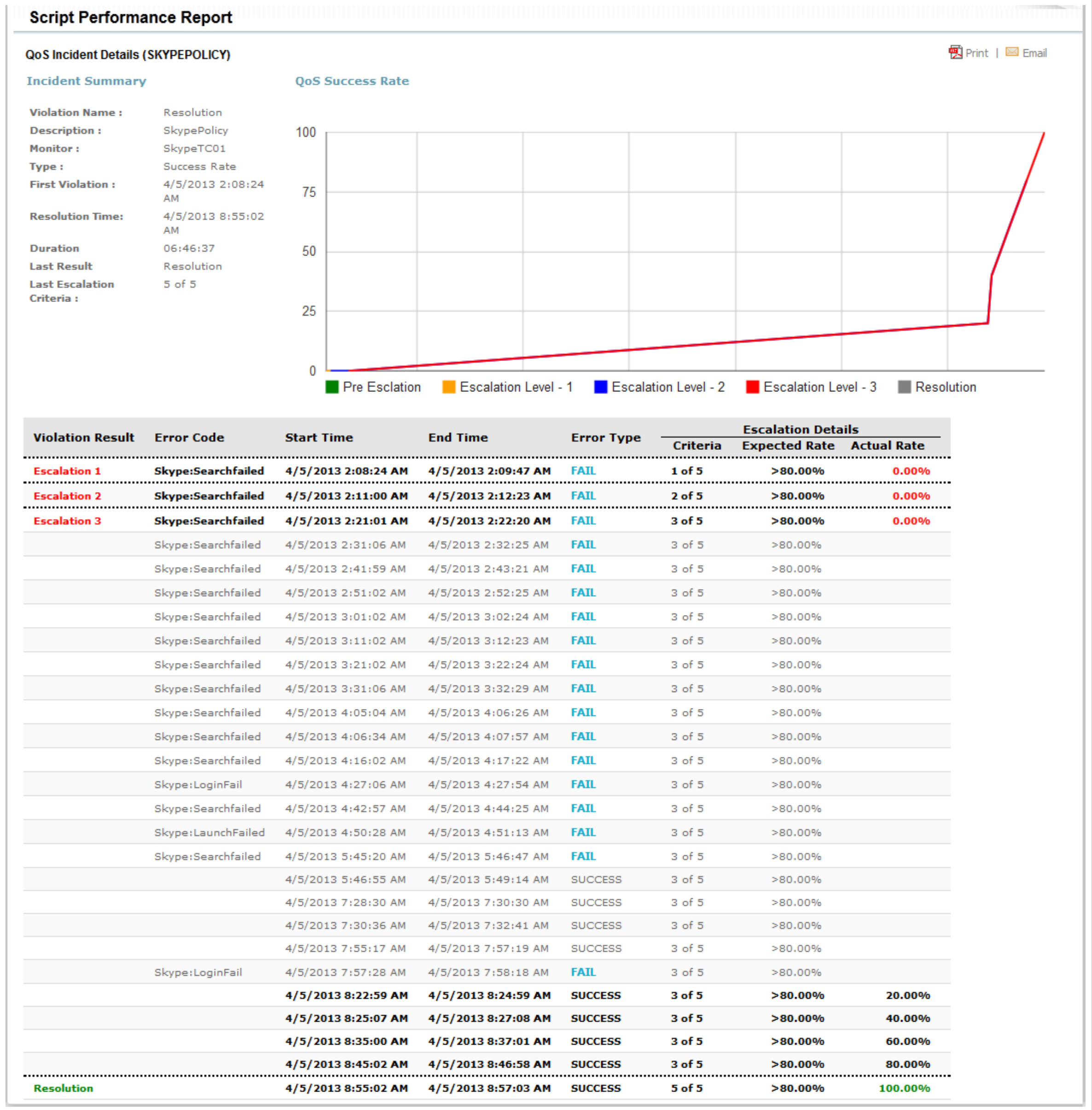
Figure 6-19 above shows an incident report for a transaction policy with the following escalation criteria:

- 1 out of 5 failed runs causes a level 1 (lowest) escalation
- 2 out of 5 failed runs cause a level 2 escalation
- 3 out of 5 failed runs cause a level 3 (highest) escalation

The report lists three consecutive runs that led up to the level 3 escalation. The incident was then resolved by republishing the project.

In the incident report for a monitor below, there were several failed runs after the run that triggered the level 3 escalation. The **Error Type** column notes whether the run failed or succeeded. The incident was resolved by 5 consecutive successful runs, which took the success rate back to 100% (i.e., 5/5 successful runs).

Figure 6-21 Incident Report for a Monitor



Script Performance Report

QoS Incident Details (SKYPEPOLICY)

Incident Summary

Violation Name :	Resolution
Description :	SkypePolicy
Monitor :	SkypeTC01
Type :	Success Rate
First Violation :	4/5/2013 2:08:24 AM
Resolution Time:	4/5/2013 8:55:02 AM
Duration	06:46:37
Last Result	Resolution
Last Escalation Criteria :	5 of 5

QoS Success Rate

Violation Result	Error Code	Start Time	End Time	Error Type	Escalation Details		
					Criteria	Expected Rate	Actual Rate
Escalation 1	Skype:Searchfailed	4/5/2013 2:08:24 AM	4/5/2013 2:09:47 AM	FAIL	1 of 5	>80.00%	0.00%
Escalation 2	Skype:Searchfailed	4/5/2013 2:11:00 AM	4/5/2013 2:12:23 AM	FAIL	2 of 5	>80.00%	0.00%
Escalation 3	Skype:Searchfailed	4/5/2013 2:21:01 AM	4/5/2013 2:22:20 AM	FAIL	3 of 5	>80.00%	0.00%
	Skype:Searchfailed	4/5/2013 2:31:06 AM	4/5/2013 2:32:25 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 2:41:59 AM	4/5/2013 2:43:21 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 2:51:02 AM	4/5/2013 2:52:25 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 3:01:02 AM	4/5/2013 3:02:24 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 3:11:02 AM	4/5/2013 3:12:23 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 3:21:02 AM	4/5/2013 3:22:24 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 3:31:06 AM	4/5/2013 3:32:29 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 4:05:04 AM	4/5/2013 4:06:26 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 4:06:34 AM	4/5/2013 4:07:57 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 4:16:02 AM	4/5/2013 4:17:22 AM	FAIL	3 of 5	>80.00%	
	Skype:LoginFail	4/5/2013 4:27:06 AM	4/5/2013 4:27:54 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 4:42:57 AM	4/5/2013 4:44:25 AM	FAIL	3 of 5	>80.00%	
	Skype:LaunchFailed	4/5/2013 4:50:28 AM	4/5/2013 4:51:13 AM	FAIL	3 of 5	>80.00%	
	Skype:Searchfailed	4/5/2013 5:45:20 AM	4/5/2013 5:46:47 AM	FAIL	3 of 5	>80.00%	
		4/5/2013 5:46:55 AM	4/5/2013 5:49:14 AM	SUCCESS	3 of 5	>80.00%	
		4/5/2013 7:28:30 AM	4/5/2013 7:30:30 AM	SUCCESS	3 of 5	>80.00%	
		4/5/2013 7:30:36 AM	4/5/2013 7:32:41 AM	SUCCESS	3 of 5	>80.00%	
		4/5/2013 7:55:17 AM	4/5/2013 7:57:19 AM	SUCCESS	3 of 5	>80.00%	
	Skype:LoginFail	4/5/2013 7:57:28 AM	4/5/2013 7:58:18 AM	FAIL	3 of 5	>80.00%	
		4/5/2013 8:22:59 AM	4/5/2013 8:24:59 AM	SUCCESS	3 of 5	>80.00%	20.00%
		4/5/2013 8:25:07 AM	4/5/2013 8:27:08 AM	SUCCESS	3 of 5	>80.00%	40.00%
		4/5/2013 8:35:00 AM	4/5/2013 8:37:01 AM	SUCCESS	3 of 5	>80.00%	60.00%
		4/5/2013 8:45:02 AM	4/5/2013 8:46:58 AM	SUCCESS	3 of 5	>80.00%	80.00%
Resolution		4/5/2013 8:55:02 AM	4/5/2013 8:57:03 AM	SUCCESS	5 of 5	>80.00%	100.00%

6.4 Detailed Run Results

Detailed results for monitor script runs are available at several points in the DAE Monitoring Portal by clicking the run result link. Links to view results are available for following types of failures:

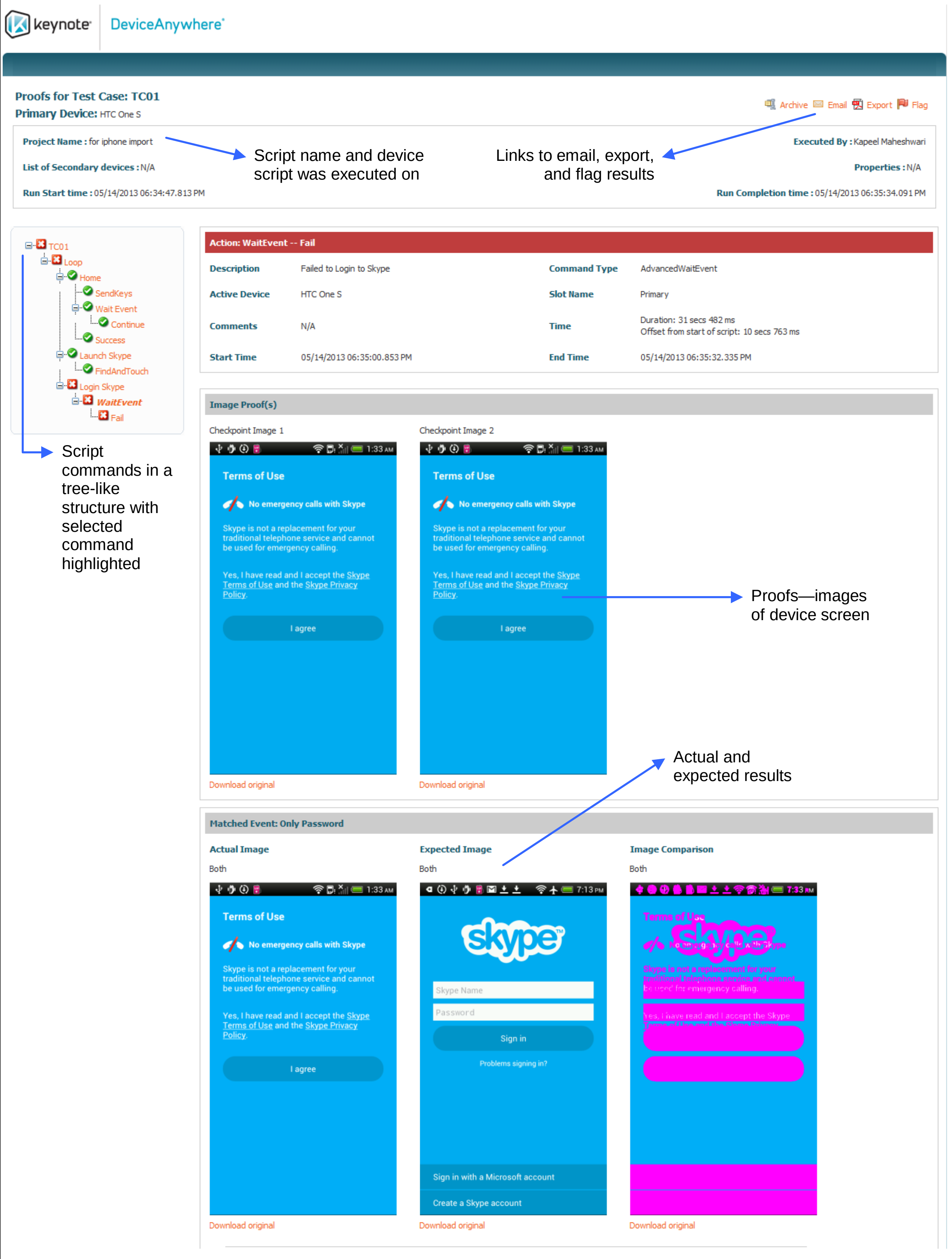
- A monitor run that encountered an error as defined by script logic (e.g., the **Fail** link in the execution report)—failed runs always have links for detailed results.
- A successful monitor run but one in which transactions failed or exceeded acceptable run times (e.g., the **Success** link in the execution report)
- A monitor run that encountered a system error and was therefore not completed as expected (e.g., the **Error** link in the execution report)

Detailed results include command-by-command results, including device screen proofs and comparisons between expected and actual results.

Script commands, including commands in embedded scripts are displayed on the left in a tree-like structure. Results for a test case containing calls to actions contain step-by-step results for embedded actions as well. Select a command on the left to view results for it in the right pane.

The figure below shows the detailed results for a monitor script that calls embedded actions. The tree structure on the left displays commands within the embedded actions. In this example, the script failed at an image verification step. For the command selected on the left, the right pane displays proofs as well as actual vs. expected results.

