



Version 22

Administration Guide

Copyright © 2022 Bocada LLC. All Rights Reserved. Bocada and BackupReport are registered trademarks of Bocada LLC. Vision, Prism, vpConnect, and the Bocada logo are trademarks of Bocada LLC. Other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

Protected by U.S patents 6,640,217; 6,708,188; 6,745,210; 7,457,833; 7,469,264; 7,496,614; 8,407,227

The material in this manual is for information only and is subject to change without notice. While efforts have been made to ensure accuracy, Bocada LLC assumes no liability resulting from errors or omissions in this document, or from the use of information contained herein.

Bocada LLC reserves the right to make changes in the product design and documentation without reservation and without notification to its users. 20201009

Contents

Introduction	8
Architecture	8
Bocada Database.....	8
Recovery Model	8
Bocada User Interface Application	8
Supported Browsers.....	9
Note:	9
Bocada Data Collection Service (DCS).....	9
Processes.....	9
Supported Data Protection Products	9
User Role Definitions	9
Administrators	9
Operators	10
Standard Users.....	10
Unit Calculation.....	11
Alerting & Incidents Module	11
Alerting & Incidents : Alert Config	11
Alert Criteria.....	13
Create an Alert	15
Edit an Alert	17
Configuration Module.....	17
Configuration : Data Collection.....	17
Update Status.....	18
Update Detail	19
Manual Data Collection.....	20
Configuration : Backup Servers.....	23
Add/Edit Servers	23
Servers Tab, which appears as the Backup Product Name after a server has been added.....	23
Schedules Tab	25
Settings Tab.....	26
Finish Tab	27
Configuration : Backup Clients.....	29
Client Properties	29
Ignore Client.....	30
Run Rules.....	30
Target Renaming	30

Configuration : Schedules	32
Configuration : Scheduled Report Management	32
Configuration : Advanced Config : Data Collection Alert Activity	32
Configuration : Advanced Config : Data Collection Servers	33
Configuration : Advanced Config : Scheduled Actions.....	33
Configuration : Advanced Config : Backup Server Groups.....	33
Configuration : Advanced Config : Backup Server Activity	33
Administration Module	34
Administration : Users	34
Adding users.....	34
Assign Reports.....	36
User Zone Assignment	36
Administration : Zones	37
Definitions and Rules	37
Add Zones	37
Zone Types	37
Assign Clients	38
Administration : Settings	38
License: Click to view license agreement:.....	38
Edit General Settings.....	39
Maintenance Tab	39
Prune Outdated Updates	40
Prune Outdated Logs	41
Prune Outdated Backup Clients	41
Prune Orphan Assets.....	41
Prune Auto Saved Reports	41
Prune Saved Reports	41
Prune Outdated Snapshot Files	41
Prune Database Maintenance Window	42
Maximum Rows Pruned per Attempt	42
Maintenance Schedule	42
Global Report Settings Tab	42
Time Zone.....	43
Error Set	43
Success for Zero Bytes and Zero Errors.....	44
Backup Day.....	44
Export Settings	44
Inactive clients	44
Custom Logo	44
Zone Enforcement.....	45
Time Zone Auto-zoning	46
Re-Zoning Clients to a New Time Zone	47

User Error Categories Tab	47
Add an Error Code	48
Delete an Error Code	48
Edit an Error code	48
Rename an Error Category Name	48
Defining Treatment of Error Category	48
Email Settings Tab	48
Application Tab	50
SQL Connection	50
Application Settings	50
License Keys	50
License Key Values	50
License Warnings	51
Scheduled License Count Email	51
SLA Tab	51
Collection Tab	51
Data Collection Process	52
Data Collection Settings	52
Web Server Tab	53
Administration : Rules	53
Rule Order	54
Run All Rules	55
Add, Edit and Copy Rules	55
Client Recognition	57
Client Assignment	58
Rules Schedule	58
Administration : Rule Groups	58
Administration : License Count	58
Advanced Module	58
Advanced : Report Usage	58
Advanced : Settings Tabular	59
Advanced : Rules Audit	59
Advanced : Custom SQL : SQL Queries	59
Advanced : Custom SQL : Custom SQL Templates	60
How to Add a New Custom SQL Template Report	61
Custom SQL Criteria	62
Advanced : SLA	63
Workflow Overview	63
Advanced : SLA : SLA Trends & Advanced : SLA : SLA Metrics	63

Advanced : SLA : SLA Config.....	64
Levels.....	64
Definitions and Rules	64
Add SLA Profile.....	65
Edit SLA Profile.....	65
Assign Backup Clients.....	65
Advanced : Policies	66
Advanced : Policies : TSM Policy Reports.....	66
Advanced : Policies : NBU Policy Reports	66
Advanced : Policies : Change Analysis.....	66
Advanced : Policies : NBU SLP (Storage LifeCycle Policy).....	66
Other Reporting Modules	66
Contacting Bocada	67
Bocada Customer Support	67
Bocada Professional Services.....	67
Bocada Finance	67
Appendices.....	68
Appendix A: Server Processes.....	68
Data Collector Processes.....	68
Application Server Processes	68
Appendix B: Error Definitions	70
Appendix C: Writing Your Own Custom SQL Reports	72
Running a Custom SQL Report.....	72
Custom Report Administration:	72
Date/Time Controls:.....	72
Report Criteria.....	73
Processing Simple Criteria.....	74
Processing Multi-Valued Criteria	74
Zones and Backup Clients	74
Filtering, Sorting and Grouping.....	75
Error Handling	75
Custom Report for Debugging	76
Example Custom Report	76
Troubleshooting Limitations	78
Appendix D: Maintenance: Tables Pruned	79
Tables Pruned by Maintenance Control Type.....	79
Backup Data Tables:.....	80
Storage Data Tables:	80
Media Data Tables:	80
Weekly Summaries Tables:	80
Monthly Summaries Tables:	80
Server Messages Tables:	80

Backup Events Tables:.....	80
Activity Log Retention Tables:.....	80
Clients Retention Tables:	81
Orphan Assets Retention Tables:.....	81
Auto Saved Reports Retention Tables:	81
Saved Reports Data Tables:	82
Outdated Requests Tables:	82
Deleted Server Tables:	83
Media Server with no associated media mount, media log, or media device inventory Tables:...	83
Deleted Alerts Tables:	83
Policy Orphan data with no associated data in any table with FK dependency Tables:.....	84
Appendix E: Parameters in the Bocada Database:	85
Master Bocada Application Server.....	85
The below features are set in the table zparams	85
MaxReportDays:.....	85
Appendix F: Bocada Website IIS Timeout Settings	88
Appendix G: Bocada License Unit Count.....	93

Introduction

This guide is intended for Administrators and Operators who configure and manage Bocada installations. Through this guide, you will become familiar in detail on how to setup, configure, and manage Bocada to meet your operational goals.

For installation and system configuration requirements please see the *Bocada Install Guide*. For information on adding specific backup products or other integrations to Bocada, please see the associated Bocada Plugin Guide. This Administration Guide does not cover in detail the complete reporting functionality of Bocada. For more information, please refer to the *Bocada Reporting Guide*. For a list of backup products and integrations supported by Bocada please see Bocada Backup Product Version Support Matrix.

Bocada product documentation is publicly available on the Bocada Support web site <https://bocada-support.force.com/>.

Architecture

Components of the Bocada tool can be installed on a single server or distributed across multiple servers to ensure maximum flexibility and scalability. As your environment grows, additional components can be added to accommodate increased capacity while maintaining performance. The following components comprise the Bocada architecture:

Bocada Database

A Microsoft SQL Server database is the core of the Bocada architecture. The database stores data collected from backup servers along with data related to the configuration and management of Bocada.

Recovery Model

The Bocada database is installed with the Recovery model set to **Simple**. Using another recovery model, such as *Full* will cause slower performance and tend to fill up transaction logs fast. The most critical backup job data stored in the Bocada database can be collected again while it exists on the backup server.

To maintain performance of the Bocada database and application, *we advise that the Bocada database be kept in **Simple Recovery Model***. Please reference Microsoft documentation for details about the differences between recovery models:

<https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server>

Bocada User Interface Application

The Bocada User Interface Application is a web-based interface enabling configuration and management of Bocada.

Supported Browsers

Current versions of the following browsers are supported; some obsolete versions of these browsers may work as well but have not been tested prior to release and are not supported.

- Chrome
- Firefox
- Internet Explorer (11.x, 10.x) is depreciated and has limited support

When using Internet Explorer, IE Enhanced Security must be turned off for all Bocada reports to run properly.

Note:

If you wish to increase the time for the Idle Time-out in the Bocada website, see [Appendix F: Bocada Website IIS Time-Out Settings](#) for how to adjust IIS settings. You may need to repeat this change after upgrading Bocada to a new version.

Bocada Data Collection Service (DCS)

The Data Collection Service is responsible for mining metadata from backup servers, for storage in the Bocada database. In addition, any active DCS (not just the master DCS) may initiate database maintenance tasks or routines.

Processes

Processes run on the Application and Data Collection servers are detailed in [Appendix A: Server Processes](#).

Supported Data Protection Products

The DCS uses a specific plugin for each backup product to interface with backup servers. These do not require any software agents to be installed on any backup servers or backup clients.

For the most up-to-date information on products and versions supported, see the *Bocada Product Version Support Matrix* at: <https://bocada-support.force.com/s/article/Bocada-Backup-Product-Version-Support-Matrix-PDF> .

User Role Definitions

Upon installation the user who performed the installation will be an Administrator in Bocada. You should add additional users to Bocada immediately after initial installation.

Administrators

Administrators have unrestricted and complete access to Bocada and all data.

Operators

Operators can manage data collection, backup server and client properties, schedules, alerts, saved reports, can save globally available reports, and can email or export reports. While zone restriction is enabled, Operators have access to backup client data in their assigned zones as well as data for all un-zoned backup clients.

Operators do not have access to the Administration section, nor the ability to manage SLA profiles or to create or edit Custom SQL reports.

Standard Users

Standard Users can run, export, and email reports using their own configured criteria. Any saved report created by a Standard User is only available to the user who created it.

If Bocada zone restrictions have been enabled, Standard Users can only see data related to backup clients in their assigned zones, and do not have access to data related to un-zoned backup clients.





Unit Calculation

The current Unit count usage can be determined at any time from the [License Count](#) view in the Administration section. The definition of a unit can be found in the Bocada End User License Agreement (EULA).

Alerting & Incidents Module

Bocada provides automatic alerting. Backup Alerts notify when backup and restore failures match pre-defined criteria as data is collected from the backup servers into Bocada. Alerts also can tell you when there has been a problem collecting data from your backup server.

Alerting & Incidents

-  Alert Config
-  Backup Alert Activity
-  Incident History
-  Instance Configuration

Alerts can be distributed in 3 different ways:

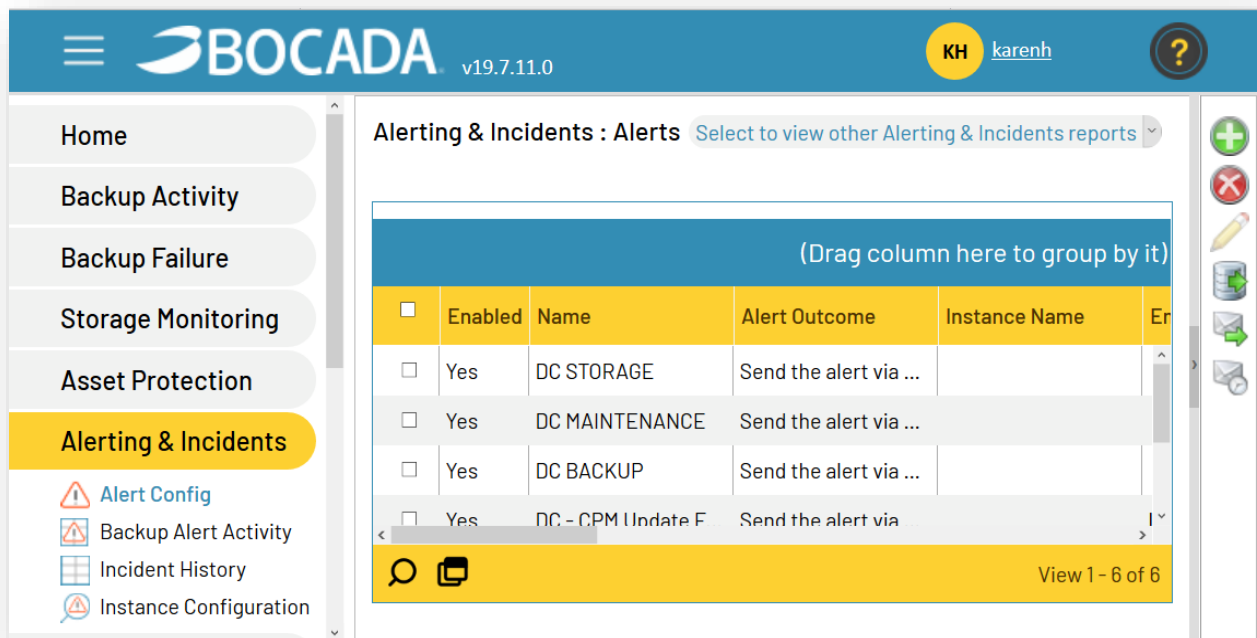
1. Receive email alerts
2. Open trouble tickets in any system that accepts emailed ticket notifications
3. Open *incidents* in ServiceNow, Remedy, Jira and other ticketing systems, and stay synchronized with the status as those incidents progress through their lifecycle.

You can also configure alerts to open and track *Incidents* or *tickets*. Incidents will be tracked and updated inside of Bocada reports so that you can see the progress of the ticket opened by the alert. Bocada also has the option to close tickets automatically when a later successful backup is found.

If you have configured multiple alerts that would trigger from the same backup failure, then all of the triggered alerts will fire. For example, if you have two alerts configured that are identical in every way except the alert name, then you would get double alerts.

Alerting & Incidents : Alert Config

Click on Alert Config to create and modify Alert Configurations.



Click on the Green button with a plus sign to add an Alert to Bocada.