Figure 6-22 Detailed Results—Failed Monitor Run



keynote DeviceAnywhere

Proofs for Test Case: TC01
Primary Device: HTC One S

Archive Email Export Flag

Project Name : for iphone import
List of Secondary devices : N/A
Run Start time : 05/14/2013 06:34:47.813 PM

Executed By : Kapeel Maheshwari
Properties : N/A
Run Completion time : 05/14/2013 06:35:34.091 PM

Script name and device script was executed on

Links to email, export, and flag results

- TC01
  - Loop
    - Home
      - SendKeys
      - Wait Event
        - Continue
      - Success
    - Launch Skype
      - FindAndTouch
    - Login Skype
      - *WaitEvent*
        - Fail

Script commands in a tree-like structure with selected command highlighted

Action: WaitEvent -- Fail

Description	Failed to Login to Skype	**Command Type**	AdvancedWaitEvent
Active Device	HTC One S	**Slot Name**	Primary
Comments	N/A	**Time**	Duration: 31 secs 482 ms Offset from start of script: 10 secs 763 ms
Start Time	05/14/2013 06:35:00.853 PM	**End Time**	05/14/2013 06:35:32.335 PM

Image Proof(s)

Checkpoint Image 1

1:33 AM
Terms of Use
No emergency calls with Skype
Skype is not a replacement for your traditional telephone service and cannot be used for emergency calling.
Yes, I have read and I accept the Skype Terms of Use and the Skype Privacy Policy.
I agree

Download original

Checkpoint Image 2

1:33 AM
Terms of Use
No emergency calls with Skype
Skype is not a replacement for your traditional telephone service and cannot be used for emergency calling.
Yes, I have read and I accept the Skype Terms of Use and the Skype Privacy Policy.
I agree

Download original

Proofs—images of device screen

Actual and expected results

Matched Event: Only Password

Actual Image

Both

1:33 AM
Terms of Use
No emergency calls with Skype
Skype is not a replacement for your traditional telephone service and cannot be used for emergency calling.
Yes, I have read and I accept the Skype Terms of Use and the Skype Privacy Policy.
I agree

Download original

Expected Image

Both

Download original

Image Comparison

Both

Download original

If you opt to collect proofs in the **Advanced** tab of a script command, the first and last screen of the device during command execution are displayed in test results.

Figure 6-23 Proofs Elected in the ***Advanced*** *Tab*

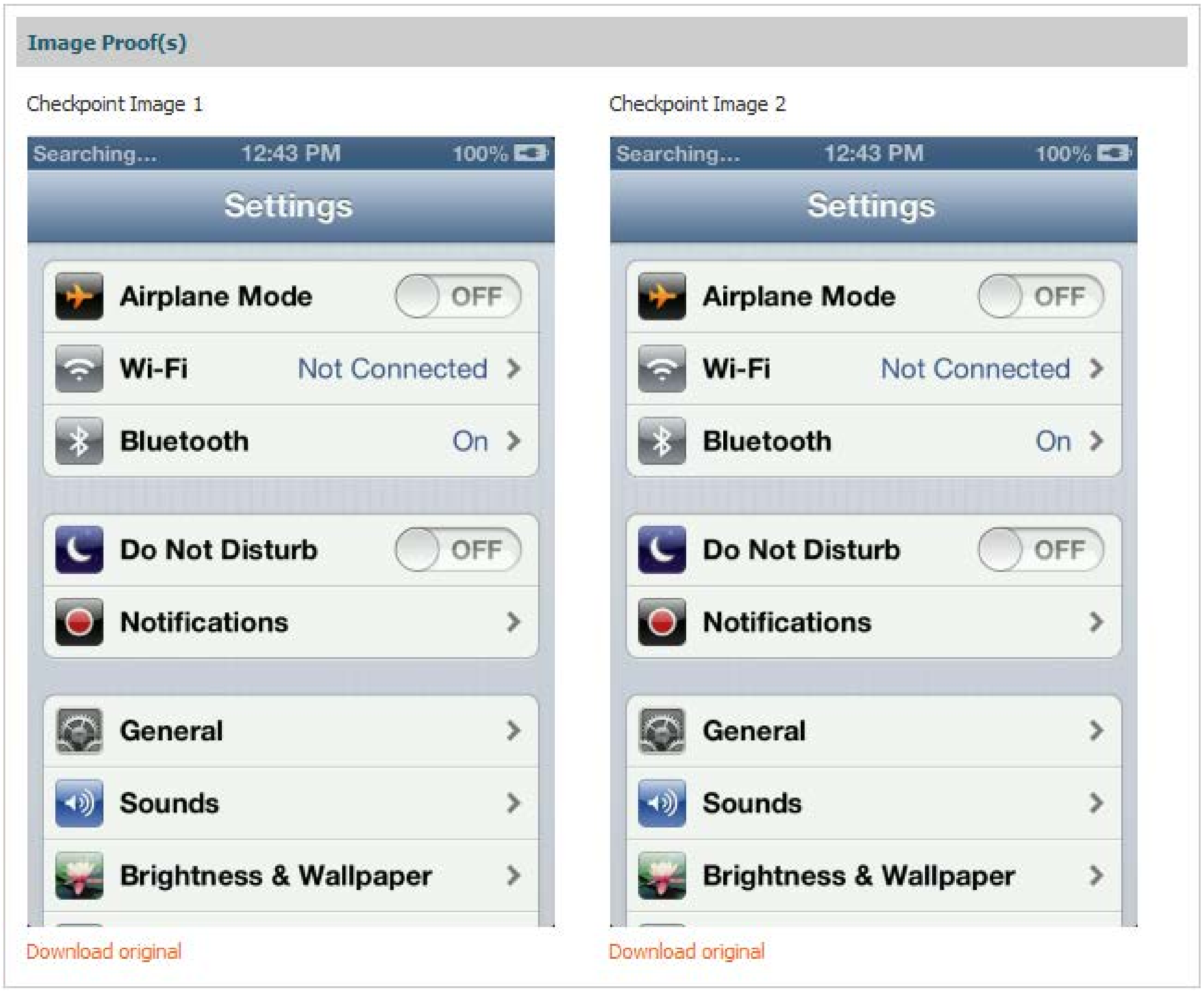
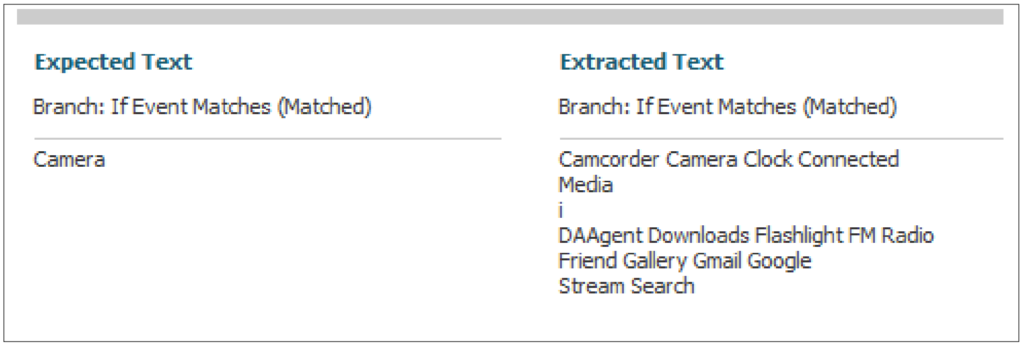


Image Proof(s)

Checkpoint Image 1	Checkpoint Image 2
Download original	Download original

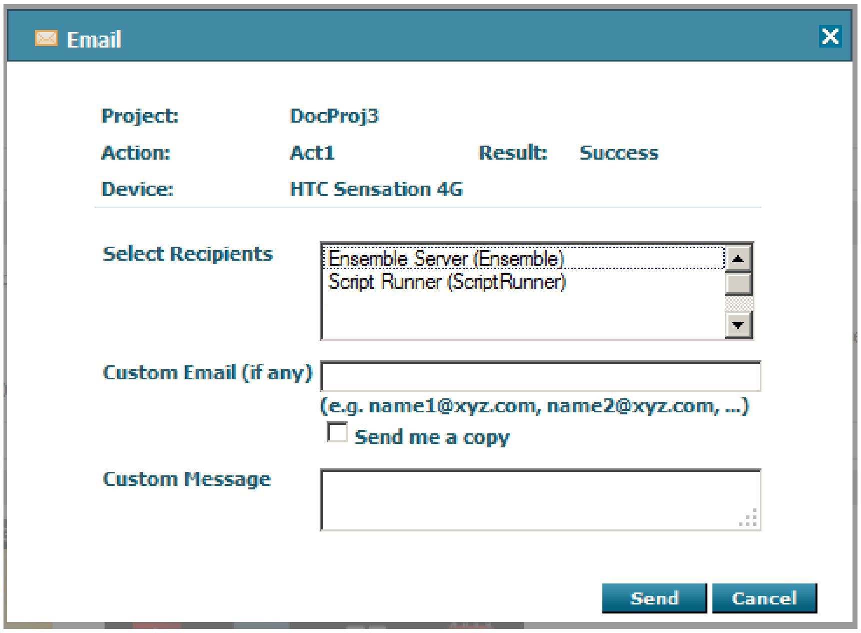
If your command uses a text-based reference point for verification, results for both extracted and expected text are displayed.



Expected Text	Extracted Text
Branch: If Event Matches (Matched)	Branch: If Event Matches (Matched)
Camera	Camcorder Camera Clock Connected Media i DAAgent Downloads Flashlight FM Radio Friend Gallery Gmail Google Stream Search

Click **Email Results** at the top left of the window to email a link to the current results page. You can **Select Recipients** from users in your account or enter a **Custom Email** address as well as mark a copy to yourself. Enter a **Message** in the field provided and click **Send**.

Figure 6-24 Emailing Test Results from the Portal



Email

Project: DocProj3

Action: Act1 Result: Success

Device: HTC Sensation 4G

Select Recipients: Ensemble Server (Ensemble)
Script Runner (ScriptRunner)

Custom Email (if any)

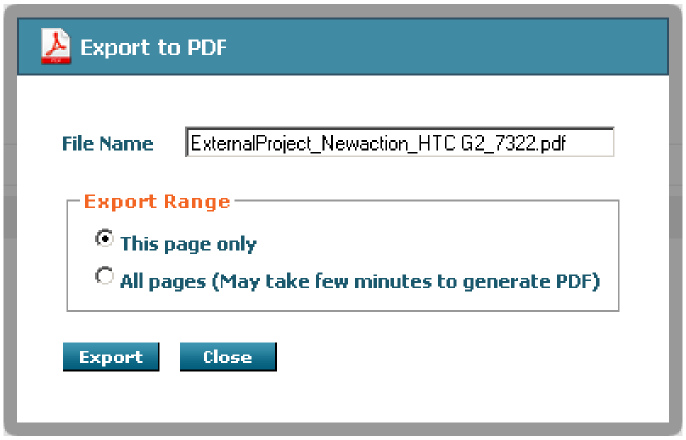
(e.g. name1@xyz.com, name2@xyz.com, ...)

□ Send me a copy

Custom Message

Click **Export** to save results as a PDF file. You can opt to save the currently displayed page (**This page only**) or results for all commands in the script (**All pages**).

Figure 6-25 Exporting Test Results from the Portal



Export to PDF

File Name: ExternalProject_Newaction_HTC G2_7322.pdf

Export Range

● This page only

○ All pages (May take few minutes to generate PDF)

7 Charts

Powerful graphing tools in the DeviceAnywhere Enterprise Monitoring Portal enable you to create charts of transaction and monitor availability and performance. Availability charts visually represent the success or failure of a transaction or monitor over a period of time. Performance charts show transaction completion times for runs in the selected date range. A monitor performance chart contains data points for completion times for transactions contained in the selected monitors. A transaction performance chart shows the completion times of each selected transaction (over the selected date range).

This chapter discusses the types of availability and performance charts that can be generated in the TCE Monitoring Portal, how to generate a chart, availability charts in detail, and performance charts in detail.

7.1 Chart and Report Types

Several report types are available for displaying performance and availability.

- *Overall*— this report type calculates performance or availability over a time frame for selected monitors or transactions, not grouped by location, device, or carrier.
- *By device location*—this report type calculates performance or availability over a time frame for selected monitors or transactions, grouped by location of the Ensemble Server to which devices are connected. For example, if you have 10 different monitors running using devices connected to 5 device servers, this type of report lets you see performance or availability for each of those 5 locations. Select this report type when you have more than one Ensemble Server location.
- *By device*—this report type calculates performance or availability over a time frame for selected monitors or transactions, grouped by the device they run on. For example, if you have 10 monitors running on 5 devices, this type of report lets you see performance or availability on each device. Select this report type when your monitors share a small group of devices. Or you might have a transaction that appears in several monitors running on multiple devices. Viewing availability by device allows you to see the pattern of transaction success or failure on each device.
- *By carrier*—this report type calculates performance or availability over a time frame for selected monitors or transactions, grouped by carrier. For example, if you have 10 different monitors running on devices with 4 carriers, this type of report lets you see performance or availability on each of those carriers. Select this report type when you have multiple carriers and more than one device per carrier.

Several chart types are available for displaying performance and availability.

- *Over time*—this type of chart shows availability (success vs. failure) or performance (transaction run times) for each run of a selected monitor or transaction over a time frame. For a larger time frame, run data is aggregated over smaller intervals and averaged for display.
- *Average*—this type of chart shows the average availability (success rate) or performance (transaction run time) of selected monitors or transactions over a time frame. This is a bar chart with a single data point for each transaction or monitor selected. For example, average performance for a transaction is calculated as the average transaction run time over a date range across all the monitors it appears in. Average monitor performance is calculated as the average run time of all its transactions over a date range.