Alerting

Emailed Alerts

When Alert occurs: Send the alert via email

Alert Name: Example Alert for Documentation

Email Addresses: test@bocada.com

Email Message: Please investigate this occurrence

Attachments:
☐ HTM (Attached)
☒ HTM (Inline)
☐ PDF
☒ CSV
☐ TXT

Enabled: ☒

Ticket Template: None (no ticket created)
[Click here to configure ticketing](#)

Alert Criteria

Alert on Backup Failures when there are 10 or more

Consecutive Failures Per Asset

☒ Filter on existing saved report criteria Backup Job Activity

Finish Cancel

Alert Criteria

When creating or editing an Alert for Backup Failures or Restore Failures, the Alert may be set to trigger when there are N or more:

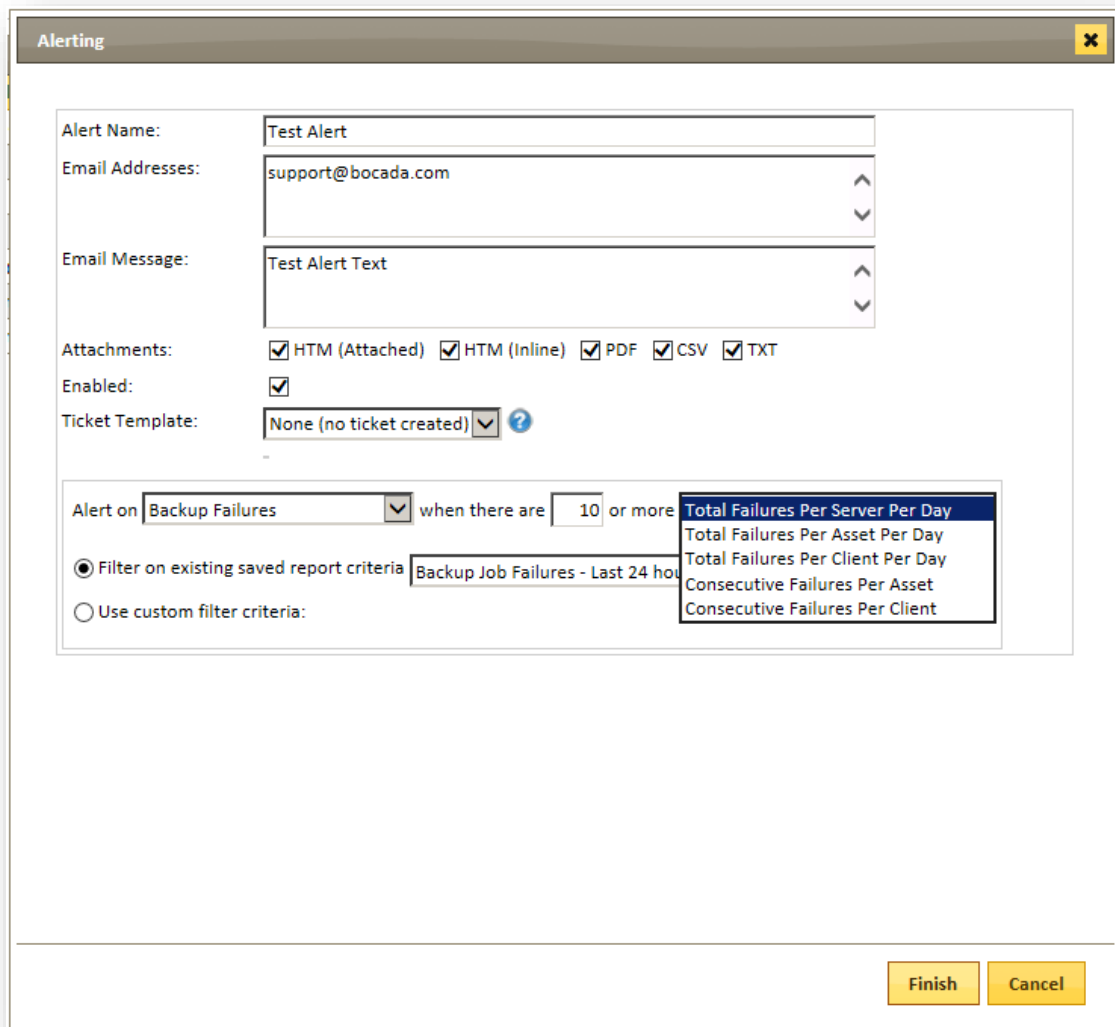
- Total Failures per Server per Day
- Total Failures per Asset per Day
- Total Failures per Client per Day
- Consecutive Failures per Target
- Consecutive Failures per Client

Alerts will be triggered when the criteria are met. For “Total Failures per Day” Alerts, the Alert will trigger each time upon reaching the specified number of failures in a single Backup Day.

“Consecutive Failures” alerts will be triggered upon each failure that meets or exceeds the specified number of consecutive failures, regardless of when they occur. For example, suppose that you have configured a Bocada alert on 3 consecutive failures. Assume that you have a client that backs up only one target, and only once per week, and it has failed for the past 2 weeks on the day that it normally runs. If the weekly backup fails again today, then you will get an alert today, even though the consecutive failed backups happened over a 15-day period. Consecutive Failures alerts can also result in multiple alerts in the same day for an Asset or Client if backups continue to start and but fail repeatedly.

Alerts may be filtered on an existing Saved Report of the appropriate type, so Alerts for Backup Failures may be filtered on saved Backup Job Activity reports, and Alerts for Restore Failures may be filtered on saved Restore Job Activity reports. The criteria used to generate that saved report will apply to the Alert. Alternatively, customized Alert filter criteria may also be set by selecting the *Use custom filter criteria* button, which expands a criteria wizard for the Alert.

Note: When creating or editing an Alert for Data Collection Failures, only custom filter criteria is available.



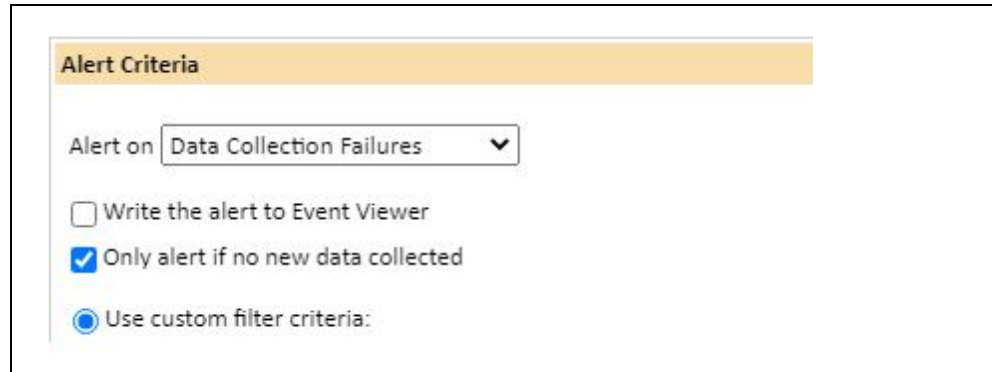
The image shows a software window titled "Alerting" with a close button in the top right corner. The window contains several input fields and checkboxes for configuring an alert. The "Alert Name" field is set to "Test Alert". The "Email Addresses" field contains "support@bocada.com". The "Email Message" field contains "Test Alert Text". Under "Attachments", checkboxes for "HTM (Attached)", "HTM (Inline)", "PDF", "CSV", and "TXT" are all checked. The "Enabled" checkbox is also checked. The "Ticket Template" dropdown is set to "None (no ticket created)". Below these fields, there is a section for defining the alert trigger. It includes a dropdown menu set to "Backup Failures", followed by the text "when there are", a text box containing "10", and the text "or more". To the right of this is a list of criteria: "Total Failures Per Server Per Day", "Total Failures Per Asset Per Day", "Total Failures Per Client Per Day", "Consecutive Failures Per Asset", and "Consecutive Failures Per Client". Below this list, there are two radio buttons. The first is selected and labeled "Filter on existing saved report criteria", with a dropdown menu showing "Backup Job Failures - Last 24 hou". The second radio button is labeled "Use custom filter criteria:". At the bottom right of the window are two buttons: "Finish" and "Cancel".

Create an Alert

Alerts are calculated as per the [Alerts Schedule](#) which is every five minutes by default. To create an Alert:

1. Click the Add icon in the right action panel. This will launch the Alerting wizard.
2. Configure the alert:
 - a. Alert Name: (required)
 - b. Email Addresses: (optional)
 - c. Email Message: (optional)
 - d. Choose attachment types
 - e. Enable or disable the Alert
 - f. Ticket Template: (optional - Please reference the *Ticketing System Integration Guide*)
3. Define alert type and failure criteria:
 - a. Backup or Restore alerts:

- i. Choose Backup or Restore Alerts
 - ii. Set the number of failures
 - iii. Select the type of failure (Total per Day or number of Consecutive failures, by type)
- b. Data Collection alerts:
 - i. Choose Data Collection alerts
 - ii. Alerts are triggered for every data collection failure; failure type and number do not apply.
 - iii. For longer data collections with multiple chunks, alerting may produce verbose messages. The “Only alert if no new data collection” option will cause alerts to be skipped for cases where any new backup data was committed and then the data collection failed. This setting only has an effect for backup data collections. This rule only works for backups that started in the past 30 days.



Alert Criteria

Alert on: Data Collection Failures ▼

☐ Write the alert to Event Viewer

☒ Only alert if no new data collected

☒ Use custom filter criteria:

4. Choose a previously saved report or define custom filter criteria to govern the Alert. The selected criteria of your saved report will be used for the alert EXCEPT and GRID FILTER (Find Records magnifying glass icon) will NOT be applied!

Details of Backup and Restore Alerts that have been triggered are displayed in the *Backup Alert Activity* report. Details of Data Collection Alerts that have been triggered are displayed in the [Data Collection Alert Activity](#) report under Configuration => Advanced Config.

The columns of data sent by an Alert are those necessary to identify those failures which contribute to the triggering of that Alert, for trouble-shooting purposes. Even if the Alert is associated with a particular report (i.e., uses the same criteria), the columns displayed in the Alert report are not necessarily identical to all those columns seen in the associated report. Columns which are seen in the Alert report are:

- Status
- ! (indicates Annotation)
- Product
- Server
- Client
- Target

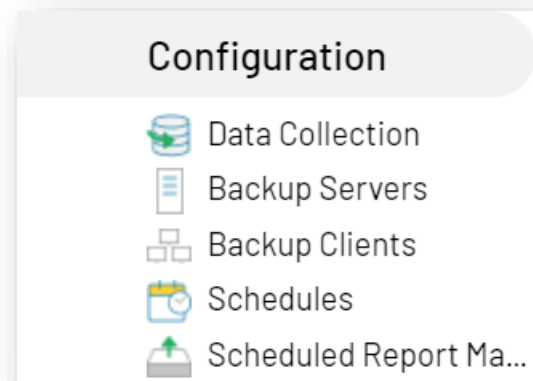
- Level
- Job Group
- Error Count
- Error Sets
- Error Codes
- Description
- File Count
- Job Start Date
- Job Complete Date
- Server Start Time
- UTC Start Time
- UTC Complete Time
- Duration
- Throughput (MB/s)
- insertiontime
- SLA Profile

Edit an Alert

Select an Alert, and click the Edit icon from the Action panel. This will launch the Alerting wizard as above to edit the fields that you would like to update.

Configuration Module

Views in the Configuration Module section are used by the Bocada Administrator or Operator for managing backup servers, data collection, alerts, schedules and backup clients.



Configuration : Data Collection

The Data Collection view enables monitoring of data mining from backup servers. The view can be used to find failed collection (and re-run collections) of backup server data, to update schedules, to update priority, or to change the Data Collection Server used for collection.

In addition, the Data Collection view can be used to manually run and cancel updates and edit backup server properties.

Note: When manually running a collection for a Custom Date Range, the collection will include those jobs *completed* (not started) within that range. For example, when manually running a collection of jobs on a particular day, make certain your date range includes enough hours into the following day to include any long-running jobs.

Update Status

Data Collection operations will display one of the following Statuses:

- Successful: The most recent successful update.
- In Progress: Updates that are currently running.
- Failed: The most recent failed update (Note: The column “Last Updated” represents the most recent success).
- Pending: The current update is queued and will be run based on the concurrent update settings as defined in the Administration/Settings section.
- Never Processed: Updates that have never been run (either according to a Schedule, or manually).
- Stopped: Updates that have been manually canceled during collection.

Update Detail

Clicking the Status (e.g., click on the word “Successful” or “Failed”) of the update in the main view will display the messages of the most recent updates from the server activity log.

Saved Reports

Backup Activity

Backup Failure

Storage Monitoring

Asset Protection

Alerting & Incidents

Cost Management

Configuration

Data Collection

Backup Servers

Backup Clients

Schedules

Scheduled Report Ma...

Configuration : Data Collection

Last 31 days Default ((GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)

> Report criteria

(Drag col

<input type="checkbox"/>	Server Name	Backup Product	Collection Type	Status	Runtime (Minutes)	Last Message
<input type="checkbox"/>	aws_rds	AWS Backup	Storage Update	In Progress	2.98	Update In Pro...
<input type="checkbox"/>	tl-ave-02.testlab.com	Avamar	Backup Update	Successful	0.15	Successfully ...
<input type="checkbox"/>	tl-ave-02.testlab.com	Avamar	Policy Update	Successful	0.13	Successfully ...
<input type="checkbox"/>	tl-ave-02.testlab.com	Avamar	Storage Update	Successful	0.13	Successfully ...
<input type="checkbox"/>	tl-dp-ws04	HPE Data Protector	Backup Update	Failed	0.12	Error 545: Co...
<input type="checkbox"/>	tl-dp-ws04	HPE Data Protector	In Progress Jo...	In Progress	2.98	Update In Pro...
<input type="checkbox"/>	tl-dp-ws04	HPE Data Protector	Policy Update	Successful	0.15	Success with...
<input type="checkbox"/>	tl-dp-ws04	HPE Data Protector	Storage Update	Successful	0.13	Successfully ...
<input type="checkbox"/>	tl-dp-ws04.testlab.com	HPE Data Protector	Backup Update	Successful	6.08	Successfully ...

For each server, selecting the text under Status will open the details of those Data Collection jobs:

Details					
Server	Product	Status	Runtime (Minu	Started	Finished
tl-ave-02.testlab.com	Avamar	Succe...	0.15	2020-05-21 02:00:00	2020-05-21
tl-ave-02.testlab.com	Avamar	Succe...	0.13	2020-05-21 01:50:00	2020-05-21

Auto refresh Duration unit: Minutes View 1 - 100 of 250

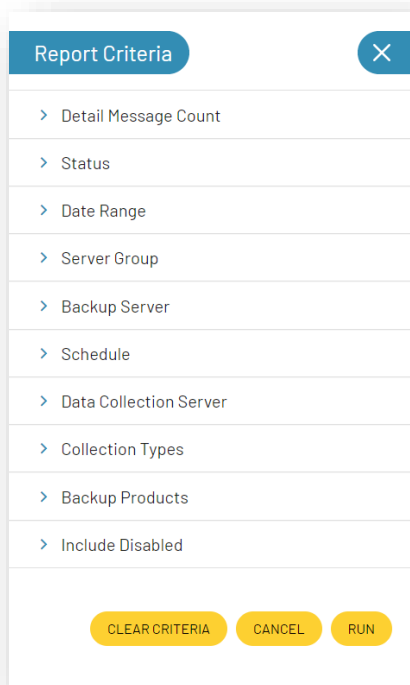
Time	Severity	Message Code	Message Text
2020-05-21 02:00:09	Info	M000	Request completed successfully
2020-05-21 02:00:08	Info		Prune disk cache
2020-05-21 02:00:08	Info		LCD: backup_id: 9268
2020-05-21 02:00:08	Info		LCD: Setting latest completion date to '2020-05-21 00:00:21'

View 1 - 39 of 39

The top panel of Details displays all collections of this type for this server (the most recently finished job is displayed by default) within the date range selected in the Date Range criteria (note that this date

range will not look backwards from the current time, but from the last attempted job). The lower panel displays the Activity Log with each step in that job, including all messages and any errors encountered. Note: Collections for many backup products will display an Activity message like “Inserted 0 server event records into the database in 0.046 seconds.”. This is for Server Events (as displayed in the Configuration > Advanced Config. > Backup Server Activity report) and should not be confused with Server Messages; A message that 0 server event records have been inserted is expected for many backup products.

In addition to many of the criteria common to other reports, Data Collection operations can be searched by the following criteria:



Report Criteria

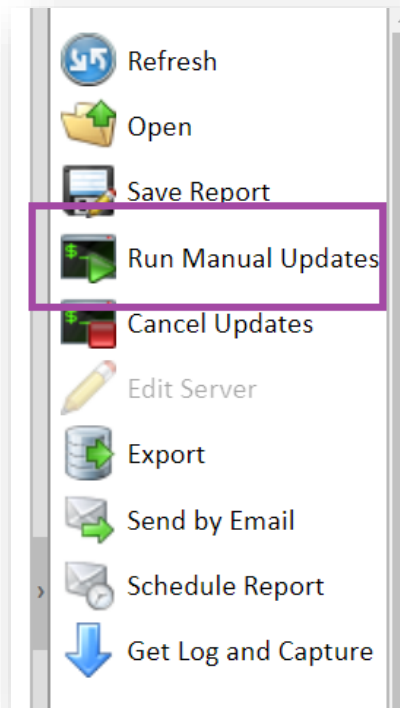
- > Detail Message Count
- > Status
- > Date Range
- > Server Group
- > Backup Server
- > Schedule
- > Data Collection Server
- > Collection Types
- > Backup Products
- > Include Disabled

CLEAR CRITERIA CANCEL RUN

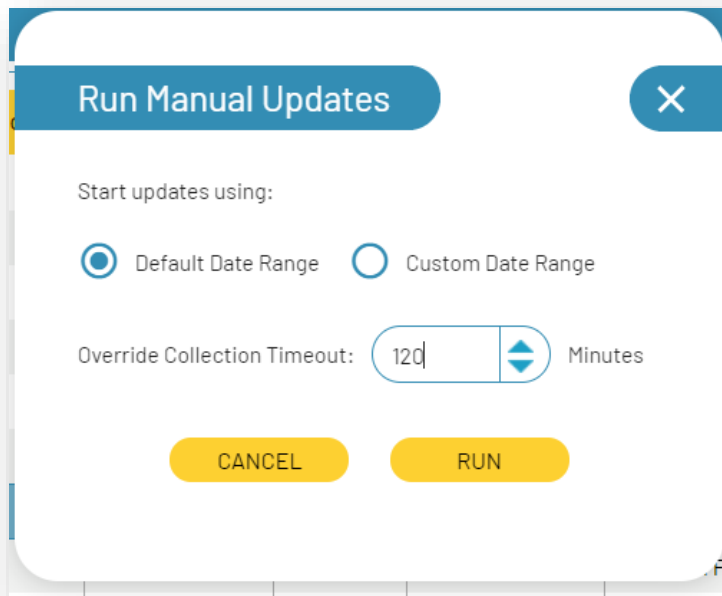
Criteria “Detail Message Count” sets the number of activity log messages displayed (default 250).

Manual Data Collection

To run a collection from the Data Collection view, select the row(s) for the server(s) and collection type(s) you would like to run, then select action *Run Manual Updates* from the right Action panel:



This opens the *Run Manual Updates* dialog. The “Default Date Range” button is selected by default, and will run collections from the last successful datetime to the present. However, manual collections may also be run over any date range desired, such as re-running a data collection which has previously occurred. To do this, select the radio button for “Custom Date Range”, and change the *To* and *From* dates to a date range which encompasses the activity which you are trying to collect:

A dialog box titled "Run Manual Updates" with a close button (X) in the top right corner. It contains two radio buttons under the heading "Start updates using:". The first radio button is selected and labeled "Default Date Range". The second radio button is labeled "Custom Date Range". Below these is a text input field labeled "Override Collection Timeout:" containing the value "120", followed by a spinner control and the word "Minutes". At the bottom are two yellow buttons: "CANCEL" and "RUN".

Run Manual Updates

Start updates using:

☒ Default Date Range ☐ Custom Date Range

Override Collection Timeout: 120 Minutes

CANCEL RUN

When manually running a collection for a Custom Date Range, the collection will include those jobs **completed** (not those that started) within that range. Note that running collections for a Custom Date Range also includes the option to override the default Collection Timeout. While the default Collection Timeout is set on the [Collection tab](#) of the [General Settings](#), a manual collection may be desired for a much longer date range, and may require overriding this value.

Click *Run* to begin the collection.

Refresh the Data Collection report until the collection completes.

Configuration : Backup Servers

The Servers report displays all the backup servers that have been added to Bocada, including Server Name, Backup Product, Time Zone of the backup server and the Data Collection Server assigned to run the updates.

Add/Edit Servers

New backup servers can be added to Bocada (and existing backup servers can be edited) by selecting the Server icon (or Edit Server icon) from the right Action panel to launch the Add Server (or Edit Server) wizard. These wizards include the following management sections:

Servers Tab, which appears as the Backup Product Name after a server has been added.

The <Servers/Backup Product Name> Tab includes the properties of the backup server, including name, backup product, and time zone. Multiple backup servers may be added simultaneously; simply enter all server names on separate lines. The next fields depend on the backup product, and settings are detailed in the respective product *Plug-in Guides*. For adding multiple servers you can fill in all of the common fields, but you must edit each server individually for any unique values.

When editing a backup server, this tab will be labeled with the name of the backup product. Editing multiple backup servers of different backup applications is supported; when performing this operation, there will be a Backup Application tab for each type of backup server product in the selected servers.

This tab will also be used to set advanced properties when necessary. Select *Show Advanced Properties* below the standard properties to view any advanced properties for that backup product:

Add Servers

×

Servers

Schedules

Settings

Updates

Server names:

myaws1
aws-2
aws03

Product for these servers:

AWS Backup

Data Collection Server:

Avamar
AWS Backup
Azure Backup Server
Azure Cloud Recovery
Azure Storage and Legacy
Backup Exec
Backup Exec Legacy

Configure Server Properties:

Access key ID

Secret access key

Time Zone

Show Advanced Properties

TEST CONNECTION

Testing the connection will add servers and save the servers' properties

CANCEL

PREVIOUS

NEXT

FINISH

Schedules Tab

The Schedules tab enables collection schedule assignment and creation. Note that Backup Activity data collections also include In Progress jobs. It is recommended that you only schedule additional In Progress job collections if you are unable to run Backup Activity data collections often enough.

Edit Servers

AWS Backup | **Schedules** | Settings | Finish

ADD SCHEDULE

Enable	Priority	Schedule
<input checked="" type="checkbox"/> Backup Activity	High	Backup Collection
<input type="checkbox"/> In Progress Jobs	High	Unscheduled
<input checked="" type="checkbox"/> Storage Collection	High	Backup Collection

Disable all collections including manual: Disable all collections

CANCEL PREVIOUS NEXT FINISH

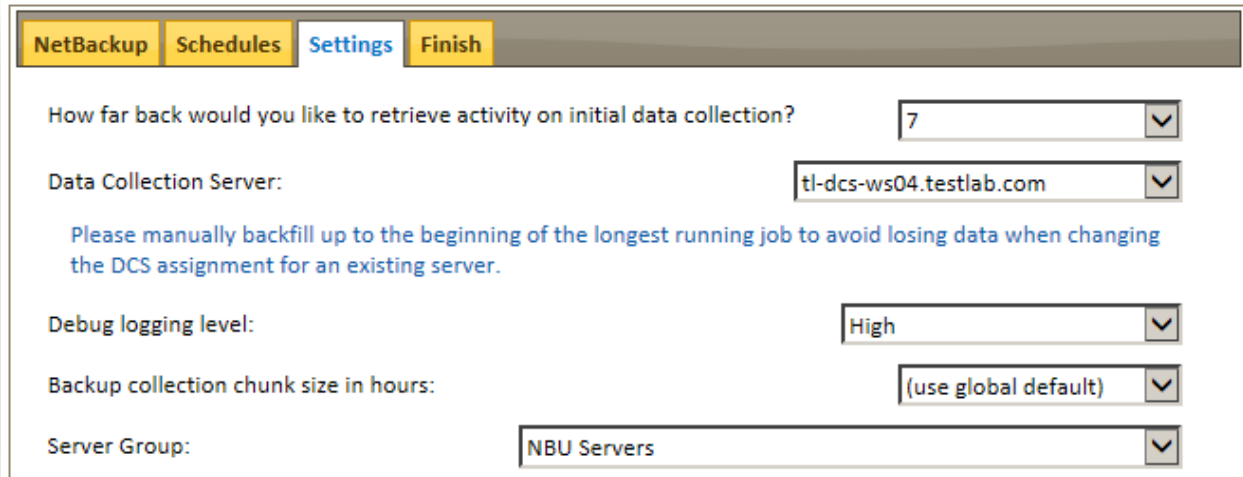
Selecting *Show Advanced Properties* will show whether the schedule is enabled for this update and priority relative to other updates.

To ensure proper mapping between vCenter virtual machines and Backup client data, vCenter updates should be run successfully prior to adding other backup servers. It is also recommended that vCenter Backup and Storage updates should be run with roughly the same frequency as other Backup Job updates.

The *Disable all collections including manual* is disabled by default “Do not disable all collections”, once it turns on with “Disable all collections”, all data collections either scheduled or manual don’t even start or fail immediately with error message “Collections are disabled for this server, re-enable in server properties”.

Settings Tab

The Settings tab allows selection of how far back historical data will be collected from the backup server for the initial update. The availability and quality of the data is dependent on what is available from the backup server.



The screenshot shows the 'Settings' tab in the Bocada Administration module. The tab bar at the top includes 'NetBackup', 'Schedules', 'Settings' (which is highlighted), and 'Finish'. The main content area contains several settings:

- 'How far back would you like to retrieve activity on initial data collection?' with a dropdown menu set to '7'.
- 'Data Collection Server:' with a dropdown menu set to 'tl-dcs-ws04.testlab.com'. Below this is a blue note: 'Please manually backfill up to the beginning of the longest running job to avoid losing data when changing the DCS assignment for an existing server.'
- 'Debug logging level:' with a dropdown menu set to 'High'.
- 'Backup collection chunk size in hours:' with a dropdown menu set to '(use global default)'.
- 'Server Group:' with a dropdown menu set to 'NBU Servers'.

The option to choose a Data Collection Server is also available when multiple Data Collection Servers are available; this can be useful for load-balancing across the Data Collection servers.

Warning (If your installation uses more than one Data Collection Server): While the 'Data Collection Server' setting makes it possible to change the DCS that a Backup Server is assigned to, be aware that long-running jobs are often held in cache files on the DCS (by default, these cache files may be found in the directory 'C:\Program Files (x86)\Bocada\DataCollection\snapshot\<BACKUP_PRODUCT>\<SERVER_NAME>') until those jobs have completed. Reassigning a Backup Server to a different DCS will **not** move any cache files remaining to the new DCS, so it is recommended to run manual collections after changing the assigned DCS to collect any jobs that may have been cached.

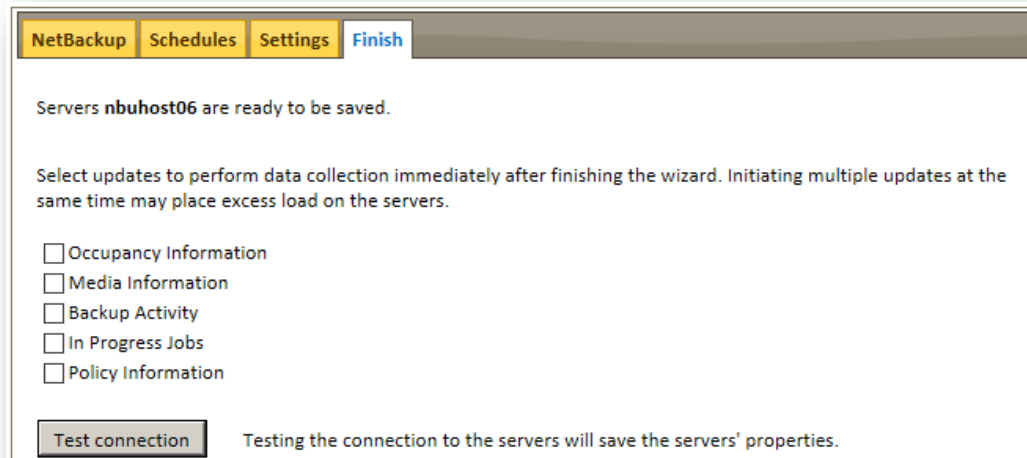
The Debug logging level is disabled by default, but can be set to medium or high to troubleshoot failed updates. The location of these logs is displayed and can be changed from the [Settings](#) view of the Administration module. If there are any issues with data collection, set Debug logging to 'High' and provide the resulting log(s) to [Bocada Support](#).

The setting *Backup collection chunk size in hours* determines the limit (in hours) of the time span collected and committed to the Bocada database. This setting defaults to 'use global default' (see the [Settings](#) section on Data Collection), but may be individually set from 1 to 72 hours. In previous versions of Bocada, when performing manual collections against a very busy Backup server, it might have been necessary to run several collections for short time-spans in order to give each collection time to capture all the Backup server activity and commit it to the Bocada database. With this feature, an Administrator can determine the time-span, or "chunk size", to be collected and committed at one time before moving on to the next chunk. Thanks to this feature, it is now recommended to allow Bocada to run collections using Default Date Range instead of customizing the date range, and to adjust the chunk size as needed.

The backup server may also be assigned to a Server Group via the pull-down menu here, if Server Groups are being used.

Finish Tab

This tab includes a test connection to confirm the entry settings, and allows for updates to be run immediately after finishing the wizard. By default, all updates are unchecked and will not run when finishing the wizard.



NetBackup Schedules Settings **Finish**

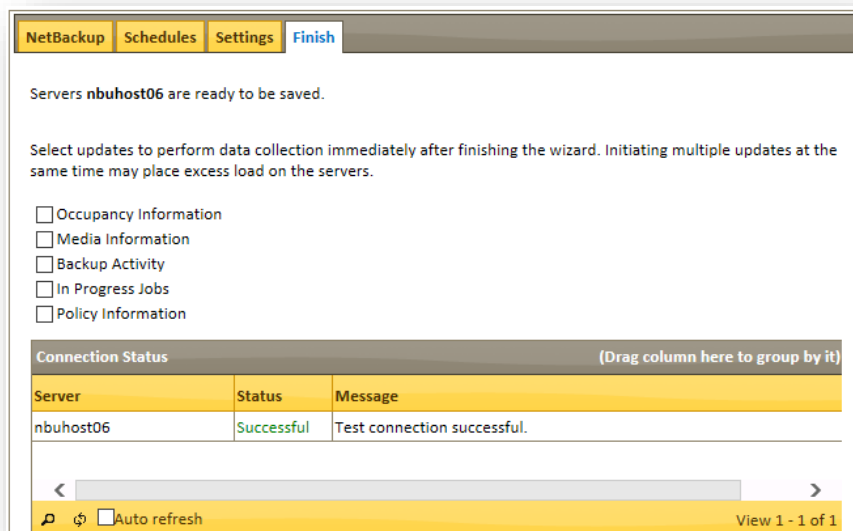
Servers **nbuhost06** are ready to be saved.