- *Time of day*—this type of chart shows performance or availability for selected monitors or transactions calculated for every hour in the day. The data point for each hour consists of runs occurring in that hour. For example, transaction performance for a given hour consists of the average completion time of all transaction runs within that hour. Monitor performance for a given hour consists of the average completion time of all runs of all transactions in the monitor within that hour.

This chapter mainly uses overall reports to generate sample charts.

7.2 Generating Charts

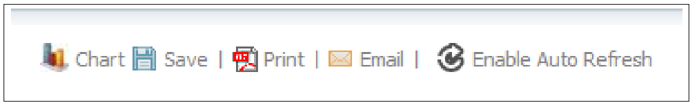
The graphing feature is available from the transaction summary (**Transactions** tab) and monitor summary (**Monitors** tab).

To view monitor charts:

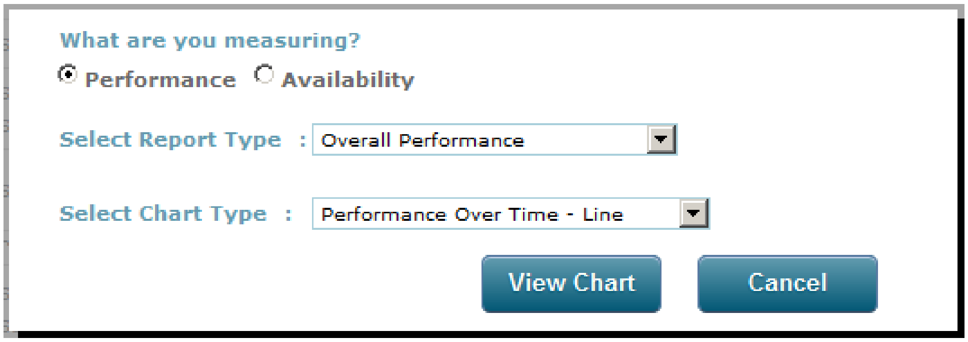
1 Navigate to the **Monitors** tab.

2 Check the box next to the monitor(s) you wish to chart.

3 Click **Chart** at the top-right corner of the page.



4 From the dialog box that appears, select your chart and report type and then click **View Chart**.


What are you measuring?

● Performance ○ Availability

Select Report Type : Overall Performance

Select Chart Type : Performance Over Time - Line

To view transaction charts:

1 Navigate to the **Transactions** tab.

2 Choose the criterion by which transaction information is split out and displayed—**Details By**. You can choose **None**, **Monitor**, **Location**, **Device**, or **Carrier**. This criterion is also used to chart the transaction(s) selected.

3 Check the box next to the transaction entries you wish to chart.

4 Click **Chart** at the top-right corner of the page.

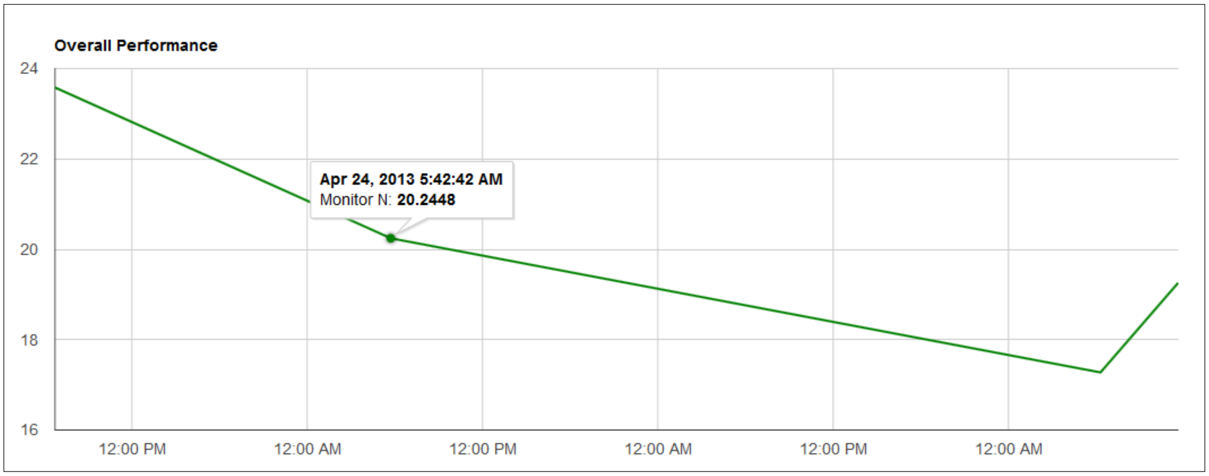
5 From the dialog box that appears, select your chart and report type and then click **View Chart**.

6 Click **Refresh** if necessary after adjusting/changing chart components.

7.3 Viewing Charts and Data

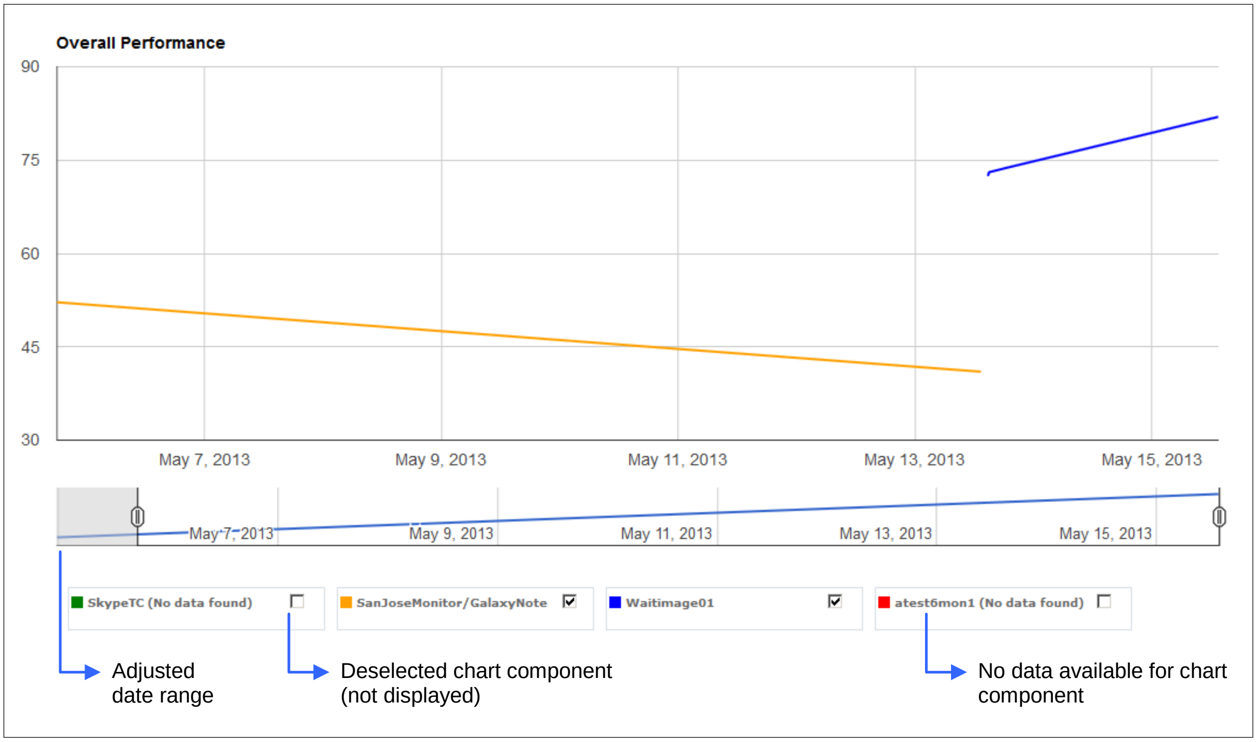
In any chart, you can hover over points to see the associated data value.

Figure 7-1 Hover Over a Graph Line to See Data Points



If a chart has several components, e.g., several monitors are chosen to chart performance, you deselect any component to refresh the chart. You can also use the slider to adjust the beginning and end of the date range for which you are viewing a chart.

Figure 7-2 Adjusting Chart Data



Adjusted date range

Deselected chart component (not displayed)

No data available for chart component

Finally, Enable Auto Refresh automatically refreshes any chart you run with new data from ongoing runs. Pages are refreshed every 10 seconds by default.

Like other reports, charts can be saved.

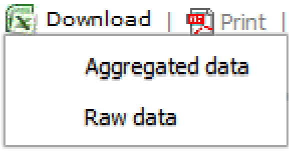
Chart data can be downloaded in aggregated or raw form. Aggregation varies depending on the date range chosen for the chart:

Table 7-1Chart Data Aggregation

Chart Time Range	Aggregation Frequency
0 – 24 hours	No aggregation
1 – 7 days	5 minutes
7 – 31 days	30 minutes
32 – 90 days	3 hours
91 – 180 days	6 hours
180 – 365 days	12 hours
> 365 days	1 day

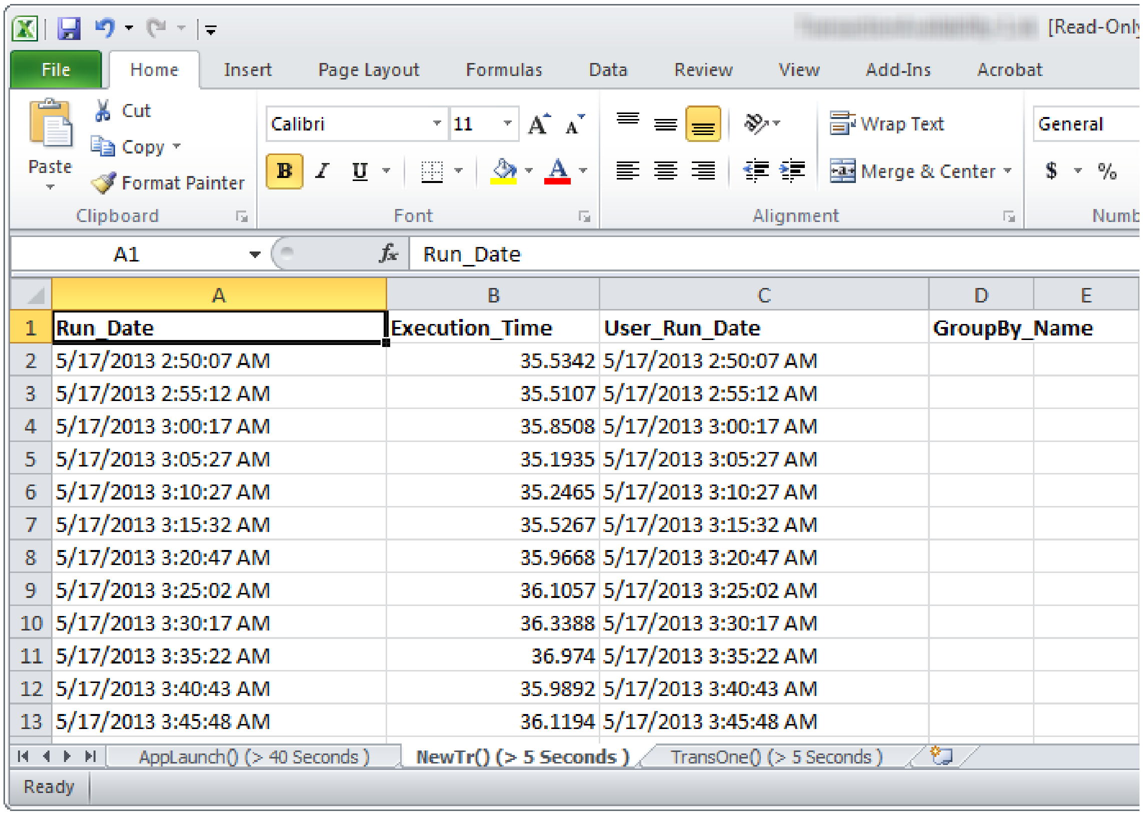
To download data in Excel format, select **Download** and then choose **Aggregated Data** or **Raw Data**.

Figure 7-3 Downloading Chart Data



If you are looking at a chart of comparative performance for several transactions (or monitors), data for each transaction is displayed in a separate sheet.

Figure 7-4 Downloaded Data



	A	B	C	D	E
1	Run_Date	Execution_Time	User_Run_Date	GroupBy_Name	
2	5/17/2013 2:50:07 AM	35.5342	5/17/2013 2:50:07 AM		
3	5/17/2013 2:55:12 AM	35.5107	5/17/2013 2:55:12 AM		
4	5/17/2013 3:00:17 AM	35.8508	5/17/2013 3:00:17 AM		
5	5/17/2013 3:05:27 AM	35.1935	5/17/2013 3:05:27 AM		
6	5/17/2013 3:10:27 AM	35.2465	5/17/2013 3:10:27 AM		
7	5/17/2013 3:15:32 AM	35.5267	5/17/2013 3:15:32 AM		
8	5/17/2013 3:20:47 AM	35.9668	5/17/2013 3:20:47 AM		
9	5/17/2013 3:25:02 AM	36.1057	5/17/2013 3:25:02 AM		
10	5/17/2013 3:30:17 AM	36.3388	5/17/2013 3:30:17 AM		
11	5/17/2013 3:35:22 AM	36.974	5/17/2013 3:35:22 AM		
12	5/17/2013 3:40:43 AM	35.9892	5/17/2013 3:40:43 AM		
13	5/17/2013 3:45:48 AM	36.1194	5/17/2013 3:45:48 AM		

In the image above, there are three spreadsheet tabs for performance data of three transactions, AppLaunch, NewTr, and TransOne. Transaction execution time (Execution_Time) is displayed by the execution timestamp based on the location of the LiveMonitor Server (Run_Date) as well as the time zone of the user (User_Run_Date).