Select updates to perform data collection immediately after finishing the wizard. Initiating multiple updates at the same time may place excess load on the servers.

- ☐ Occupancy Information
- ☐ Media Information
- ☐ Backup Activity
- ☐ In Progress Jobs
- ☐ Policy Information

Test connection Testing the connection to the servers will save the servers' properties.

Test the connection before exiting the wizard to perform basic connectivity checks:



NetBackup Schedules Settings **Finish**

Servers **nbuhost06** are ready to be saved.

Select updates to perform data collection immediately after finishing the wizard. Initiating multiple updates at the same time may place excess load on the servers.

- ☐ Occupancy Information
- ☐ Media Information
- ☐ Backup Activity
- ☐ In Progress Jobs
- ☐ Policy Information

Connection Status (Drag column here to group by it)		
Server	Status	Message
nbuhost06	Successful	Test connection successful.

< >

Auto refresh View 1 - 1 of 1

Delete Servers

Backup servers can be deleted in the following steps:

1. Select the server to be deleted.
2. Click the Delete icon from the right Action panel
3. Confirm by clicking the Delete button in the Delete Selected Items popup window.

Note that deleting a backup server will delete all historical data for the server including any client, backup job, policy, or other data mined for that backup server.

The screenshot shows the 'Operations : Servers' interface. A table lists servers with columns: Server Name, Backup Product, Logging, Time Zone, Server Group, and Data. The first row, 'nbuhost06', is selected. A dialog box titled 'Confirm Delete Selected Items' is overlaid on the table, asking 'Are you sure you want to delete 1 selected server(s)?' with 'Delete' and 'Cancel' buttons. On the right, an action panel contains icons for Refresh, Add, Delete, Edit Server, Open, Save Report, Export, Send by Email, Schedule Report, and Assign Data Domain.

	Server Name	Backup Product	Logging	Time Zone	Server Group	Data
<input checked="" type="checkbox"/>	nbuhost06	NetBackup	High	(GMT-08:00) Pacific Tim...	NBU Servers	tl
<input type="checkbox"/>	nbuhost06.testlab.com	NetB...	Web	(GMT-08:00) Pacific Tim...	Unassigned	tl
<input type="checkbox"/>	nbuhost07	NetB...			Unassigned	tl
<input type="checkbox"/>	nbuhost07.testlab.com	NetB...			Unassigned	tl
<input type="checkbox"/>	nbuhost08	NetB...			Unassigned	tl
<input type="checkbox"/>	nbuhost08.testlab.com	NetB...			Unassigned	tl
<input type="checkbox"/>	nbuhost76ga	NetB...			Unassigned	tl
<input type="checkbox"/>	nbuhost76ga.testlab.com	NetBackup	High	(GMT-08:00) Pacific Tim...	Unassigned	tl

Configuration : Backup Clients

The Backup Client Properties view displays information related all the backup clients reported in Bocada. The top panel lists all backup clients, which backup product and backup server was used to back them up, when each client was last backed up, and to which zones each backup client is assigned. The bottom panel lists the Targets (assets) associated with each backup client.

Client Properties

Client properties can be managed by the Backup Clients view. They can be changed by selecting a backup client, and choosing the Client Properties icon from the right action panel. This launches the Client Properties wizard to set the following:

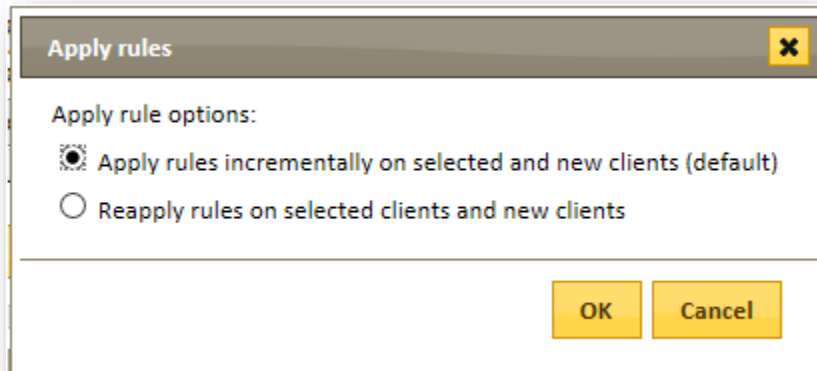
- Zones** Client can be assigned to the zones created in the Zones view of the Administration section. Zone enforcement is detailed in the [Zones](#) and [Users](#) sections of this document.
- SLA Profile** All SLA profiles will appear in the list of SLA Profiles and can be applied to the selected backup clients. SLA Profiles have a one-to-many profile-to-client property.
- Price List** All Price Lists will appear and can be applied to the selected backup clients. Price Lists have a one-to-many profile-to-client property.
- Ignore Targets** Data for specific backup targets can be ignored when generating reports. The backup target can either be ignored for specific date ranges, or ignored forever.
- Target Renaming** Use the [Target Renaming](#) feature to display like-Targets as single entities, simplifying reports.
- Data Pruning** Data pruning applies to pruning and recalculating the SLA calculations with any changes made to the backup client properties, such as recalculating for an updated SLA Profile.

Ignore Client

Selecting a client (or clients) and then clicking Ignore Client from the right Action Panel will allow you to ignore that client(s) for a selectable date range, or always, when generating reports.

Run Rules

Selecting a client (or clients) and then clicking Run Rules from the right Action panel will run all [Rules](#), in order, on the selected client(s). This action will open a limited Apply Rules dialog:



Option 1: Applies Rules, in order, on the selected clients (and on any new clients). If any of the selected clients are not new (that is, Rules have previously been run against those clients), Rules will not be run against them.

Option 2: Will remove all assignments of any kind and then apply rules against the selected clients (and on any new clients). Note that this will undo all previous assignments to any zone, price list, or SLA regardless of whether the original assignment was done manually or by a rule.

Target Renaming

A backup target is the smallest backup client resource for which key metrics (such as backup date/time, byte count, errors, etc.) are available. For many backup jobs, the target corresponds to the file path backed up. For example, if the C: drive is backed up by a given job, the target is "C:\". A target can also represent an activity specific to the backup server.

In some environments, multiple separate targets may refer to the same protected asset. This can happen when the targetname has a date stamp in it, which sometimes happens when a script is used to do the backup. For some backup products, the backup server performs index backups for each backup client. This index generates new targets for each backup with similar names such as "index:5aa5a1b5" and "index:5AA5A488". Target renaming allows these targets to be combined into a single entity such as "index".

Target Renaming uses a pattern to identify the targets that should be renamed and the new name is the Display Name. The original target name is preserved in the Bocada database, and the new name is

stored in a linked table for display in reports. The new name takes effect immediately, even for historical data. No wildcards are supported, so you will need to identify a single common pattern in each set of targets that you want to rename. That pattern can be at the beginning, end, or middle of the original target name.

Client Properties

Zone SLA Profile Price list Ignore Targets Target Renaming Data Pruning

Order	Move Up	Move Down	Target Name	Match Target	Display Name	Mat
-------	---------	-----------	-------------	--------------	--------------	-----

records to view

Add Record

Order

Target Name

Match Target Name Left

Display Name

Match Target for Server nbuhost06.testlab.com

Match Target for Client t1-vm64-client1

Submit Cancel

Previous Next Finish Cancel

Note that target renaming is immediately applied for current and historical data. So a report run for previously collected data will use the new target names once this is configured.

Configuration : Schedules

The Schedules view displays all schedules that have been created and allows schedules to be created, edited, paused/resumed, disabled, or deleted. Schedules define times when data collection updates run and when reports are scheduled to be exported or emailed.

Important Notes:

- Deleting a schedule will cause any processes that rely on it (e.g.: data collection or scheduled exports) to cease functioning. It is recommended that you confirm in Scheduled Actions that it is no longer being used.
- Schedules are not unique to a single process, and allow for multiple actions to be performed on the same schedule. It is recommended that you name the schedule descriptively, and have minimal overlap between different process types (i.e., data collection versus export).

There are five default schedules which govern Bocada processes; these cannot be deleted but can be edited:

Alerts: Frequency of Alert calculation, defaults to Every 5 minutes.

Policy Changes: Frequency of the Policy Change Analysis calculation, defaults to Every 5 minutes.

Pruning, Database Maintenance: Frequency at which the Bocada database is pruned, defaults to Daily at 4 AM GMT.

Rules Incremental: Frequency newly discovered clients are assigned with the Rules process, defaults to Every 4 hours.

SLA Compliance Validation: Frequency of the SLA compliance calculation, defaults to Daily at 00:00:00 GMT.

Configuration : Scheduled Report Management

The Scheduled Report Management view is used to manage reports that have been scheduled for export to email or to a UNC path. This report displays and allows for editing of scheduled report configuration properties, including:

- Status of most recent attempt and last error if any
- Configuration Name
- Report Type
- Report Name
- Types of files for export, if any
- If email is configured and to which addresses
- Export location for file, which must be accessible by global settings export account for scheduled export
- Schedule name and description
- User that configured the scheduled report

Configuration : Advanced Config. : Data Collection Alert Activity

This report view displays the Data Collection Alerts caused by failed collection updates that met the criteria of Data Collection alerts defined in the *Alert Config* report view.

Configuration : Advanced Config. : Data Collection Servers

This view displays activity details for all Data Collection Servers (DCS), including their status, current collections activity, and active scheduled actions.

Configuration : Advanced Config. : Scheduled Actions

The Scheduled Actions view displays all scheduled operations and their results. This provides a window into Alerting, Database Maintenance, Data Collection, Report Generation, Rules, and SLA functionality, among other scheduled actions.

Configuration : Advanced Config. : Backup Server Groups

New to Bocada 11.0, this report displays the grouping of backup servers into Server Groups. Unlike [Zones](#), Server Groups are cardinality 1 (a backup server may only be assigned to one Server Group at a time). Server groups may be added, edited, and deleted via this report.

Configuration : Server Groups		
Report criteria		
<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	Group A	
<input type="checkbox"/>	Group B	
View 1 - 2 of 2		
Server Group Servers		
Server Name	Backup Product	Schedules
aws_24107	AWS Backup	Unscheduled

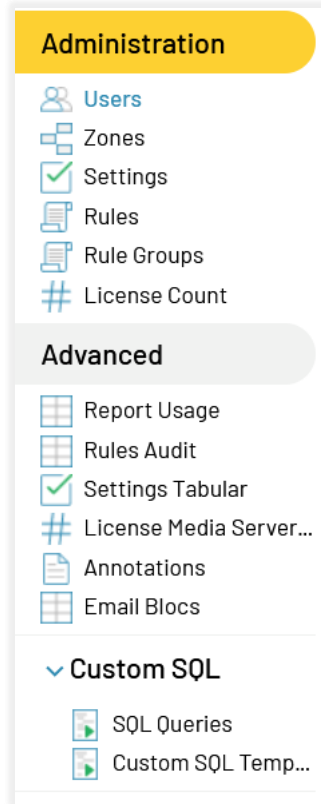
Once a Server Group has been created, assigning a backup server or servers to that server group is accomplished within [Backup Servers](#), by selecting the server(s), editing the server properties, and selecting a Server Group on the [Settings](#) tab.

Configuration : Advanced Config. : Backup Server Activity

This report view displays general backup server information. This data can include but is not limited to messages related to sessions, user actions, media cleaning, session statuses, database operations, media mount requests, job queue messages, and general backup & restore job messages.

Administration Module

The Administration Module includes the views shown below.



The Administration Module is only accessible to Bocada Administrators.

Administration : Users

Bocada has three user types, and the roles for each are detailed in the [User Role Definitions](#) section. Each user role can see a set of reports and views defined by Administrators.

Only Windows Domain Users can be added as Bocada users. The Active Directory associated with the domain in which Bocada is installed defines the users that can be added to Bocada. Users from other domains may also be added to Bocada as any role, so long as those users are visible to the Active Directory on each Bocada Application server. Normally, this means that any other Domain is trusted by the Domain in which the Application server has been installed. You cannot use Bocada for users in multiple Windows Domains that do not have trust.

Adding users

Users can be added by highlighting the desired role, launching the *Add Users* wizard, and choosing the desired users to be added to the highlighted role.

Add users to role: Administrator

Please select the users and groups you would like to add to this role. Search using the "domain\name" format. The user list is acquired from the directory service.

Search for users:

(Drag column here to group by it)			
<input type="checkbox"/>	Name	Email	Current Role
<input type="checkbox"/>	TESTLAB\UM Management		
<input type="checkbox"/>	TESTLAB\User1	User1@testlab.com	Administrator
<input type="checkbox"/>	TESTLAB\User2	User2@testlab.com	Standard User
<input type="checkbox"/>	TESTLAB\User3	User3@testlab.com	Standard User
<input type="checkbox"/>	TESTLAB\User4	User4@testlab.com	
<input type="checkbox"/>	TESTLAB\User5	User5@testlab.com	
<input type="checkbox"/>	TESTLAB\user6	User6@testlab.com	
<input type="checkbox"/>	TESTLAB\user7	user7@testlab.com	
<input type="checkbox"/>	BUILTIN\Users		

View 1 - 9 of 9

Assign Reports

Administrators can manage the reports visible to the Operator and Standard User roles by highlighting the desired role, launching the *Assign Reports* wizard and choosing which reports are enabled for the highlighted role.

Note: Available Reports are defined at the role level and cannot be defined on a per-user basis.

User Zone Assignment

Only Bocada Administrators can manage which Zones are assigned individual Operators and Standard Users. Backup Clients in the Zones assigned to an Operator or Standard User are visible to that User. To assign Zones to a User, highlight a single User, select the *Zone Assignment* action and assign the desired Zones using the wizard.

Note that the global setting for Zones Enforcement must be configured for Users to be constrained to view clients in the assigned Zones. See the [Edit General Settings, Global Report Settings](#) section above.

Administration : Zones

Zones logically group backup clients based on any user defined attributes such as application, backup administrator assigned, location, etc.

Definitions and Rules

The following are used to define Zone interaction and behavior.

Zone Type Zone Types are the highest level of zoning and are used to logically categorize Zone hierarchies. Clients cannot be assigned directly to Zone Types but can be assigned to Zones created within the Zone Type.

Zone Cardinality Cardinality refers to the number of Zones within a Zone Type to which a backup client can be assigned.

Cardinality 1 Each backup client can be assigned to only one specific Zone within a Zone Type (that client may also be assigned to other Zones in other Zone Types). The assignment is not inherited by Zones above the direct assignment. Assignment of a backup client to a Zone in this case will remove the previous Zone assignment.

Cardinality 2 Each backup client can be assigned to any number of Zones within a Zone Type and the assignment is inherited by all Zones directly up to the Zone Type. Assignment of a backup client to a Zone in this case will not affect assignments in other branches of the hierarchy, but remove any previous assignments directly below the current Zone in the chain. NOTE: When a Zone Type already has Cardinality 2, it cannot be changed to Cardinality 1.