7.4 Availability Charts

Availability charts visually represent the success or failure of a transaction or monitor over a period of time. A value of 100 represents a success while 0 represents a failure. However, when viewing availability over a long period of time, data is aggregated over smaller intervals and then averaged. The resulting data point is then plotted in the chart instead of the individual values of 100 and 0.

7.4.1 Availability over Time

The most basic availability chart shows the success/failure of one or more transactions or monitors over a selected time frame. You can choose more than one item to view a comparison of availability over the same time frame.

To view availability over time from the chart selection dialog box:

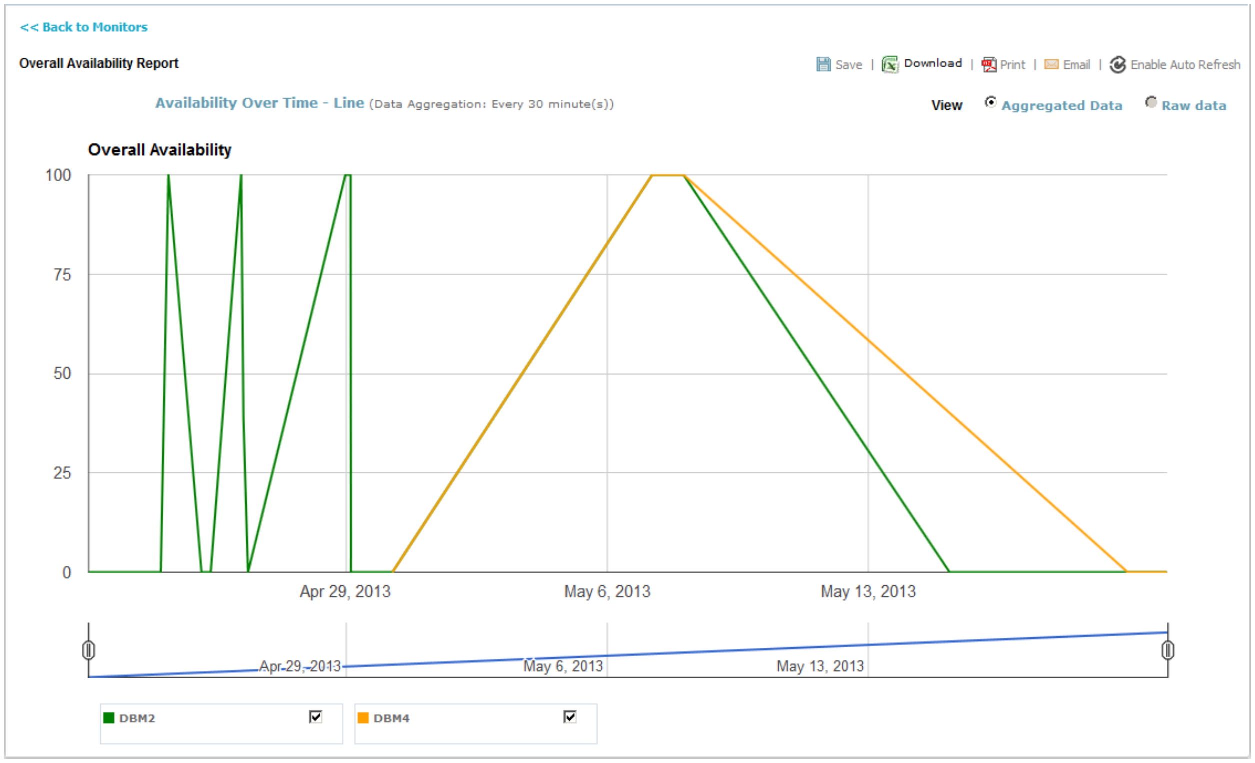
1 Select the **Availability** radio button.

2 Select a **Report Type** (monitors only).

3 Select the **Availability Over Time – Line** from the **Chart Type** drop-down list.

The image below shows the overall availability over several weeks of two monitors. A value of 100 represents a successful run while a value of 0 represents a failed run.

Figure 7-5 Chart: Overall Availability over Time

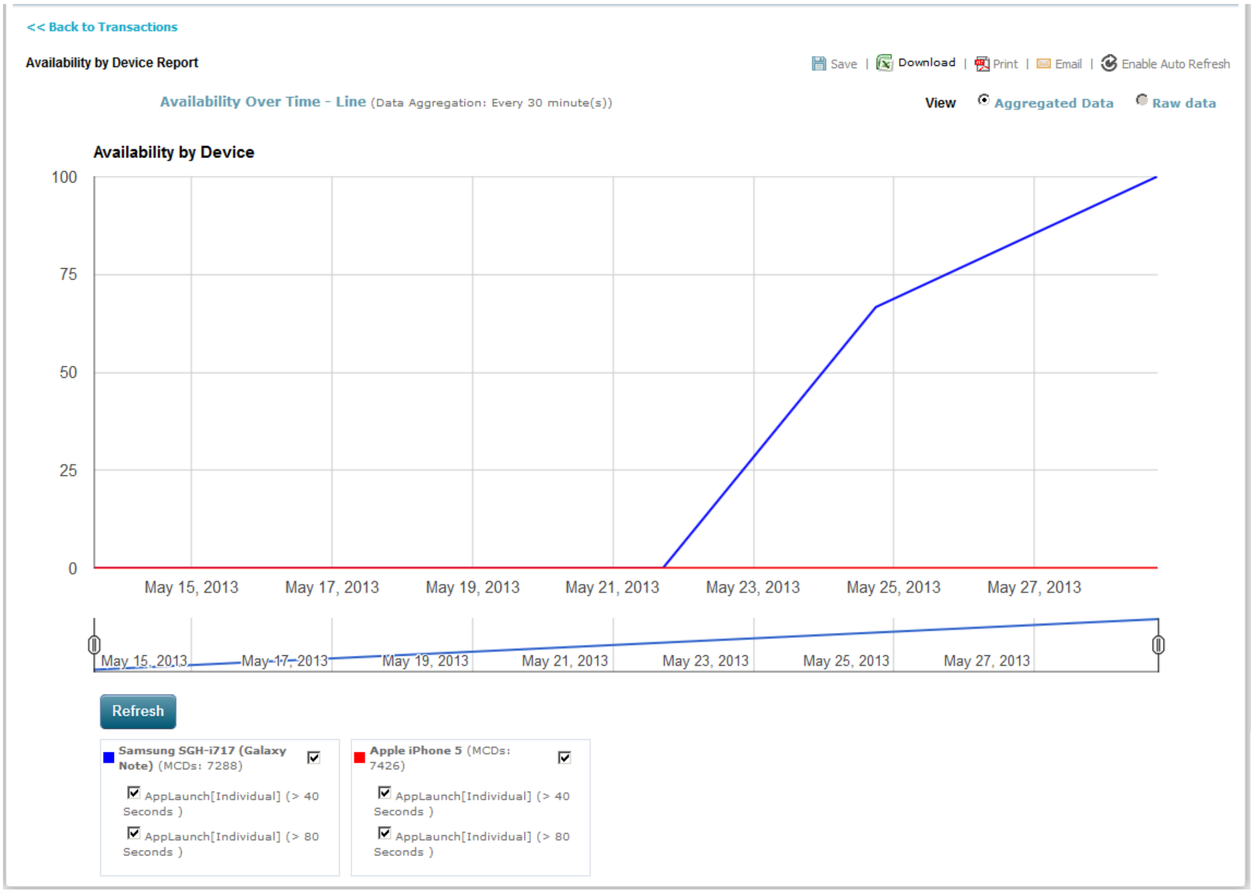


<< Back to Monitors
Overall Availability Report
Save | Download | Print | Email | Enable Auto Refresh
Availability Over Time - Line (Data Aggregation: Every 30 minute(s))
View ● Aggregated Data ○ Raw data
Overall Availability
100
75
50
25
0
Apr 29, 2013
May 6, 2013
May 13, 2013
Apr 29, 2013
May 6, 2013
May 13, 2013
DBM2 ☑
DBM4 ☑

The image below shows availability of a single transaction (but with two different failure thresholds) by device over the span of a few days. Availability on the first device (graphed in blue) is steadily improving over the date range, while availability on the second device (graphed in red) is at 0% through the entire date range.

Data in this chart is aggregated every 30 minutes, which means that if a transaction has more than one run in a given 30-minute interval, its success/failure values are aggregated and averaged into a single data point.

Figure 7-6 Chart: Availability over Time by Device



Availability by Device Report

Availability Over Time - Line (Data Aggregation: Every 30 minute(s))

View ● Aggregated Data ○ Raw data

🟦 Samsung SGH-i717 (Galaxy Note) (MCDs: 7288) ☑

☑ AppLaunch[Individual] (> 40 Seconds)

☑ AppLaunch[Individual] (> 80 Seconds)

🟥 Apple iPhone 5 (MCDs: 7426) ☑

☑ AppLaunch[Individual] (> 40 Seconds)

☑ AppLaunch[Individual] (> 80 Seconds)

7.4.2 Average Availability

Average availability displays the average of all the success (100%) and failure (0%) values for monitor or transaction runs over a period of time. Selecting more than one transaction or monitor allows you to view a comparison of availability in a bar chart.

To view average availability from the chart selection dialog box:

1 Select the **Availability** radio button.

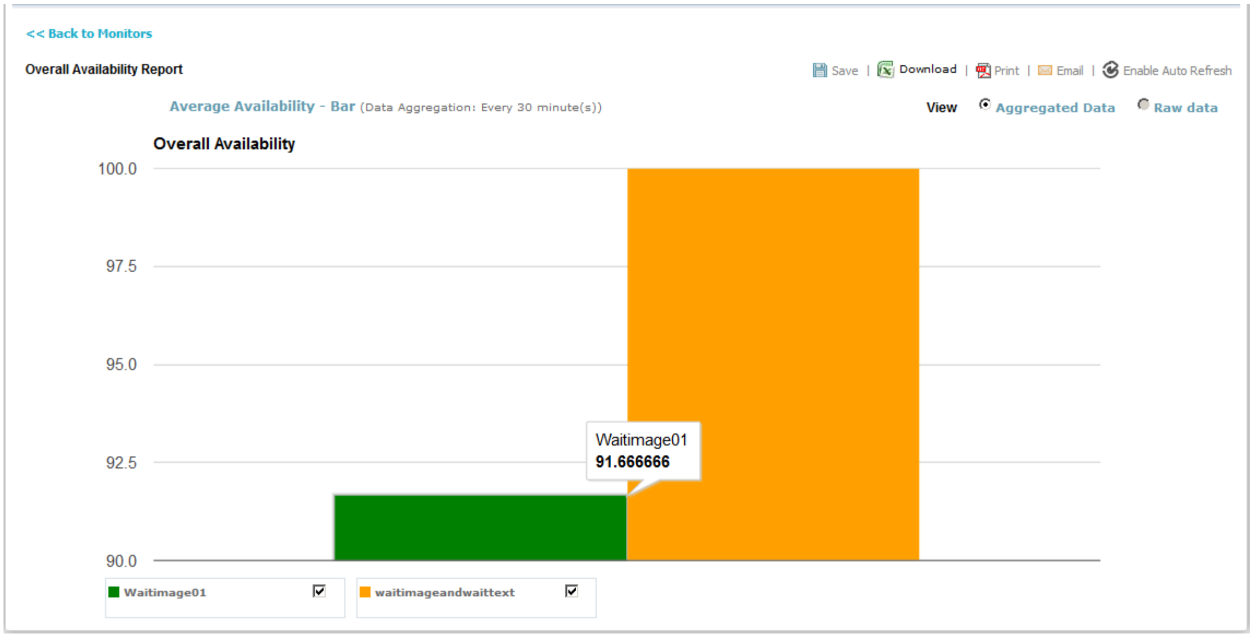
2 Select a **Report Type** (monitors only).

3 Select the **Average Availability – Bar** from the **Chart Type** drop-down list.

The chart below shows the average availability for two monitors—91.67% for one and 100% for the other. In other words, the success rate of the monitor over the time period is interpreted as average availability.

The y axis represents success percentage. You can deselect the check box for either monitor to view a graph with only one monitor's availability.

Figure 7-7 Chart: Average Overall Availability


<< Back to Monitors
Overall Availability Report
Save | Download | Print | Email | Enable Auto Refresh
Average Availability - Bar (Data Aggregation: Every 30 minute(s))
View ● Aggregated Data ○ Raw data
Overall Availability
100.0
97.5
95.0
92.5
90.0
Waitimage01
91.666666
🟩 Waitimage01 ☑
🟧 waitimageandwaittext ☑

7.4.3 Availability by Time of Day

Availability by time of day shows availability for each hour of the day, across all the days in the date range selected. Run result values (100 for success, 0 for failure) are aggregated for each hour across all days and then averaged. The data point for a particular hour, e.g., 12:00., represents average availability of runs in the preceding hour (11 a.m. – 12 p.m.) on all days in the date range, e.g., November 1 – 7.

This chart is useful to view at what times of day availability is impacted, e.g., because of peak traffic.

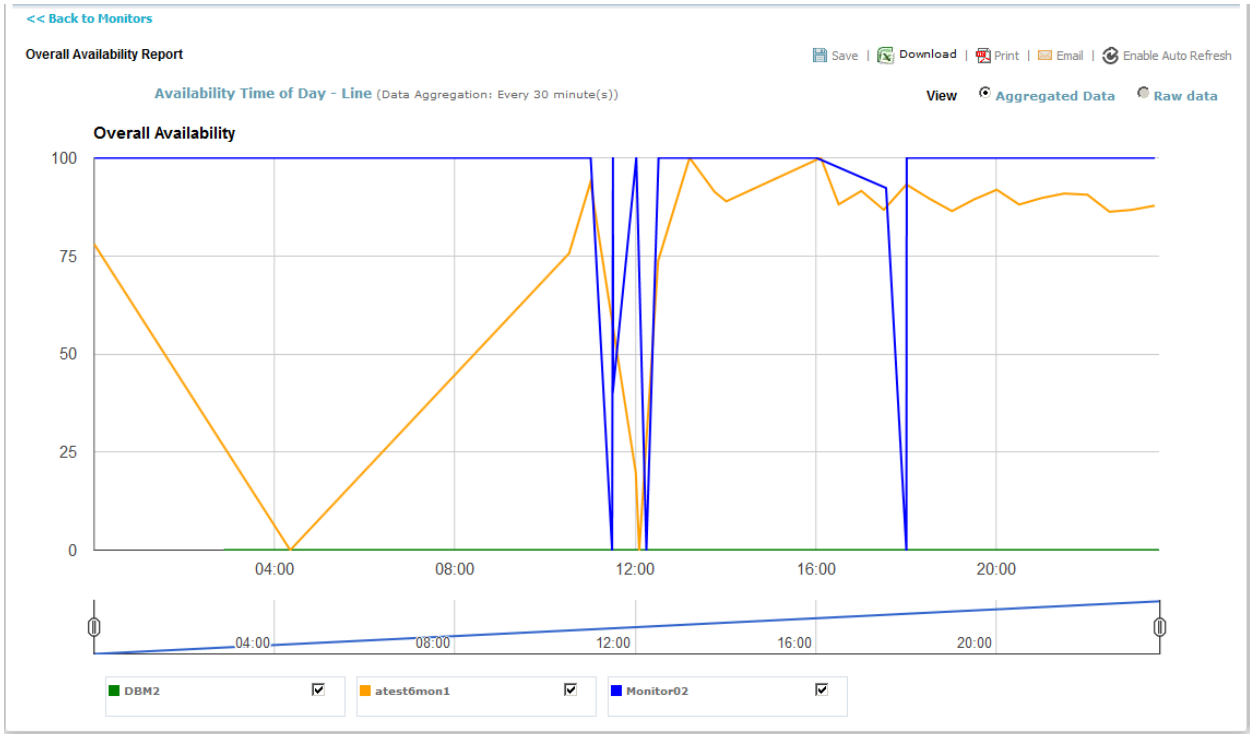
To view availability by time of day from the chart selection dialog box:

1 Select the **Availability** radio button.

2 Select a report type (monitors only).

3 Select the **Availability Time of Day – Line** chart type.

Figure 7-8 Chart: Overall Availability by Time of Day


<< Back to Monitors
Overall Availability Report
Save | Download | Print | Email | Enable Auto Refresh
Availability Time of Day - Line (Data Aggregation: Every 30 minute(s))
View ○ Aggregated Data ○ Raw data
Overall Availability
100
75
50
25
0
04:00
08:00
12:00
16:00
20:00
04:00
08:00
12:00
16:00
20:00
🟩 DBM2 ☑
🟧 atest6mon1 ☑
🟦 Monitor02 ☑

In the figure above, you can see availability for three monitors. The first monitor (green graph) shows a 0% availability over all hours of the day; the second monitor (yellow graph) shows higher availability post noon; the third monitor (blue graph) has perfect availability up to noon, and then after 6:00 p.m.

7.5 Performance Charts

Performance charts show transaction completion times for runs in the selected date range. If there is a lot of data to plot for a long time range, several data points (i.e., transaction completion time) can be aggregated, averaged, and displayed as a single chart entry. The time period for data aggregation, if any, is displayed above the chart.

7.5.1 Performance over Time

The performance chart over a period of time for a monitor shows completion times, plotted together, for all transactions in the monitor. A data point in the graph for monitor performance over time can represent the run time of any of the transactions contained in the monitor. You can select several monitors to be displayed in a comparative chart of transaction completion times. This information is especially useful when the monitors use the same transactions.

A performance over time chart for transactions shows the completion times of each transaction, across all the monitors it appears in, over the selected date range.

To view performance over time from the chart selection dialog box:

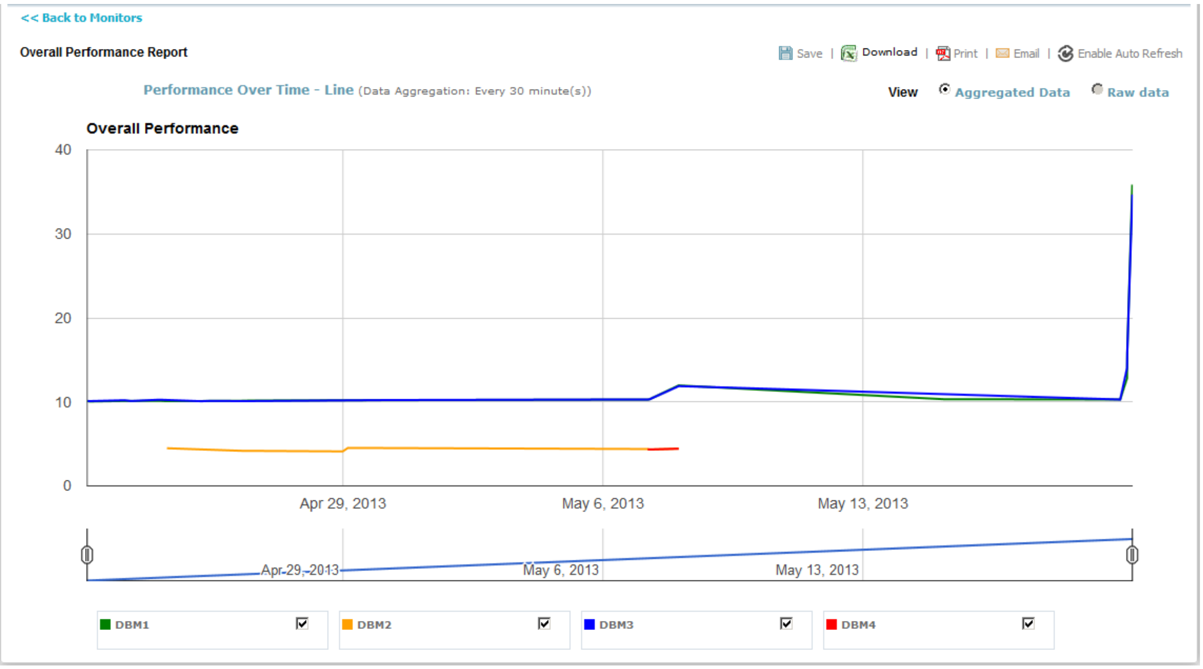
1 Select the **Performance** radio button.

2 Select a **Report Type** (monitors only).

3 Select the **Performance Over Time – Line** from the **Chart Type** drop-down list.

The image below shows the performance of four monitors. Two monitors (graphed in blue and green) show consistently higher transaction run times.

Figure 7-9 Chart: Overall Performance over Time



<< Back to Monitors

Overall Performance Report

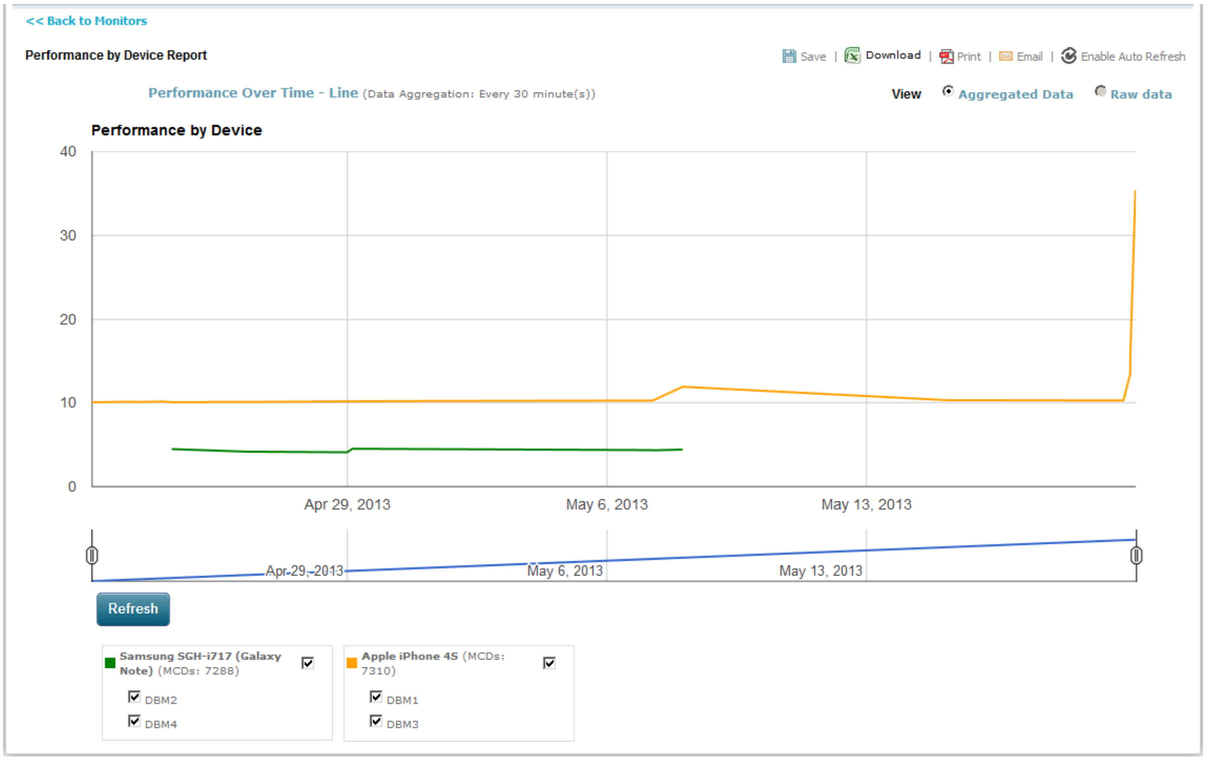
Performance Over Time - Line (Data Aggregation: Every 30 minute(s))

View ● Aggregated Data ○ Raw data

🟩 DBM1 ☑ 🟧 DBM2 ☑ 🟦 DBM3 ☑ 🟥 DBM4 ☑

The figure above shows performance of the same four monitors by device. Different colored graph lines for each device clearly show differences in performance (transaction completion times).

Figure 7-10 Chart: Performance over Time by Device



<< Back to Monitors

Performance by Device Report

Performance Over Time - Line (Data Aggregation: Every 30 minute(s))

View ● Aggregated Data ○ Raw data

🟩 Samsung SGH-i717 (Galaxy Note) (MCDs: 7288) ☑
☑ DBM2
☑ DBM4

🟧 Apple iPhone 4S (MCDs: 7310) ☑
☑ DBM1
☑ DBM3

7.5.2 Average Performance

The average performance chart over a period of time for a monitor shows the average completion times for all transactions in the monitor taken together. You can select several monitors to be displayed in a comparative chart of average transaction completion times. This information is especially useful when the monitors use the same transactions.

An average performance chart for transactions shows the average completion time of each transaction over the selected date range.

To view average performance from the chart selection dialog box:

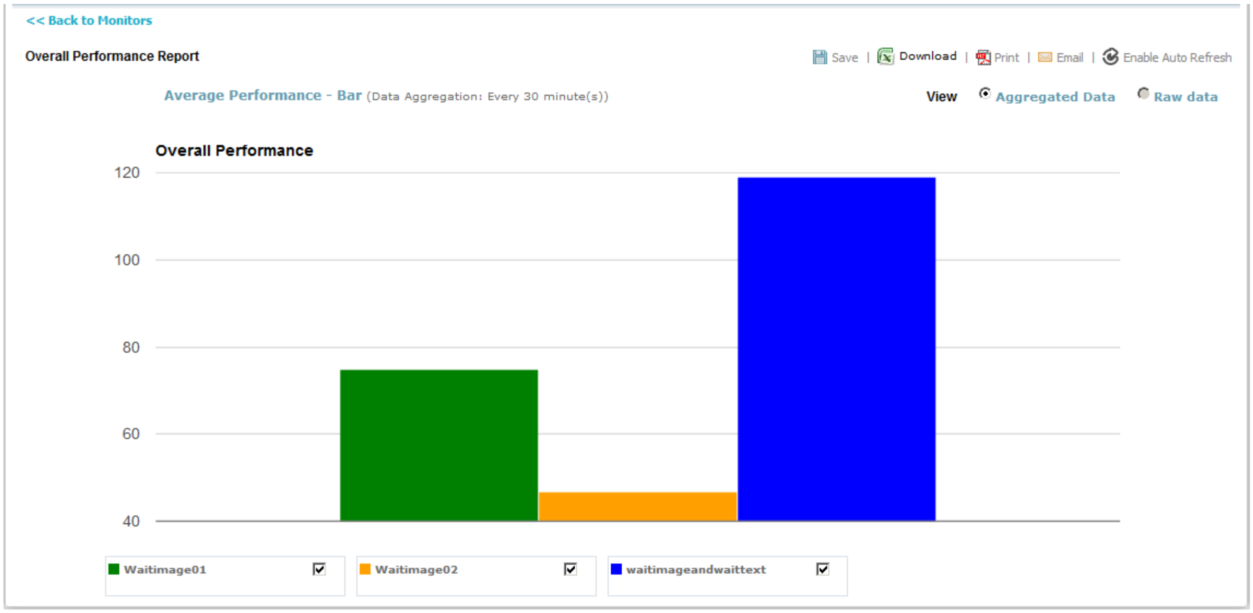
1 Select the **Performance** radio button.