Add Zones

1. Select the Zone (or Zone Type) under which you want the Zone to reside.
2. Click the *Add Zone* icon in the right action pane.
3. Enter a name for the Zone (required).
4. Enter a description for the Zone (optional).
5. Click *Add* to confirm the Zone addition.

Zone Types

Bocada provides built-in Zone Types as follows:

Application Recommended for grouping by software applications; ex: SAP, Remedy, Oracle, etc. This default Zone Type has a cardinality of 2.

Customer Recommended for grouping by customer to associate backup servers dedicated to a particular customer. This default Zone Type has a cardinality of 1.

- Department** Recommended for functional or administrative grouping to associate backup servers, backup clients and job groups within your company's organizational structure. This default Zone Type has a cardinality of 1.
- Operating System** Recommended for grouping by operating system. This default Zone Type has a cardinality of 1.
- Priority** Recommended for grouping by the level of importance of backup clients or backup servers. This default Zone Type has a cardinality of 1.
- Region** Recommended for geographical or territorial mapping to which you associate backup clients and backup servers. This default Zone Type has a cardinality of 1.

You can also create your own custom Zone Types. If you need to create a custom Zone Type:

1. Click the *Add Zone Type* icon in the right action pane.
2. Enter a name for the Zone Type.
3. Select a Cardinality Level (1 or 2) via the radio buttons for this Zone Type.
4. Click *Add*.

Assign Clients

Backup Clients can be assigned to Zones from the Backup Clients view in the Configuration section, or via Rules for automatic assignment.

1. Navigate to the Backup Clients view (Configuration Section).
2. Filter report for desired backup clients (optional).
3. Select the backup client(s) intended for assignment to a Zone.
1. Click *Client Properties* in the right action pane.
2. Click the *Zones* tab of the Client Properties wizard.
4. Select the Zone(s) for backup client assignment.
5. Click *Finish*.

Administration : Settings

The Settings view in the Administration section displays the most basic of configurations of Bocada for quick reference. This view and related functionality is available to Bocada Administrators only.

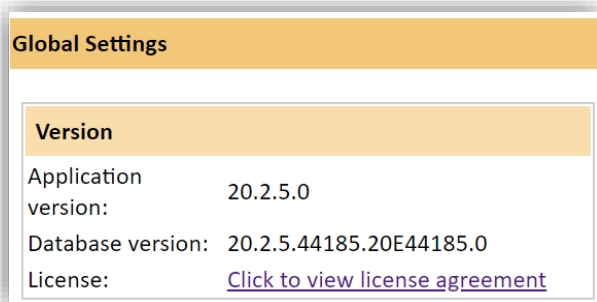
Note: Both the version of the Bocada Application and the version of the Bocada Database (both set during installation) are displayed at the top of the Global Settings, and for Bocada to function properly, these must match. For example, the following are a matching pair:

Application version: 20.2.5.0

Database version: 20.2.5.44185.20E44185.0

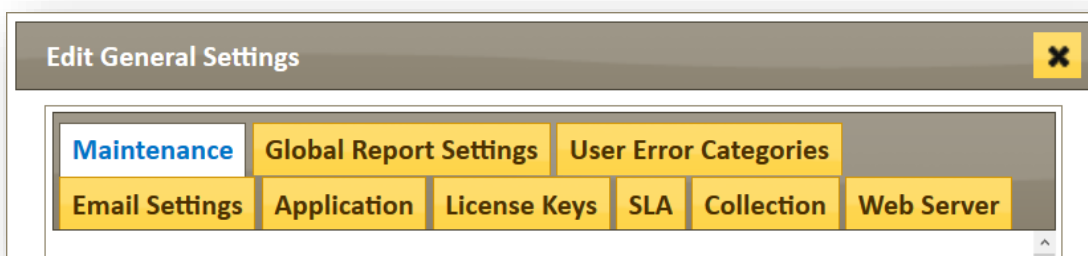
License: Click to view license agreement:

The Bocada EULA (as seen in the installation of both the Data Collection server and Application server) is available by clicking the link provided in the Settings view.



Edit General Settings

Clicking the Edit icon in the Actions panel to the right of the view launches the Edit General Setting wizard, where the many configurations can be viewed and managed.



Maintenance Tab

Maintenance functions selectively prune data based on age or activity as defined by an Administrator. This is useful in limiting database size, and lack of pruning can negatively impact performance as the database size grows. Outdated data collection activity logs are pruned automatically (this setting defaults to every seven days). Server Messages are set to be pruned after 90 days as the default. Pruning other data is not enabled by default, but is recommended to maintain optimal performance unless a complete historical data set is required.

Individual DCS servers cannot be delegated or specified to initiate database maintenance routines; maintenance will be performed by the Master DCS. A Master DCS with slow or remote network connections may negatively impact Database Maintenance performance.

For a listing of specific tables in the Bocada Database affected by each of these settings, see [Appendix D](#). Maintenance jobs run the SQL stored procedure dbMaintenance, in your Bocada database, which prunes records based on your Maintenance settings.

Edit General Settings

Maintenance
Global Report Settings
User Error Categories
Email Settings
Application
License Keys
SLA
Collection
Web Server

Prune Outdated Updates

☐ Backup data: 365 days
☐ Weekly summaries: 52 weeks

☐ Occupancy data: 365 days
☐ Monthly summaries: 12 months

☐ Media data: 365 days
☒ Server messages: 90 days

☐ Policy data: 365 days
☐ Backup events: 2557 days

Prune Outdated Logs
Activity log retention: 7 days
Prune Auto Saved Reports
Auto Saved Reports retention: 24 hours
Prune Outdated Backup Clients
☐ Clients retention: 365 days
Prune Saved Reports
☐ Saved reports data: 45 days
Prune Orphan Assets
☐ Orphan Assets retention: 15 days
Prune Outdated requests
☒ Requests: 35 days
Prune Outdated Snapshot Files
Snapshot Retention: 7 days

Prune Database Maintenance Window
Maximum duration: 2 Hours
Maximum number of rows being pruned per attempt
Maximum rows per attempt: 1000 rows

Schedule to Update Weekly and Monthly Summary
Mo,Tu,We,Th,Fr,Sa,Su at 4 AM GMT - [Edit Schedule](#)
Update Summary timeout: 300 minutes

Previous
Next
Finish
Cancel

Prune Outdated Updates

To specify a setting for one of the update categories, select the check box for the item and specify the age of the data that is pruned. The following maintenance functions are available:

Backup data	Prunes backup data older than this setting. Range: 31-10000 days.
Storage data	Prunes Storage data older than this setting. Range: 31-10000 days.
Policy Data	Prunes policy data older than this setting. Range: 31-10000 days
Weekly summaries	Prunes weekly summaries. Range: 1-10000 weeks.
Monthly summaries	Prunes monthly summaries. Range: 1-10000 months.
Server messages	Server message data is collected during backup updates and is displayed in the Server Activity report in the Configuration > Advanced Config. section. This data relates to backup server processes but not directly to backup operations. Range: 3-10000 days.

Backup events Prunes backup events from the Job Message log. Range: 3-10000 days.

Prune Outdated Logs

Activity log retention: The activity log lists the events performed by the Bocada each time data is collected. These logs are displayed in the Data Collection status details. Range: 3-10000 days; about 30 days is suggested setting.

Prune Outdated Backup Clients

Select this option only if you want to permanently delete backup clients with no daily, weekly, or monthly job data from the reporting database. Once a backup client is pruned, no historical data will be available for it. This setting gradually removes your production application servers that have ceased to be treated as backup clients, and the rate of this process depends on the backup log pruning setting. An inactive backup client is retained in the database so long as it is associated with data in the summary tables. If the daily, weekly, and monthly logs are pruned frequently, inactive backup clients are pruned frequently. If these tables are never pruned, inactive backup clients are retained indefinitely.

Important Note: Backup reporting data cannot be retrieved after backup clients have been pruned. Bocada recommends that this setting be left blank, unless you know that you have a need to prune outdated backup clients.

Prune Orphan Assets

Orphan Assets retention: Select this option to delete assets (targets) with no Clients from the reporting database. As above, an inactive asset is retained in the database so as long as it is associated with data in the summary tables. Range: 7-10000 days.

Prune Auto Saved Reports

Saved reports data: Auto-saved reports are pruned after the time specified by this setting if they have not been scheduled. Range: 2-120 hours.

Prune Saved Reports

Saved reports data: User created saved reports are deleted when they have not been accessed within the time specified by this setting (default is 30 days, range: 1-10000 days), and the saved report is:

- Not assigned to a summary dashboard configuration.
- Not assigned to an alert.
- Not assigned to a scheduled email or export configuration.
- Not set as the default report for any users.
- Not a template created during installation.

Prune Outdated Snapshot Files

By default, Snapshot files are retained for 7 days. When data collection (beupdate.exe) runs, it removes any snapshot files which are older than "Snapshot Retention" days in the following folder:

```
C:\Program Files (x86)\Bocada\DataCollection\snapshot
```

Prune Database Maintenance Window

This setting determines the length of time the maintenance task will run before timing out and stopping. Default is 120 minutes.

Maximum Rows Pruned per Attempt

This setting determines the number of rows that are set to be pruned that are committed to the Bocada database in a single batch. Range: 1-3000 rows.

Maintenance Schedule

By default, the schedule for Bocada internal database Maintenance tasks is set to run every day at 04:00 GMT, but can be changed to run at any weekly or monthly frequency. The schedule is named *Pruning, Database Maintenance* for all pruning except for *Weekly Summaries* and *Monthly Summaries*. The pruning schedule can be edited by the usual *Schedules* view under *Configuration*. Pruning for monthly & weekly schedules is controlled by clicking on *Edit Schedule* under *Schedule to Update Weekly and Monthly Summary* at the bottom of the Maintenance tab.

You can see the history of the pruning runs in the *Configuration > Advanced Config. > Scheduled Actions* view. The *Database Maintenance* Operation Type only does the *Weekly Summaries* and *Monthly Summaries* pruning. All other pruning is done by the *Pruning, Database Maintenance* Operation Type.

Global Report Settings Tab

The Global Report Settings tab contains global default settings related to Time Zone, default global Error Set, Backup Day, Export Settings, and Custom Logo specification. Adjustment of these settings has immediate impact on report templates and saved reports.

Time Zone

Set this to be the most commonly used time zone in your environment. Data Collection datetimes and Activity messages will be displayed in this time zone.

Error Set

The definition of backup outcome criteria can be adjusted in Bocada. By adjusting error sensitivity, reports can be molded to reflect backup policies of different organizations or to meet other reporting goals. For example, it may be desired that failed backups which only failed because of “Locked File” errors be considered successful.

The setting “Normal” means:

- The job will show as a Failure (red) if the error occurred and zero bytes were backed up.
- Partially Successful (yellow) if the error occurred but bytes were backed up, and no other errors which are set to “Always Red” were encountered.

The default error set is adjusted by clicking the “Set error definitions” link. The default Bocada reports, and individual reports saved with the “Global Default Errorset”, are governed by this setting. Note that Individual reports can be also saved using a custom error set definition.

On installation, equal weight is given to each error, regardless of its error category. Bocada error definitions are detailed in [Appendix B: Error Definitions](#).

Success for Zero Bytes and Zero Errors

It is often desirable to consider a job with zero bytes and zero errors as successful. These checkboxes allow different types of jobs to be considered successful even with zero bytes / errors.

Backup Day

This defines the start time of a 24-hour Backup Day so that it does not have to correspond with a calendar day. The backup day affects “Best Attempt” outcomes in reports such as Backup Activity because a re-run of a failed backup must be started in the same Backup Day as the failure to count as the Best Attempt for that job on that day. This setting also affects the Backup Day date shown in reports such as the Job Trends report. For most environments, the majority of backups are run during off hours (typically running overnight), so Bocada recommends setting your Backup Day to begin at “Noon Today”, unless your environment has different specific tracking needs.

For example, a backup that is run at 9:00pm and fails can be rerun the next morning at 7:00am and, if successful, will count as the Best Attempt for that backup day so long as both times are in the same backup day.

A backup scheduled to run near midnight might start a little before midnight some days, but might be queued and start a little after midnight on other days. Having the backup day start at Noon Today ensures that the backups are shown on consecutive days instead of having 2 backup jobs on one day, and no backup jobs on another day.

The Backup Day date shown in reports is the day that contains the greater number of hours. For example, consider a backup started at 1:00 am Tuesday. Despite the backup starting on the calendar Tuesday, many organizations consider this a Monday night backup. Setting the Backup Day to begin at “Noon Today” will make backup be displayed as a Monday backup attempt.

Export Settings

This defines authentication, and pruning functionality of all scheduled report exports, and the default UNC Path location. During scheduling of a report for file export, users can specify this default or non-default export location. Any non-default location specified while creating a *scheduled* export must be accessible to the default Bocada user credentials in the global export report settings.

Inactive clients

Clients will be considered Inactive after a configurable number of days, and are not shown in reports and report criteria, based on this setting.

Custom Logo

Bocada can be configured to use a custom logo for exported and emailed reports, along with branding of the Bocada reports. This can be done by browsing for and selecting a desired logo, and clicking the ‘Upload Files’ button. Please note the recommended resolution for each logo:

- Report Export Logo: 770 x 130
- Product Logo: 189 X 30.

The Bocada Product logo is located by default on the master application server in this file:

C:\Program Files (x86)\Bocada\Application\WebUI\images\white-logo.png

To change the logo displayed at the top of the Bocada application browser window:

1. click "Choose File" next to Product Logo
2. navigate to an image file of the proper dimensions and click on it
3. click "Upload Files"
4. your browser will have cached the previous image, so test by clearing all images out of your browser cache, or running in a new browser window in incognito mode
5. NOTE: the previous image file will be retained in the same directory but renamed to a file *white-logo.png.M_DD_YYYY_HH_MM_SS.bak* in case you need to revert to any previous image.

To change the logo displayed at the top of reports sent by Bocada, click "Choose File" next to Report Export Logo, navigate to an image file of the proper dimensions, then click "Upload Files". This image will be stored in the directory:

C:\Program Files (x86)\Bocada\Application\Logos\ExportLogo\pdflogo.bmp

Note that the previous image file will be *not* retained in case you need to revert to any previous image, so a backup should be done manually if you wish to wish to revert to the original Bocada logo, or any previous logo, if desired in the future.

Zone Enforcement

As explained in the Users section of this document, Operators and Standard Users can be set to have limited access to backup client data, based on backup clients in zones and User assignment to zones. This feature allows for restrictions to be removed for either or both roles so that these user types have unlimited access to backup client data.

Should you choose to use Zone Enforcement, Operator and Standard User roles must be enabled for the appropriate zones for these roles to see any reports. For this reason, Bocada recommends that you restrict report viewing only if required in your environment.

Edit Servers

×

Veeam

Schedules

Settings

Finish

Data Collection Server:

dev-ws01.bocada.com

Configure Server Properties:

SQL Server Name

default

SQL Instance

veeamsql2012

SQL Database

veeambackup

Database Authentication

Windows

User Name

testlab\pradmin

Password

Time Zone

(GMT-08:00) Pacific Time (US & Canada);

Show Advanced Properties

TEST CONNECTION

Testing the connection to the servers will save the servers' properties.

CANCEL

PREVIOUS

NEXT

FINISH

Custom Logo

Image size can not exceed 4096 KB.