2 Select a **Report Type** (monitors only).

3 Select the **Average Performance – Bar** from the **Chart Type** drop-down list.

The image below shows average performance of three monitors that use the same transaction. The y axis represents transaction completion times (performance) in seconds.

Figure 7-11 Chart: Average Overall Performance



Overall Performance Report

Average Performance - Bar (Data Aggregation: Every 30 minute(s))

View ● Aggregated Data ○ Raw data

To facilitate comparison, you can refresh the chart by comparing fewer monitors.

7.5.3 Performance by Time of Day

Performance by time of day shows performance for each hour of the day, across all the days in the date range selected. Transaction run times are aggregated for each hour across all days and then averaged. The data point for a particular hour, e.g., 7 a.m., represents average availability of runs in the preceding hour (6 a.m. – 7 a.m.) on all days in the date range, e.g., November 1 – 7.

This chart is useful to view at what times of day performance is impacted, e.g., because of peak traffic.

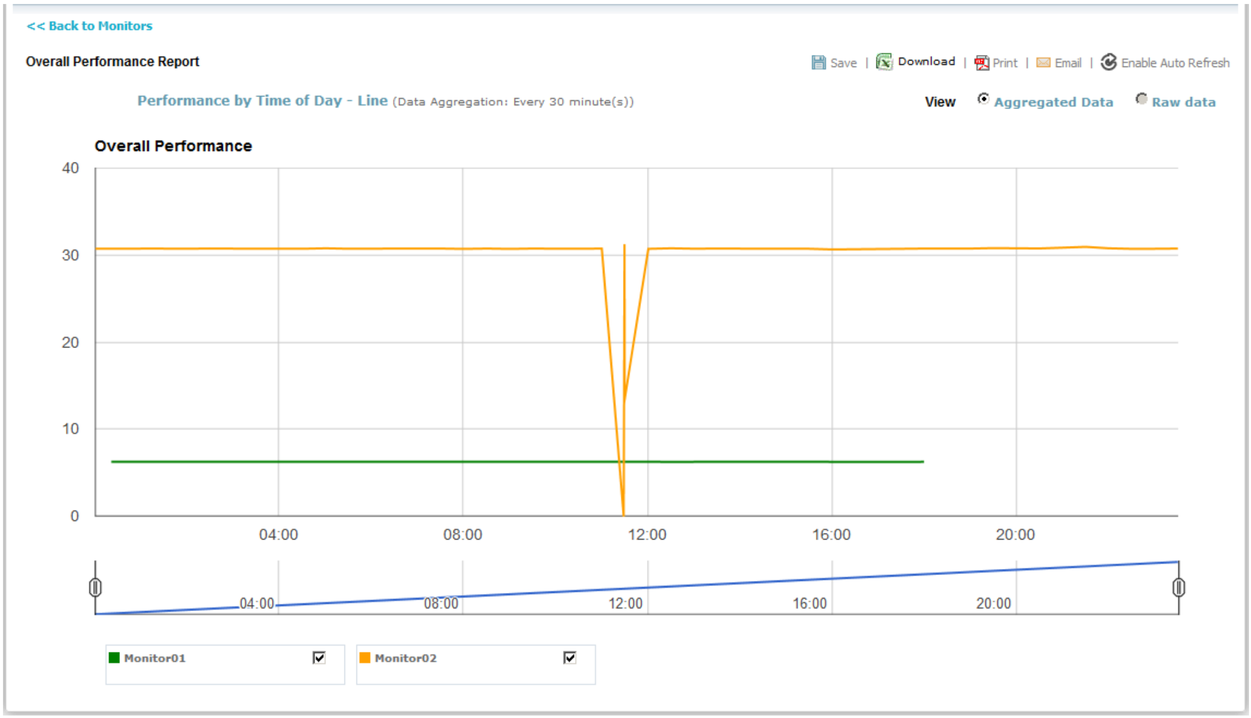
To view performance by time of day from the chart selection dialog box:

1 Select the **Performance** radio button.

2 Select a report type (monitors only).

3 Select the **Performance by Time of Day – Line** chart type.

Figure 7-12 Chart: Overall Performance by Time of Day


<< Back to Monitors
Overall Performance Report
Save | Download | Print | Email | Enable Auto Refresh
Performance by Time of Day - Line (Data Aggregation: Every 30 minute(s))
View ● Aggregated Data ○ Raw data
Overall Performance
40
30
20
10
0
04:00
08:00
12:00
16:00
20:00
04:00
08:00
12:00
16:00
20:00
🟩 Monitor01 ☑
🟧 Monitor02 ☑

In the figure above, you can see hourly performance for two monitors. For the first monitor (green graph), performance by time of day does not vary at all. The second monitor experiences performance irregularity around midday. You can clearly see the difference in actual run times.

7.6 Candlestick Charts

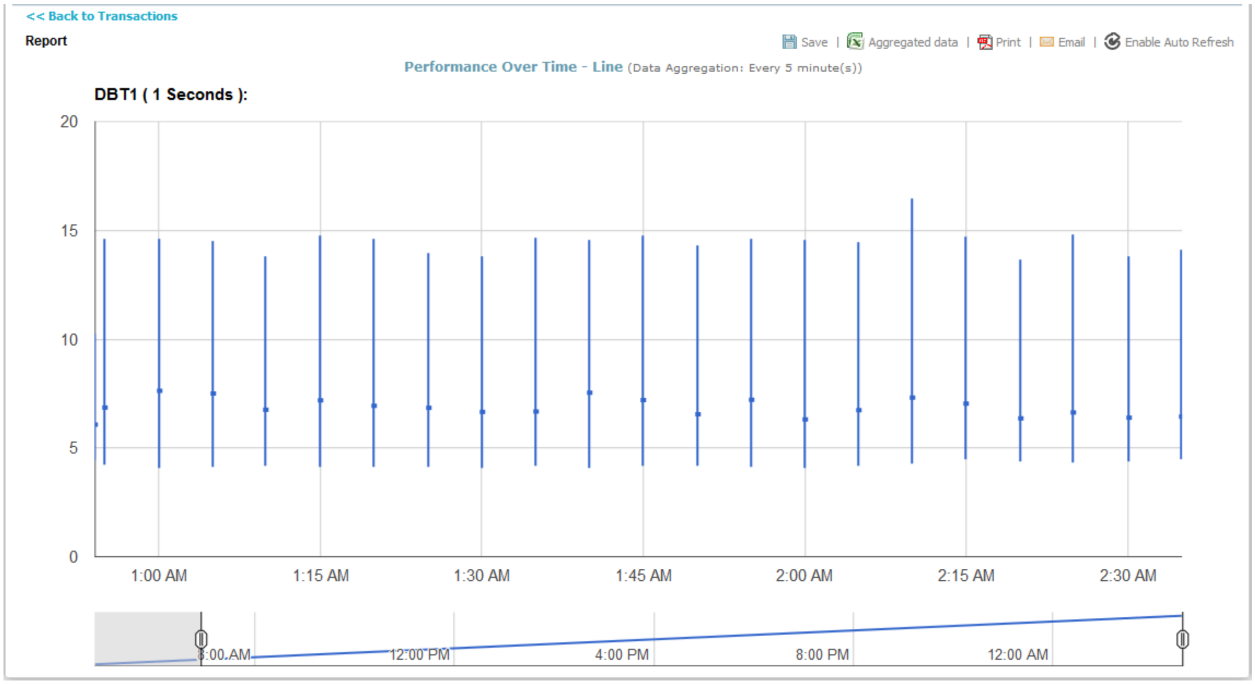
A candlestick chart shows the maximum, minimum, and average run time for a transaction at different points in the day over a date range. You can view a candlestick chart for one transaction at a time:

1 Select the **Transactions** tab.

2 Ensure that you are viewing a date range of at least two days.

3 Click the **View** link (in the Candlestick column) for a transaction in the transaction summary.

Figure 7-13 Candlestick Chart



8 Saving Reports and Criteria

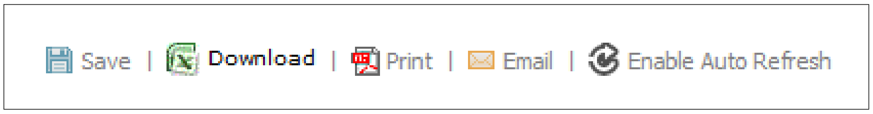
At various points in the DAE Monitoring portal, you can save one-time, ad hoc reports (i.e., graphs and raw or aggregated data) or you can save report criteria in order to schedule reports for periodic generation.

- The Saved Reports tab displays one-time reports that you have saved.
- The Manage Criteria tab displays report criteria you have saved. In this tab, you can edit and schedule criteria for periodic report generation and delivery.

8.1 Saving and Viewing Reports

To save a report, as it appears with filters applied and date ranges customized:

1 Click **Save** at the top-right corner of the page you wish to save.



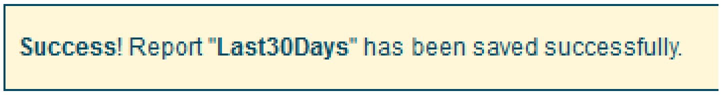
NOTE This command does not appear on all pages in the DAE Monitoring Portal. You can save the following monitor or transaction charts and reports:

- Availability
- Performance
- Summary

2 From the dialog box that appears (see Figure 8-1, select the **Report** radio button.

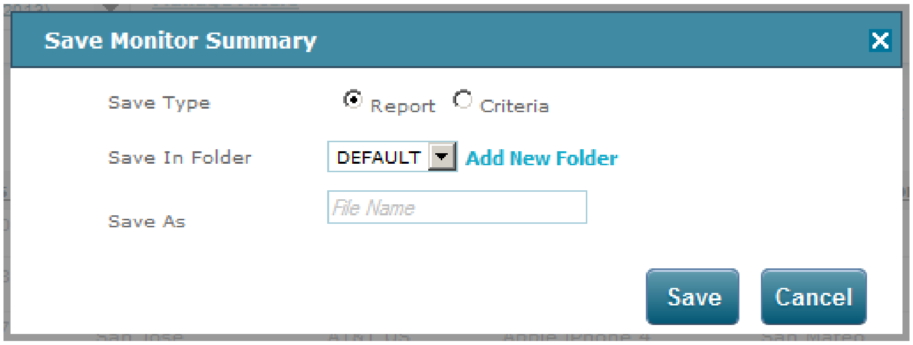
3 Optionally, create a folder in which to save the report (**Add New Folder** > enter a name > **Add**). Or leave your report in the **DEFAULT** folder.

4 Enter a name for the report and click **Save**. This name identifies your report in the **Saved Reports** tab. A message indicates that your report has been saved successfully.



Success! Report "Last30Days" has been saved successfully.

Figure 8-1 Saving a Report



Save Type ● Report ○ Criteria

Save In Folder DEFAULT

Save As File Name

Reports are saved as they appear on your screen, i.e., with any filters applied after they are first generated. Reports are saved as PDF files.

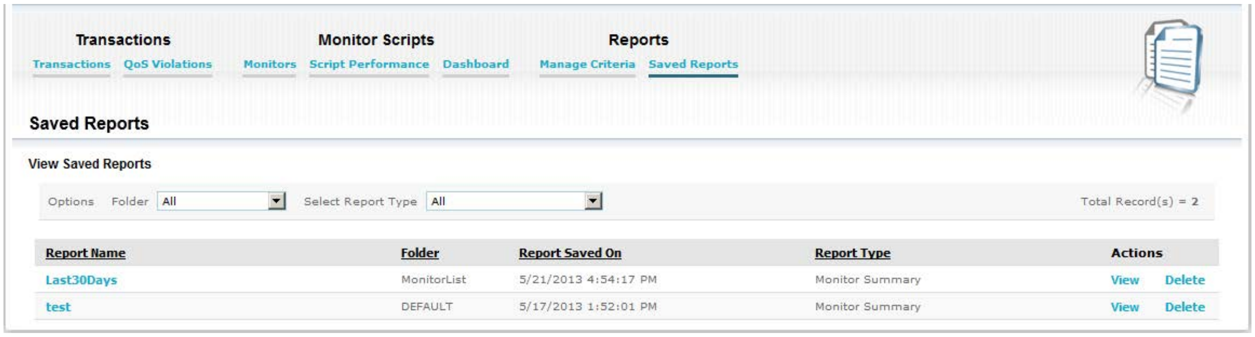
To view a saved report:

1 Select the **Saved Reports** tab (see Figure 8-2).

2 Optionally, filter the list of reports by **Report Type** or **Folder** name. Saved report types can include monitor or transaction availability, performance, or summaries.