Report Export Logo

Recommended resolution is 770 X 130.

Choose File

No file chosen

Product Logo

Recommended resolution is 189 X 30.

Choose File

No file chosen

Icon for showing Job Trends Partial that have only file errors

Recommended resolution is 18 X 18.

Choose File

No file chosen

Upload Files

Zones

Enforce zones for:

Operators and Standard Users

☒ Auto-zone clients by server time zone

Date Format

Date format of trend reports:

MM/DD

Custom View For Reporting

Custom view for reporting:

default

Previous

Next

Finish

Cancel

Time Zone Auto-zoning





To enable auto-zoning by time zones, click the checkbox under Zones "Auto-zone clients by server time zone" as shown in images above.

As soon as you run data collection for any server, all clients on that server will be zoned to a new zone that is named with the time zone name in a zone type "Time Zone". The time zone is set based on the server time zone as shown in "Edit Servers" dialog.

All clients will be zoned by time zone when rules or data collection is run for the server.

Administration : Zones

Actions



Report criteria

	Name	Zone Type\FqName	Description
<input type="checkbox"/>	• Time Zone	Time Zone\	Backup Server Timezone
<input type="checkbox"/>	• (GMT+05:30) Chennai, Kolkata, Mumbai, New ...	Time Zone\GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi	Zone for autozoning based on server time zone
<input checked="" type="checkbox"/>	• (GMT+06:00) Sri Jayawardenepura	Time Zone\GMT+06:00) Sri Jayawardenepura	Zone for autozoning based on server time zone
<input type="checkbox"/>	• (GMT-05:00) Eastern Time (US & Canada)	Time Zone\GMT-05:00) Eastern Time (US & Canada)	Zone for autozoning based on server time zone
<input type="checkbox"/>	• (GMT-08:00) Pacific Time (US & Canada); Tiju...	Time Zone\GMT-08:00) Pacific Time (US & Canada); Tijuana	Zone for autozoning based on server time zone

Zone Clients

Client	Server	Contact	Zones	Job Group	Product	Last Job Timestamp	Go
778020575969 us west (...)	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	Unassigned	Veeam		Un
bocada-sql-test	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	Unassigned	Veeam		Un
f-linuxagent-wrong-por...	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	Foreign transform	Veeam	2022-07-20 00:45:28	Un
metallic-mysql-db-insta...	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	Unassigned	Veeam		Un
s-efs-2-aws-app-taw-a...	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	S-EFS-2-aws-app	Veeam	2022-07-20 13:05:04	Un
s-longrunning-wc01-2-d...	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	S-Backup-to-Tape-GFS...	Veeam	2022-08-01 09:30:14	Un
s-vm-wc12-2-cifs	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	S-Backup-to-Tape-Non...	Veeam	2022-07-20 22:45:13	Un
taw-aws-efs-02	tl-vem-ws01-postcopyple...		Time Zone\GMT+0...	S-EFS-2-aws-app, taw...	Veeam	2022-08-03 00:35:07	Un

Re-Zoning Clients to a New Time Zone

1. Set time zone for backup server to a new time zone
2. Run either backup collection or policy collection for the backup server

Note: Backup data in Bocada database is set to the time zone the server was assigned at the time of collection.

User Error Categories Tab

The error sensitivity (error set) functionality allows Bocada Administrators to determine how a given error category is evaluated in reports. Most Bocada users find the default error categorizations are accurate for their environment. User Error Categories can be created to govern specific backup product errors so that they can be treated separately from their default group.

Note: Please inform Bocada if you find a need to modify the error categories as described below, so that we can consider modifying the default error categories in our next release.

For example: Suppose four low-impact errors are identified for a given backup product and a decision is made to ignore them, as the backups are still recoverable even if these errors occur. By default, these are grouped with more severe errors of the same type, so that the entire error Bocada set definition cannot be ignored. In this example, however, a custom category can be created, assigned these errors, and set to display Always Green in the Error Set Definitions.

Add an Error Code

1. Click the triangular icon to the left of the desired Error Category.
2. Click the *Add (+)* icon.
3. Select the Product and enter the proprietary error code from the backup product.
4. Click Submit to close the Add Record wizard.

Note: Each customized error row is limited to one proprietary error code.

Delete an Error Code

1. Click the triangular icon to the left of the desired Error Category.
2. Highlight the Row of the desired error code.
3. Click the *Delete (-)* icon.

Edit an Error code

1. Click the triangular icon to the left of the desired Error Category.
2. Highlight the Row of the desired error code.
3. Click the *Edit* icon.
4. Update the desired fields.

Rename an Error Category Name

1. Highlight the desired *Error Category Name* row (next to the triangle icon).
2. Click the *Edit* icon at the bottom left of the wizard.
3. Enter the desired name of the Error Category and click Submit.
4. Recommended that the User Error Category names are *Always Red*, *Normal*, and *Always Green* to make it clear what the purpose of each group is.

Defining Treatment of Error Category

Once the desired updates have been made to the User Error Categories, finish the Edit General Settings wizard to implement the newly defined behavior. Treatment of these new error categories can now be done from the Global Report Settings tab after re-launching the Edit General Settings wizard.

Note: New error categorizations will only apply to newly collected data, not previous collections.

Email Settings Tab

Email settings define the mail server and account used to send emails from Bocada including emailed reports and alerts. The Hyperlink / URL used for links to the Bocada application UI can also be configured here, if different from the Hyperlink / URL as seen from the Bocada Application server.

Note:

- The Bocada Application Server must have SMTP connectivity to the mail server to send email.
- To disable the Hyperlink / URL in emailed reports, simply uncheck setting 'Include report URL in emailed reports' (enabled by default).

Email Settings

Mail Server:

SMTP Port: Default: 25

☐ Send Email anonymously

Account name: Use format: "user@domain.com"

Password:

Sender Email:

Sender Name:

☒ Require SSL

☒ Include report URL in emailed reports

Report URL

URL on Emailed Reports:

Examples:

http://machineName.company.com/
http://machineName.company.com:port/
http://machineName.company.com/Bocada/
http://machineName.company.com:port/Bocada/

- **Mail Server** (required field): The name of the Mail Server used to send email
- **SMTP Port**: Will default to 25 if left blank
- **Send Email anonymously**: Provides option to send email anonymously if authentication is not required by the mail server
- **Account name**: The account used to send email, if not sent anonymously
- **Password**: The password of the account used to send email, if not sent anonymously
- **Sender Email**: Displayed as the sender email address on emailed reports
- **Sender Name**: Displayed as the sender name on emailed reports, not required
- **Report URL**: May be used to specify a Hyperlink / URL to appear on reports as the link to the report page

Application Tab

SQL Connection

The SQL settings are the settings which the Bocada Application uses to connect to the database. To edit the SQL settings:

SQL server The fully qualified domain name (FQDN) of the SQL server on which the Bocada database is installed. If the database resides on a named instance, it will be with appended to the FQDN using a backslash. Ex: `servername.domain.com\instance`.

DB Name The database name of the Bocada database. The default is “Bocada”

Windows Authentication If Windows Authentication is used, it will use the Bocada Application Service User authentication to connect to the database. If the service user is not a domain user, then Windows Authentication will not work for connection to the database.

User Name This is the SQL Authenticated user and will be disregarded when Windows Authentication is selected.

Password This is the password for the SQL authenticated user entered above and will be disregarded when Windows Authentication is selected.

Seconds before timeout This is the number of seconds that the application can stay open before the SQL connection times out.

Important Note: Regardless of authentication type used, the user must have DB Owner (dbo) permission to access the Bocada database.

Application Settings

The application server log path and level can be specified for use in troubleshooting application performance or security logging. This should only be changed if disk space is limited in the default log path location.

License Keys

See separate document on updating license keys here:

<https://bocada-support.force.com/s/article/How-to-Update-Bocada-License-Keys>

License Key Values

License keys are specific for the following Bocada deployment values:

- SQL Server Fully Qualified Domain Name (FQDN)
- SQL Instance name (Default is no instance)
- SQL Port (Default is 1433)
- Database name (Default is Bocada)

Red Text represents an invalid or expired license.

Yellow Text represents a valid license will expire within the next 30 days.

Back Text indicates a valid license.

License Warnings

Licensing issues will produce warning messages that are displayed in the top banner section next to the product logo. These are visible only to Administrators and Operators.

Exceeding Licensed Units

This message indicates that current usage exceeds the purchased licensed amount. You can run the License Count report in the Administration section to determine where the units are being used. This can be resolved by deleting Servers from Bocada, or by purchasing additional Units from [Bocada Finance](#).

The definition of a unit and how the unit count is calculated is detailed in the Bocada End User License Agreement (EULA).

License Expiration

When the license is due to expire, a message will display as an orange warning when within 31 days of expiration, and a red warning when within 10 days of expiration. **Note:** Once the License has expired, data collections will not run and you will not be able to see reports. To avoid possible loss of data, contact [Bocada Finance](#) to renew your license prior to the expiration date.

Scheduled License Count Email

This setting enables the [License Count](#) report to be automatically sent to the emails listed under 'Recipient Email Address' according to the schedule "Auto Monthly License" (defaults to the first Monday of each month).

SLA Tab

The SLA calculation governs how much historical data to use for the initial calculation of SLA compliance; this is limited by the time-span of historical data collected on the initial update.

When checked, the *Impacted SLA Dialog* is displayed as a pop-up in the Activity reports when data which affected an SLA profile is present in the report. The Impacted SLA dialog can be dismissed by the individual user for the remainder of their session when encountered, but this setting allows it to be disabled or enabled globally for all users.

Collection Tab

The setting in this section governs global data collection settings, as well as settings for specified data collectors when multiple collectors have been installed.

Data Collection Process

The setting for *Minutes before timeout* determines how long data collection updates will run before timing out. By default, the timeout is set to 120 minutes; This setting can be extended if you find that your collection updates are taking more than two hours to complete.

The setting *Backup collection chunk size* determines the limit (in hours) of the time span collected and committed to the Bocada database. Note that this is the Global setting, and may also be set within the Settings for each Backup Server. By default, this is set to 24 hours, but may be set as low as 12 or as high as 48 hours.

Data Collection Settings

The settings in this section govern the individual Data Collection Server chosen in the drop down.

Enabled: Determines if the Data collection server is enabled and available. Data Collection Servers are disabled automatically when the service is uninstalled, or can be disabled manually here. Collections will not run for backup servers assigned to a disabled Data Collection Server.

Snapshot Location: The snapshot location is where the data is stored during collection prior to being committed to the database (Default location: C:\Program Files (x86)\Bocada\DataCollection\snapshot). This data remains for a period of time after updates are completed and can be used for troubleshooting. The amount of time snapshot data remains in the directory can depend on plugin type and the properties of the Backup Server.

Important: If you change this snapshot folder location, be sure to copy the files from the old location to the new location first. Here is how move the data collection and snapshot folders to a new disk:

1. Stop the DCS service on the DCS that you will move the log & snapshot folders.
2. Create the folder structure in the new disk. It is suggested that you use the same folder structure as in Bocada default, changing only the disk drive letter, so they can be easily found. Default location is:
 - C:\Program Files (x86)\Bocada\DataCollection\snapshot
3. Copy the old snapshot folder & subfolders to the new location. Some backup job data is temporarily cached in these snapshot files for some backup products.
4. Change the snapshot & log location in Bocada setting as shown in the screenshot above, preferably by only changing the C drive letter to your new disk.
5. Restart DCS service

Log File Location: The log location is where the logs of the data collection processes are stored and can be located for troubleshooting (Default location: C:\Program Files (x86)\Bocada\DataCollection\log).

Concurrency Settings: Determines how many collection updates or report generations can be run concurrently (Default: 3 for each). Concurrency is specified individually for each type: Backup, Storage, Media, Policy, In Progress, and Report Generation.

Logged Services: Additional services can be logged to the log file location to be used for troubleshooting. Bocada Support may ask for one or more of these to be enabled when diagnosing a Support Case issue. Most of these, when selected, generate a single log file from a single service; Setting 'Log Extended Info' provides more verbose logging from certain services.

Web Server Tab

The Web Server Log Path sets where the BocadaWebUI.log file will be written on the master Application server. Default location is: C:\Program Files (x86)\Bocada\Application\Log\BocadaWebUI.log.

Administration : Rules

Rules enable automatic assignment of new Backup Clients to [Zones](#), [SLA Profiles](#) and [Price Lists](#) as they are discovered by Bocada. Client assignment is performed by the Rules process that runs every four hours by default, based on the editable schedule 'Rules Incremental' located in the Schedules view. Rules are evaluated in order; higher-order Rules are processed first. Rules are only applied to newly discovered Backup Clients. The 'Date Last Run' in this report indicates the last time a client met that rule's criteria and was so assigned; 'Date Last Run' remains blank until a client meets that rule's criteria.

Rule Order

Rules of higher order take precedence over lower order Rules when the assignment criteria overlap. If a Backup Client matches the criteria defined in one Rule but a higher-priority rule has already been applied, for the same item type, to that client, then the results of the higher-priority rule will remain.

Here is an example of how rule-order precedence works:

Suppose you have a new backup client named: *win2012_exch_can*

Suppose you have four separate rules, defined as follows, in this precedence order:

1. If client name matches **_can** then put it in Region\Canada zone
2. If client name matches **_exch_** then put it in Application\Exchange zone
3. If client name matches **win2012_** then put it in OS\Windows\2012 zone
4. If client name matches **_ca** then put it in the Region\USA\California zone

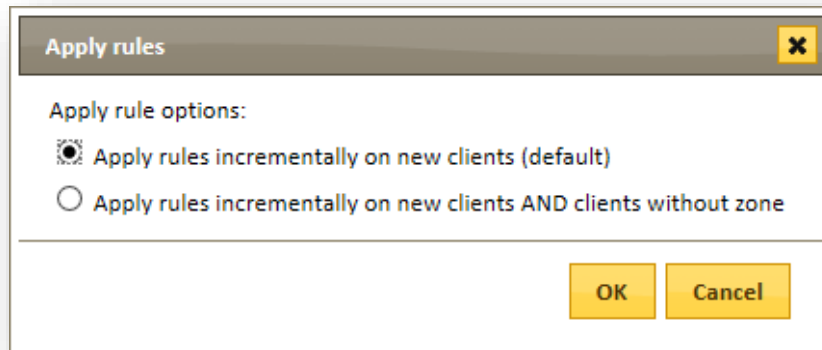
The new client matches the criteria for all four rules. Because the first three rules are each assigning the client to a different zone type, each of the three rules will trigger on the client, and make their assignments regardless of their order, so long as they are above the last rule. The last rule is also trying to assign a Region-type zone, but because a rule of higher precedence has already assigned a Region type zone, Rule #4 will not assign anything and the client will be assigned to Region\Canada. If Rule #4 was moved to the top of the list, then this client would have been assigned to California instead of to Canada.

Rules can be reordered by moving up, down, or directly to the first, last, or a relative position, with the following actions:

- Move Up
- Move Down
- Move To...

Run All Rules

Selecting Run All Rules from the right Action panel will run all rules immediately, in order, on any newly-discovered clients.



Option 1: Apply rules incrementally on new clients (default) – this simply runs the normal rules job now instead of waiting for the next scheduled run.

Option 2: Apply rules on all clients incrementally – Will apply rules on new clients AND those clients that have not been assigned to the zones, price list, and/or SLA that match the rules selection criteria.

Add, Edit and Copy Rules

Rules can be created or changed using the Add Rule or Edit Rule action from the right panel. These will launch a Rule wizard:

Add Rule

Rule Name:

Group:

Find with: matches

In: [Criteria](#)

Actions to Apply

Assign to Zone(s) [Edit](#)

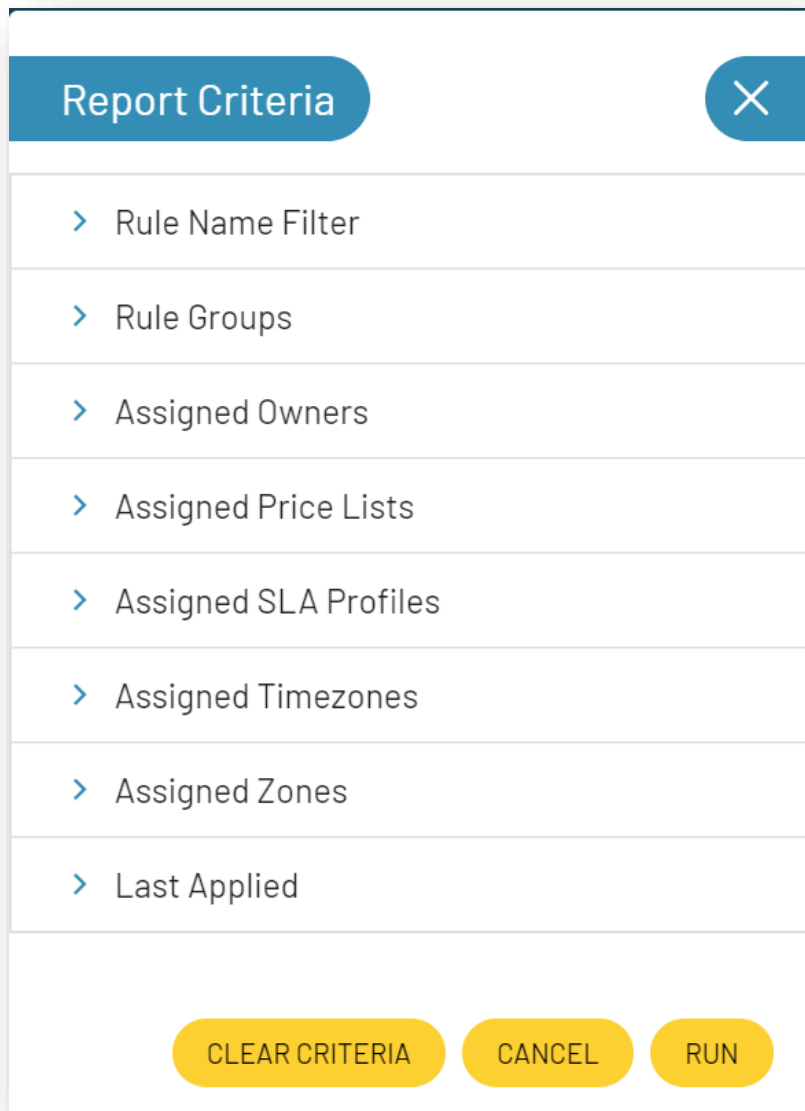
myZoneType
test_01

Price List:

SLA Profile:

Finish **Cancel**

Clicking the Criteria link within the Rule wizard will open a wide array of criteria Administrators can use to recognize and assign new clients:

A dialog box titled "Report Criteria" with a close button (X) in the top right corner. The dialog contains a list of criteria, each preceded by a right-pointing chevron (>). The criteria are: Rule Name Filter, Rule Groups, Assigned Owners, Assigned Price Lists, Assigned SLA Profiles, Assigned Timezones, Assigned Zones, and Last Applied. At the bottom of the dialog are three yellow buttons: "CLEAR CRITERIA", "CANCEL", and "RUN".

Report Criteria
> Rule Name Filter
> Rule Groups
> Assigned Owners
> Assigned Price Lists
> Assigned SLA Profiles
> Assigned Timezones
> Assigned Zones
> Last Applied

CLEAR CRITERIA CANCEL RUN

Rules can also be copied by using the Copy Rule action. Using the Copy Rule action will load the recognition and assignment criteria as defined in the currently highlighted rule.

Client Recognition

Backup Clients are discovered as they are added to Bocada based on string pattern matching with wildcards for:

- Backup Server name
- Client name
- Job Group name
- Media Server name
- Target name

Wildcard Note: '?' is interpreted as 'any single character' and '*' as 'any characters'.

Clients can also be discovered using standard Bocada criteria, as above.

Client Assignment

Backup Clients matching the rule criteria can be assigned to any combination of one Price List, one SLA Profile, and multiple Zones.

Rules Schedule

The rules process runs every four hours (by default) as defined by the *Rules Incremental* schedule. As with all schedules, this schedule is editable in the Configuration module, from the Schedules view. Selecting [Run All Rules](#) from the right Action panel will run all rules immediately, in order, on any newly-discovered clients, without waiting for this schedule to launch the process.

Administration : Rule Groups

Rule Groups enable grouping of [Rules](#) for organizational and rule evaluation order purposes.

Administration : License Count

The License Count is a tabular report that shows the active [Unit](#) counts of Bocada, broken out by Backup Server Units, Media Server Units, Backup Client Units, and Unassigned VM Units, by backup product. This report also compares the current Licensed Units to the Active Units.

The bottom section of the License Count view provides insight into how the Unit count is calculated. The details include the backup servers, clients, date of last backup for each client and correlated VM name if applicable.

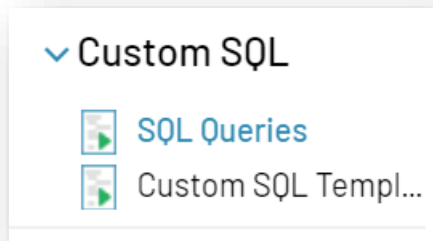
Bocada Finance will request a semi-annual License Count report, or "True-Up", to ensure customers are not using more Units than they are Licensed for. If so, they may be required to purchase additional licenses.

Advanced Module

The Advanced Module includes the views listed below. The Advanced Module is only accessible to Bocada Administrators.

Advanced : Report Usage

Reports Usage shows you metrics about which Bocada reports were run, by whom, with what criteria and when they were run. The below screenshot shows you how to see the report criteria.



Write or paste the SQL query that you wish to run into the “Edit SQL” textbox under the Report criteria:



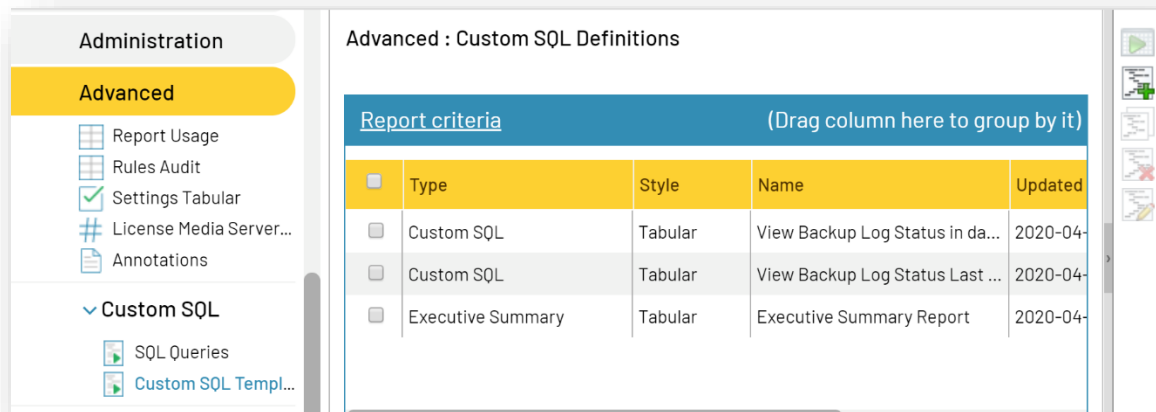
Saved SQL Query reports will appear under Saved Reports as Report Type *Admin SQL Queries*.

Advanced : Custom SQL : Custom SQL Templates

Custom SQL Report templates are defined, managed, and run through this interface. Administrators can run and manage any Custom SQL report template.

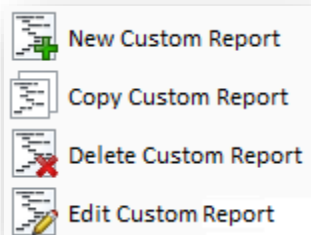
Once a custom report template is added via this view, then users can see, run, and save Custom SQL reports with their own criteria via the Saved Reports view. This is the only place where saved versions of a custom report type can be run.

You can add and manage custom SQL report templates, as well as run the base template, in the Custom SQL Templates view.



How to Add a New Custom SQL Template Report

Writing Custom SQL Templates for Bocada is covered in *Appendix C: Writing Your Own Custom SQL Reports*. Once you have the SQL code for a new report, perhaps from Bocada Professional Services, then you can add it to your Bocada Deployment by using these actions:



Click New or Edit Custom Report icon button to see the dialog.

Edit 'Failures with Error Message Samples' report's criteria

Name: Failures with Error Message Samples

Show report to: ☐ Administrator ☐ Operator ☒ Everyone

Report SQL:

```
-- AllJobs custom Template v8.20160526.1
-- Note: all reported times in backup server time, aka local - no TZ conversions
-- Note: date range times in GMT

-- proc to handle zone security for backup clients criteria
EXEC UmpConvertZoneCriteriaToClients
--select * from #criteria -- DEBUG

-- values used for zone security in the query
DECLARE @show_unzoned_clients BIT
DECLARE @has_user_id BIT
SET @show_unzoned_clients = (SELECT value_bool FROM #criteria WHERE
criteriaName = 'ShowUnzonedClients')
SET @has_user_id = CASE WHEN EXISTS(SELECT value_string FROM #criteria WHERE
criteriaName = 'UserSid') THEN 1 ELSE 0 END

-- report criteria available to the user
DECLARE @backupproducts_isnegated BIT
```

Sum columns:

Columns should be entered as comma separated values with no names repeated.

Finish Cancel

Give the template a name, set the custom report accessibility with the radio buttons. Paste your SQL text into the Report SQL text box. When columns are added to the 'Sum columns' section, the report will appear as before but with those columns first and the sum of those columns' values at bottom.

Click Finish, and then run your base template report!

Only administrators can edit the SQL code. When access is granted to non-administrator roles, they will only be able to run the report from the Saved Reports view and edit and save and with their own criteria.

Saved Custom SQL Templates will appear under Saved Reports as Report Type *Custom SQL* as Templates.

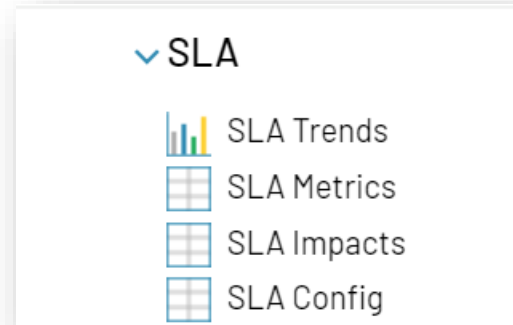
Custom SQL Criteria

It is possible to write criteria into Custom SQL Templates which can be set to filter data through the same mechanisms of standard Bocada reports. These report templates can then be managed through the Saved Reports interface, run and saved with different criteria filtering applied. For example, Custom SQL reports may be created from the same template with different criteria for different end users. More information on this functionality can be found in [Appendix C](#).

Note: Due to changes in the Bocada database in version 10.6, several fields formerly defined as type INT are now type BIGINT. If your Custom SQL report encounters errors after upgrading, it may be necessary to change variables formerly defined as type INT to type BIGINT.

Advanced : SLA

Service Level Agreement (SLA) reports are an additional feature to track and troubleshoot SLA compliance. Bocada SLA reporting can be configured to depend on many different definitions and uses of SLA procedures.



The SLA section is visible to Administrators and Operators; however, the Manage SLA functionality is only available to Administrators. To best address specific SLA needs, Bocada Support is available to discuss available options for different requirements.

Workflow Overview

The following steps describe the process from defining SLA Profiles to viewing the compliance results.

1. Define SLA Profiles, as described in the [SLA Configuration](#) section.
2. [Assign Backup Clients](#) to SLA Profiles using the Backup Clients View.
3. Allow time for SLA Calculations to run. Calculations will need to be re-enabled if previously disabled.
4. Run the SLA Trends Report to view the percentage of SLA compliance on each day.
5. Drill into the SLA Trends or Metrics reports to view assets that have not complied with SLA requirements as defined in your SLA Profiles.

Advanced : SLA : SLA Trends & Advanced : SLA : SLA Metrics

Daily backup SLA results are displayed in the following ways:

- If a daily backup is required, jobs that have not run during the backup day will be displayed as Gray: *No backup attempts yet*.
- When the backup day has ended, jobs that have not run are displayed as Red: *Did not meet SLA*.
- Failed backups are displayed as Red: *Did not meet SLA*. This status can change to green with successful backup attempts during the same backup day.

Weekly or monthly backup SLA results are displayed in the following ways:

- When a weekly or monthly backup is required but the week or month has not completed, absence of the weekly or monthly backup will be considered in each day's SLA compliance metric as Gray: *No backup attempts yet*.
- Once the weekly or monthly backup is completed, all previous days in the week or month will reflect the result.
- If the backup week or month has completed and the weekly or monthly backup still has not been run, the result will be reflected in each day as Red: *Did not meet SLA*.

Advanced : SLA : SLA Config

The SLA Config view in the SLA section enables Administrators to create and manage SLA Profiles. SLA profiles must be configured and assigned to clients prior to running SLA compliance reports.

When you click on SLA Config, you will be shown up to two rows per SLA profile, one for each type of frequency requirement that you define.

Levels

The following levels count for each category:

Full	'Full'
Any	'Archival', 'Differential', 'Full', 'Incremental', 'Manual', 'Other', 'Partial', 'Unknown', 'Severed', 'Duplicate', 'Replication Read', 'Replication Write', 'Synthetic Full'
Not Counted	'Recovery point', 'Snapshot', 'Restore', 'Verify', 'Skipped'

Definitions and Rules

Compliance criteria for SLA profiles have the following options for Full Backup and Any Backup attempts:

Per Active Day	During the current backup day any attempt to perform a backup on a target requires a successful backup of that target. If no attempt is made there will be no calculation for the assigned clients.
Daily	This calculation requires a backup of all targets on all assigned clients regardless of attempts during the backup day. No attempts during a backup day will be deemed as failure to comply with SLA.
Weekly	This calculation requires a backup of all targets on all assigned clients regardless of attempts during the week. No attempts during the specified week will be deemed as failure to comply with the SLA.
Monthly	This calculation requires a backup of all targets on all assigned clients regardless of attempts during the month. No attempts during the specified month will be deemed as failure to comply with the SLA.
No Requirements	The specified backup requirement is not part of this SLA.