3 Click a report name or click **View** to open the PDF file. (You can also **Delete** a saved report.)

Figure 8-2 Saved Reports Tab



Saved Reports

View Saved Reports

Options Folder All Select Report Type All Total Record(s) = 2

Report Name	Folder	Report Saved On	Report Type	Actions
Last30Days	MonitorList	5/21/2013 4:54:17 PM	Monitor Summary	View Delete
test	DEFAULT	5/17/2013 1:52:01 PM	Monitor Summary	View Delete

8.2 Saving Report Criteria

If there is a report that you view often, you can save the report criteria, including any custom filters you apply, and have it scheduled for periodic generation and delivery by email. You can also generate reports from the saved criteria at any time.

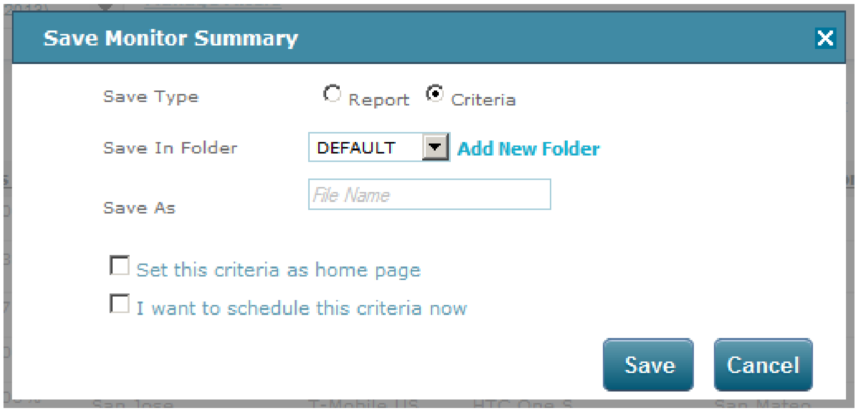
To save report criteria:

1 View or generate your summary, availability, or performance report.

2 Apply filters to adjust your report criteria.

3 Click **Save** at the top-right corner of the page.

4 From the dialog box that appears, select the **Criteria** radio button.



Save Type ○ Report ● Criteria

Save In Folder DEFAULT

Save As File Name

□ Set this criteria as home page

□ I want to schedule this criteria now

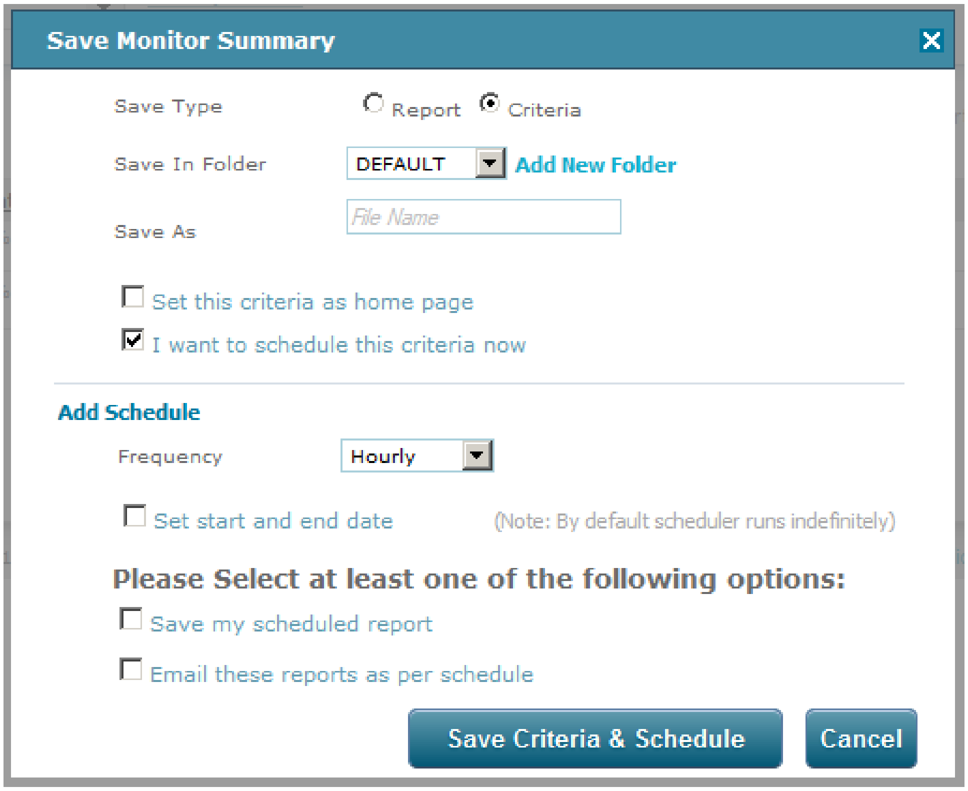
5 Optionally, create a folder in which to save the criteria (**Add New Folder** > enter a name > **Add**). Or leave your criteria in the **DEFAULT** folder.

6 Enter a name for the report criteria.

7 Optionally, check **Set this criteria as home page**. You will then see the report generated from these criteria when you log back in to the DAE Monitoring Portal.

8 Optionally, check **I want to schedule this criteria now** to schedule your criteria. You will see options to set up a report generation schedule, save generated reports, and email generated reports.

Whether scheduling report generation while saving criteria or later, in the **Manage Criteria** tab, the steps for doing so are the same. Filling out this dialog box to schedule reports is discussed in Scheduling Report Generation below.



Save Monitor Summary

Save Type ○ Report ● Criteria

Save In Folder DEFAULT

Save As File Name

□ Set this criteria as home page

☑ I want to schedule this criteria now

Add Schedule

Frequency Hourly

□ Set start and end date (Note: By default scheduler runs indefinitely)

Please Select at least one of the following options:

□ Save my scheduled report

□ Email these reports as per schedule

9 To finish, click **Save Criteria & Schedule**, or if not scheduling your criteria right away, click **Save**.

8.3 Manage Criteria Tab

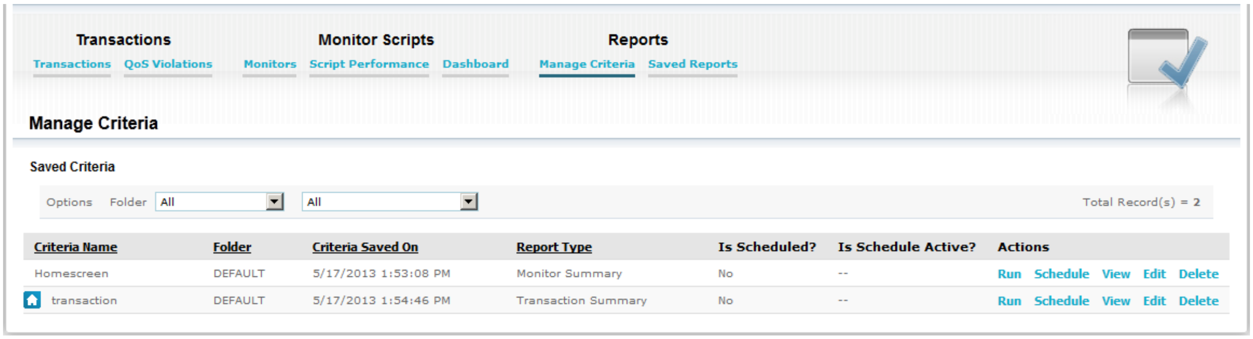
The **Manage Criteria** tab in the Reports view displays saved report criteria. From this tab, you can run reports instantly, schedule report generation, edit criteria, or delete saved criteria.

To view saved criteria:

1 Select **Manage Criteria** (see Figure 8-3 below).

2 Optionally, filter the list of criteria by **Report Type** or **Folder** name. Saved report types can include monitor or transaction availability, performance, or summaries. Criteria set as your home page are displayed with an identifying icon.

Figure 8-3 Saved Criteria in ***Manage Criteria***



Manage Criteria

Saved Criteria

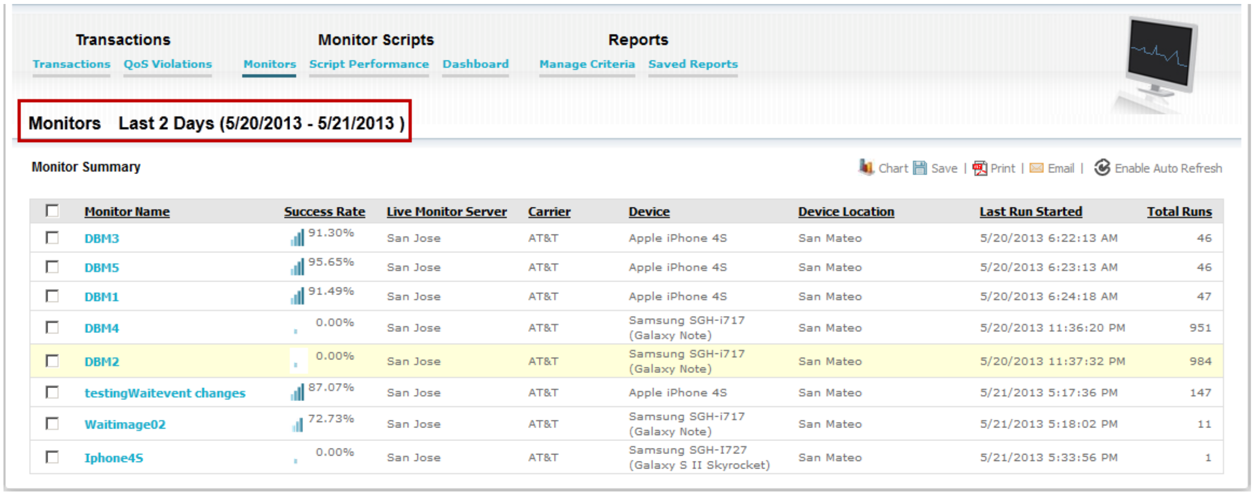
Options Folder All All Total Record(s) = 2

Criteria Name	Folder	Criteria Saved On	Report Type	Is Scheduled?	Is Schedule Active?	Actions
Homescreen	DEFAULT	5/17/2013 1:53:08 PM	Monitor Summary	No	--	Run Schedule View Edit Delete
transaction	DEFAULT	5/17/2013 1:54:46 PM	Transaction Summary	No	--	Run Schedule View Edit Delete

8.3.1 Running and Deleting Criteria

Click **Run** next to saved criteria to run a report instantly. A report/chart is generated, clearly displaying the time frame saved as part of report criteria:

Figure 8-4 Running a Report from Saved Criteria



Monitors Last 2 Days (5/20/2013 - 5/21/2013)

Monitor Summary

□	Monitor Name	Success Rate	Live Monitor Server	Carrier	Device	Device Location	Last Run Started	Total Runs
□	DBM3	91.30%	San Jose	AT&T	Apple iPhone 4S	San Mateo	5/20/2013 6:22:13 AM	46
□	DBM5	95.65%	San Jose	AT&T	Apple iPhone 4S	San Mateo	5/20/2013 6:23:13 AM	46
□	DBM1	91.49%	San Jose	AT&T	Apple iPhone 4S	San Mateo	5/20/2013 6:24:18 AM	47
□	DBM4	0.00%	San Jose	AT&T	Samsung SGH-i717 (Galaxy Note)	San Mateo	5/20/2013 11:36:20 PM	951
□	DBM2	0.00%	San Jose	AT&T	Samsung SGH-i717 (Galaxy Note)	San Mateo	5/20/2013 11:37:32 PM	984
□	testingWaitevent changes	87.07%	San Jose	AT&T	Apple iPhone 4S	San Mateo	5/21/2013 5:17:36 PM	147
□	Waitimage02	72.73%	San Jose	AT&T	Samsung SGH-i717 (Galaxy Note)	San Mateo	5/21/2013 5:18:02 PM	11
□	Iphone4S	0.00%	San Jose	AT&T	Samsung SGH-I727 (Galaxy S II Skyrocket)	San Mateo	5/21/2013 5:33:56 PM	1

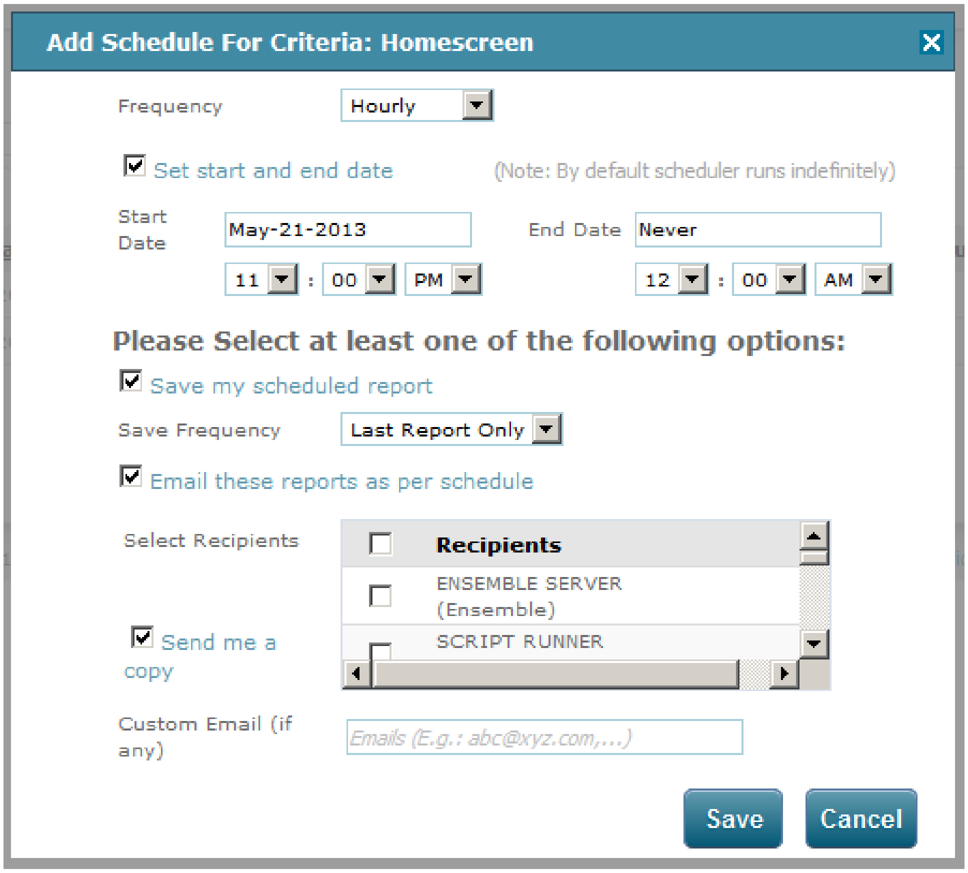
To delete a set of saved criteria, click the **Delete** link displayed for the criteria.

8.3.2 Scheduling Report Generation

Scheduling report generation from criteria can be done at two points in the DAE Portal:

- In the dialog box displayed while saving report criteria
- By clicking **Schedule** next to saved criteria in the **Manage Criteria** tab

Figure 8-5 Interface for Scheduling Report Generation



Add Schedule For Criteria: Homescreen

Frequency: Hourly

☑ Set start and end date (Note: By default scheduler runs indefinitely)

Start Date: May-21-2013 11 : 00 PM

End Date: Never 12 : 00 AM

Please Select at least one of the following options:

☑ Save my scheduled report

Save Frequency: Last Report Only

☑ Email these reports as per schedule

Select Recipients

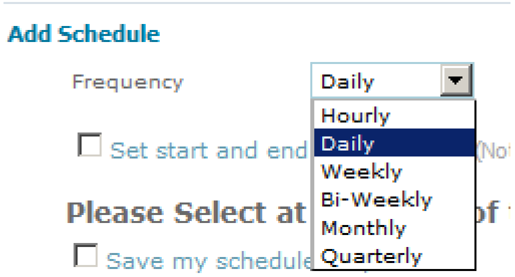
□	Recipients
□	ENSEMBLE SERVER (Ensemble)
□	SCRIPT RUNNER

☑ Send me a copy

Custom Email (if any): Emails (E.g.: abc@xyz.com,...)

The steps for scheduling report generation are the same in both cases:

1 Select a report generation **Frequency** (e.g., **Hourly**, **Daily**, **Weekly**, **Bi-Weekly**, **Monthly**, or **Quarterly**).



Add Schedule

Frequency: Daily

□ Set start and end

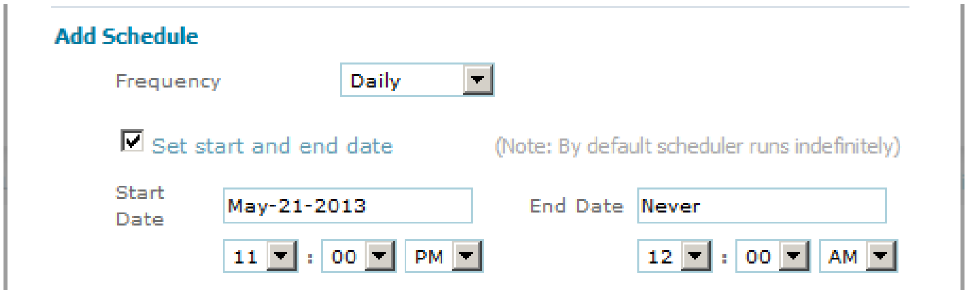
Please Select at

□ Save my schedule

2 Optionally, check **Set start and end date** to set a period for report generation. If you do not specify a period, reports are generated indefinitely.

NOTE This period is different from the date range covered in your report. For example, you could save criteria for a transaction summary report for a period of 7 days. You could have it generated and mailed to you daily over a period of 3 months.

3 Enter a **Start Date** and time and **End Date** and time using the controls provided.



Add Schedule

Frequency: Daily

☑ Set start and end date (Note: By default scheduler runs indefinitely)

Start Date: May-21-2013 11 : 00 PM

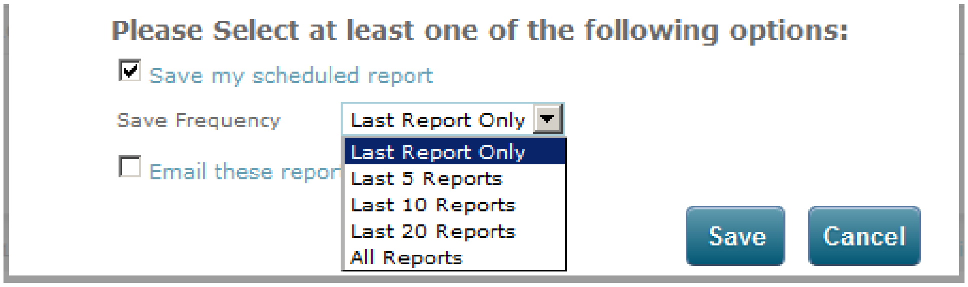
End Date: Never 12 : 00 AM

4 Save and/or have the generated reports emailed to you.

To have reports saved to the DAE Portal:

a Check **Save my scheduled report**.

b From the drop-down list that appears, choose how many of the most recent reports you would like saved to the DAE Portal.



Please Select at least one of the following options:

☑ Save my scheduled report

Save Frequency: Last Report Only

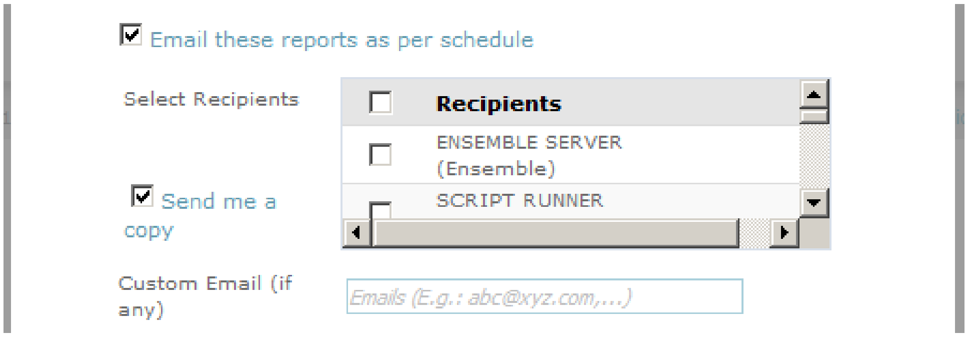
☐ Email these repor

To have reports emailed:

c Check **Email these reports as per schedule**.

d Select email recipients—report emails can be sent to users in your DAE Monitoring environment or to other write-in addresses.

e Optionally, email report copies to yourself.



☑ Email these reports as per schedule

Select Recipients

☐	Recipients
☐	ENSEMBLE SERVER (Ensemble)
☐	SCRIPT RUNNER

☑ Send me a copy

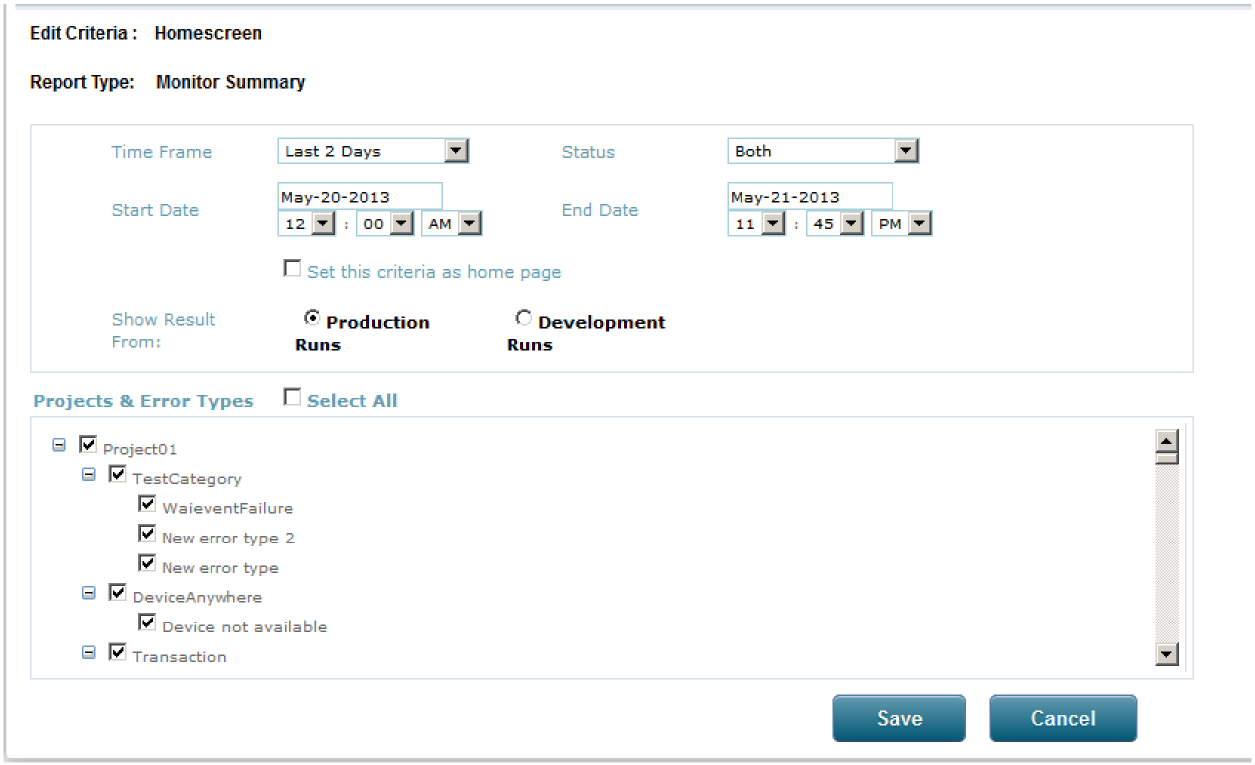
Custom Email (if any): Emails (E.g.: abc@xyz.com,...)

5 To finish, click **Save Criteria & Schedule** (while saving criteria) or **Save** (in the **Manage Criteria** tab).

8.3.3 Viewing and Editing Criteria

To edit a set of saved criteria for report generation, click **Edit** next to it. You will see a panel enabling you to edit the set of saved criteria.

Figure 8-6 Editing Saved Report Criteria



Edit Criteria : Homescreen

Report Type: Monitor Summary

Time Frame: Last 2 Days

Status: Both

Start Date: May-20-2013 12 : 00 AM

End Date: May-21-2013 11 : 45 PM

□ Set this criteria as home page

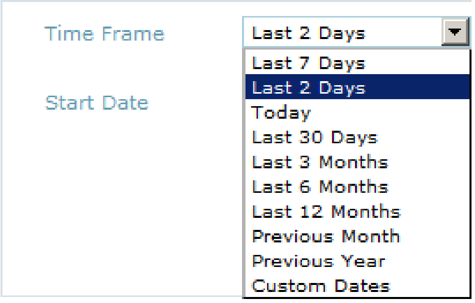
Show Result From: ● **Production Runs** ○ **Development Runs**

Projects & Error Types □ **Select All**

- ☑ Project01
  - ☑ TestCategory
    - ☑ WaieventFailure
    - ☑ New error type 2
    - ☑ New error type
  - ☑ DeviceAnywhere
    - ☑ Device not available
  - ☑ Transaction

The editable fields are:

- Run type—of monitors selected for the report—you can choose **Production Runs** or **Development Runs**.
- **Time Frame**—time period over which data is gathered for the report—for example, a monitor summary for the **Last 30 Days** looks at production or development runs over the preceding 30 days.



Time Frame: Last 2 Days

Start Date

- **Start Date** and **End Date** and time—of the **Time Frame** of the report

NOTE If you manually change the **Start** or **End Date**, the **Time Frame** changes to **Custom Dates**.

- **Projects & Error Types**—if you deselect a project, any monitors/transactions in that project are filtered out.

  Check boxes for error types and categories only appear in criteria for monitor reports. If you deselect an error category, monitor runs that triggered errors from that category are filtered out. If you deselect an error type, monitor runs that triggered that error type are filtered out.

Save your changes to report criteria or click **Cancel** to exit the screen.