Backup window	Allows for SLA Profiles to only look at jobs that begin in specific Backup Windows, as well as to include or exclude weekends as having Backup Window restrictions.
----------------------	---

Add SLA Profile

1. Click the *Add* icon from the right Action panel. This will open an SLA Profile wizard.
2. On the Name tab, enter a Name (required) and Description (optional). Click *Next*.
3. Choose any error categories that can be ignored (optional). Click *Next*.
4. Configure compliance criteria for the SLA profile (see above). Click *Finish*.

Edit SLA Profile

The workflow to edit an SLA Profile is similar to that for adding one:

1. Highlight an SLA Profile
2. Click the *Edit* icon from the right Action panel. This will open the SLA Profile wizard.
3. On the Name tab, edit the Name and Description (if desired). Click *Next*.
4. Choose any error categories that can be ignored (optional). Click *Next*.
5. Configure compliance criteria for the SLA profile (see above). Click *Next*.
6. Additionally, whenever you edit the attributes of an SLA profile, there is an option for how far back to recalculate the SLA profile with the new compliance criteria. This defaults to 3 days, but this time-span should be increased to beyond the SLA time criteria; For example, with pruning set at three days, a weekly backup that is successful on Friday would be pruned from the records by Monday and would appear to be out of SLA compliance when the report is viewed on Wednesday.
7. Click *Finish*.

Assign Backup Clients

Clients can be assigned to an SLA profile using the [Backup Clients](#) view in the Configuration module. This view shows other aspects of the clients and permits sorting and grouping, in order to assign clients to your desired SLA Profile.

1. Navigate to the Configuration module, Backup Clients view.
2. Filter report for desired clients (optional).
3. Select the backup client(s) intended for assignment to an SLA profile.
4. Click *Client Properties* in the right action pane.
5. Click the *SLA Profile* tab of the Client Properties wizard.
6. Select the SLA Profile for client assignment.
7. Click *Finish*.

Note: Each backup client can only be assigned to one SLA profile. All active targets on the client must meet the SLA requirements.

Advanced : Policies

These reports display the backup policies, or backup configurations for various supported backup products. The data reported includes name, type, schedules, backup clients, targets, and retention, among other configuration variables. The Change Analysis report also reports on changes to policies for NetBackup and TSM.

Advanced : Policies : TSM Policy Reports

TSM Policy views display information gathered from TSM Policy collection. These views display TSM Policy configurations and TSM Clients associated with TSM Policies.

Advanced : Policies : NBU Policy Reports

NBU Policy views display information gathered from NetBackup Policy collection. These views display NetBackup Policy configurations and NetBackup Clients associated with NetBackup Policies.

Advanced : Policies : Change Analysis

Change Analysis reporting is included for tracking changes to NetBackup & Spectrum Protect (TSM) Policies.

Advanced : Policies : NBU SLP (Storage LifeCycle Policy)

NBU SLP section contains views specific to NetBackup LifeCycle Policies. These reports display NetBackup LifeCycle Policy configurations, trends, and protection of the LifeCycle policies.

Other Reporting Modules

See the Bocada Reporting Guide for information about reports beyond Bocada Administration.

Contacting Bocada

Bocada Customer Support

Email: support@bocada.com

Phone: 425-898-2400

Both new and existing customers who are active subscribers to annual support and maintenance have full access to post-installation support:

- Online knowledge base and problem ticketing system
- E-mail and toll-free telephone assistance Monday through Friday, 6 a.m. to 6 p.m. Pacific, US Time (except holidays)
- Product documentation and documentation updates
- Program error fixes, hotfixes, and service packs
- Product upgrades for your Bocada deployment

To access the new support portal, click on “Customer Support Portal” from the following URL:

<https://www.bocada.com/product-support/>

Bocada Professional Services

Bocada offers Professional Services assistance for installation and continuing support of our products. Bocada solutions are built with an open architecture that allows for custom reporting and integration with third party solutions. Please consult with our sales or support team to determine if your organization would benefit from Bocada Professional Services:

- Deployment Planning and Guided Assistance
- Bocada Migrations (from earlier Bocada products)
- Training
- Custom Report Design, Review, and Delivery
- Installation and Configuration
- Backup Assessments

Bocada Finance

Email: finance@bocada.com.

Appendices

Appendix A: Server Processes

This section describes the main processes that run on the Bocada Data Collection and Application servers.

Data Collector Processes

PrismDataCollection.exe Main DCS service that runs all processes on the Data Collection server.

beenum.exe Enumerates plugins during start of DCS.

bepolicy.exe Scheduled task that calculates policy changes.

BeReportGen.exe Generates saved reports for email or export based on user defined schedules.

betestconn.exe Used to test connection of plugins.

beupdate.exe Data collection process which extracts records of backup, media and/or policy activity from backup servers and inserts them into the database.

bocadasettings.exe Launches a GUI from command line to change the database connection settings in the registry. This process is obsolete and the functionality exists in the [Edit General Settings](#) feature from the Bocada Settings view.

brrule.exe Runs rules for new backup clients.

Brprune.exe Maintenance process that populates the summary tables and prunes older data from the database based on configurable maintenance settings.

brslacc.exe Scheduled task that calculates SLA compliance.

PrAlert.exe Scheduled task that monitors backup job failures and sends alerts to email or ticketing systems based on Administrator configured settings.

PrLicense.exe Scheduled task that calculates license usage.

Application Server Processes

BocadaService.exe Windows Communication Foundation (WCF) service that runs the application.

Appendix B: Error Definitions

By default, equal weight is given to each error, regardless of its error category. The error Definitions defined in Bocada are detailed in Appendix B.

- Aborted Backup Error (1)** Backup job was manually stopped by a user/operator.
- Backup Configuration Error (2)** Installation or configuration of the backup product, either on the backup server or the backup client, resulted in an error (ex: a missing backup client agent).
- Backup File Busy Error (3)** File was in use during the backup job.
- Backup File Corrupt Error (4)** Either a file changed while it was being saved to media (timestamp error), or the backup server detected a virus (infected file).
- File I/O Error (5)** Server encountered an I/O error while reading a file (e.g. a backup client's hard disk crashed during the backup job).
- Backup File Locked Error (6)** File was locked by another during the backup job.
- Backup File Permission Error (7)** Backup server had insufficient permissions to access a file (e.g. did not have read access).
- Backup File Verification Error (8)** The backup copy of a file differed from its source (e.g. the file changed since backup).
- Backup Group Error (9)** An error was recorded within this target's Job Group. Some backup products record certain errors per Job Group, meaning, that if a single target is associated with a given error, every target within the Job Group will record the same error.
- Backup Media Unavailable Error (10)** ... No writable media was available for this backup job (ex: the tape in the drive belonged to the wrong media pool).
- Backup Media I/O Error (11)** Storage device (tape library) encountered an error while writing the backup job to media (ex: insufficient free storage space on the tape).
- Backup Network Error (12)** Network connectivity error occurred during the backup job (ex: a backup client was unavailable).
- Backup Software Error (13)** Backup software failed to operate properly (ex: the backup server encountered an access violation).

Backup Time-out Error (14)	Backup job was automatically terminated because it exceeded the expected amount of time (ex: a stalled backup was timed out by the backup server).
Backup Unknown Error (15)	An error was recorded for this backup, but specific details are not available.
Backup Window Error (16)	Backup job was automatically terminated because it exceeded the backup window allotted for the job.
Backup X1 Error (17)	Supported product-specific error category.
Backup X2 Error (18)	Supported product-specific error category.
User Category 1 (19)	Supported user-defined error category. For more information about how configuring this error category, see the <i>User Error Categories</i> section of this guide.
User Category 2 (20)	Supported user-defined error category. For more information about how configuring this error category, see the <i>User Error Categories</i> section of this guide.
User Category 3 (21)	Supported user-defined error category. For more information about how configuring this error category, see the <i>User Error Categories</i> section of this guide.
User Category 4 (22)	Supported user-defined error category. For more information about how configuring this error category, see the <i>User Error Categories</i> section of this guide.
User Category 5 (23)	Supported user-defined error category. For more information about how configuring this error category, see the <i>User Error Categories</i> section of this guide.
User Category 6 (24)	Supported user-defined error category. For more information about how configuring this error category, see the <i>User Error Categories</i> section of this guide.

Appendix C: Writing Your Own Custom SQL Reports

Bocada supports creating custom SQL reports (as seen above in the [SQL Queries](#) section), with [criteria](#) as seen below, and supports access controls so reports can be run by and shared with all users, operators, or administrators.

Running a Custom SQL Report

Custom SQL reports are available to designated users through the [Saved Reports](#) tab of the [Health Check](#) module.

Custom Report Administration:

Administrators can manage custom SQL reports by using the tools found under [Administration](#) > [Custom SQL Templates](#), above.

Date/Time Controls:

The following comments will toggle date / time controls when added to Custom SQL:

```
-- TimeEnableBocada -- enables time controls
-- TimeZoneEnableBocada -- enables time zone control
-- IncludeBackupServerTimeBocada -- includes backup server time as a
timezone
SET @start_date = CONVERT(VARCHAR, (SELECT value_datetime FROM
#criteria WHERE criterianame = 'FromDatetime'), 101)
SET @end_date = CONVERT(VARCHAR, (SELECT value_datetime FROM #criteria
WHERE criterianame = 'ToDatetime'), 101)
```


Report Criteria

The table below lists the criteria that can be used in a report. Bocada will automatically detect which criteria are provided to the user if the report follows the rules described later. A custom report does not need to have criteria.

Criterion	Value Type ++ = see notes below	Multi-value	Notes
UserSid	value_string ++		This is an automatically supplied value equal to the SID of the user and is not a control.
FromDateTime ToDateTime TimeZone = Date Range	value_datetime value_datetime value_bigint [timezone.timezone_id]		The value of ToDateTime will be the date of one day past the date selected by the user if only a date is specified. That will make the date ranges be start day and end day inclusive.
BackupProducts	value_bigint [backupproducts.product_id]	Yes	
BackupLevels	value_string	Yes	
BackupServers	value_bigint [servers.server_id]	Yes	
BackupClients	value_bigint [clients.client_id]	Yes	
Assets	value_bigint [asset.asset_id]	Yes	
JobGroups	value_bigint [backupgroups.backupgroup_id]	Yes	
MediaServers	value_bigint [mediaserver.mediaserver_id]	Yes	
MediaLibraries	value_bigint [medialibrary.medialibrary_id]	Yes	
Zones	value_bigint [zone.zone_id]	Yes	
SLAProfiles	value_bigint [slaprofile.slaprofile_id]	Yes	
PriceLists	value_bigint [pricelist.pricelist_id]	Yes	

Attempt = Backup Attempts	value_bigint ++		1 = best 2 = last 3 = all
IncludeIgnoredItems	value_bool		

Processing Simple Criteria

Below is an example showing how to extract single values from specified criteria.

To extract single values from the criteria use this code:

```
SET @criterion_value =
  SELECT value_type FROM #criteria
  WHERE criterianame = 'criterion'
```

The **value_type** and **crit**erion are user-specified; The example above will result in No Data when the report is run unless these are changed to real values.

Processing Multi-Valued Criteria

All multi-valued criteria support selecting by either inclusion or exclusion. Therefore, to use these criteria, the report needs to first check if the set is negated using this code:

```
SET @criterion_isnegated =
  SELECT TOP 1 isnegated FROM #criteria
  WHERE criterianame = 'criterion'
```

Based on the result, the criteria values either identify the values included or excluded. To specify exclude/include in a report query, use the following example edited for your purposes:

```
AND (@criterion_isnegated IS NULL
  OR @criterion_isnegated = 0
  AND id IN (SELECT value_bigint FROM #criteria
    WHERE criterianame = 'criterion'))
OR @criterion_isnegated = 1
  AND id NOT IN (SELECT value_bigint FROM #criteria
    WHERE criterianame = 'criterion')
```

Zones and Backup Clients

WARNING: Your SQL code is responsible for implementing zone security. To ensure that users will not have access to clients that they are not authorized to see, you must follow the instructions in this

section. There is nothing in place to prevent a report from displaying data from zones that the user does not have access to; this is entirely the responsibility of the report author.

To enforce zones, the report must include this at the top of the SQL code to set things up:

```
EXEC dbo.UmpConvertZoneCriteriaToClients
DECLARE @show_unzoned_clients INT
DECLARE @has_user_id INT
SET @show_unzoned_clients =
    (SELECT value_bool FROM #criteria
     WHERE criterioname = 'ShowUnzonedClients')
SET @has_user_id =
    CASE WHEN EXISTS (SELECT value_string FROM #criteria
                     WHERE criterioname = 'UserSid')
    THEN 1 ELSE 0 END
```

Next, add this condition to your SQL query:

```
(@has_user_id = 0
 OR clients.client_id IN
    (SELECT DISTINCT clients.client_id
     FROM clients WITH (NOLOCK)
     LEFT JOIN backupclientzone AS bcz WITH (NOLOCK)
         ON bcz.client_id = clients.client_id
     LEFT JOIN zwebuserzone AS wuz WITH (NOLOCK) ON wuz.zone_id =
bcz.zone_id
     LEFT JOIN zwebusers AS wu WITH (NOLOCK) ON wu.user_id = wuz.user_id
     LEFT JOIN #criteria ON #criteria.value_string = wu.sid
         AND #criteria.criterioname = 'UserSid'
 WHERE (#criteria.value_string IS NOT NULL OR bcz.client_id IS NULL)
       AND (@show_unzoned_clients = 1 OR bcz.zone_id IS NOT NULL))
```

See the sample report below to see how zones are used in a report.

Note that this code does not enable the Zones criteria to the user. To enable zones without actually querying directly for zones, add this comment to your SQL query:

```
-- criterioname = 'Zones'
```

Filtering, Sorting and Grouping

The user viewing the report will be able to use filters, sorting, and grouping just as they can for all tabular reports.

Error Handling

If the Custom SQL report returns “No Data” when run, you can verify your custom SQL query using the SQL query analyzer built into Microsoft SQL Server or contact your SQL administrator for further troubleshooting steps.

Custom Report for Debugging

Here is a custom report that is particularly useful for testing different criteria to demonstrate the #criteria table looks like when your report is run:

```
SELECT * FROM #criteria
WHERE criterioname = 'BackupClients'
      OR criterioname = 'BackupServers'
```

Add as many lines as necessary, listing each of the criteria names you want to use in your report. If you don't set any criteria values, you will see "No Data", as the criteria table does not include any values for unset criteria.

Example Custom Report

The following example Custom SQL report will show information about backup servers and the time of the last backup, as well as how to implement zone security.

```
-- Call proc to handle zone security for backup clients criteria.
EXEC UmpConvertZoneCriteriaToClients

-- These values are used for zone security in the query.
DECLARE @show_unzoned_clients INT
DECLARE @has_user_id INT
SET @show_unzoned_clients =
  (SELECT value_bool FROM #criteria
   WHERE criterioname = 'ShowUnzonedClients')
SET @has_user_id =
  CASE WHEN EXISTS(SELECT value_string FROM #criteria
                    WHERE criterioname = 'UserSid')
  THEN 1 ELSE 0 END

-- These values are the report criteria available to the user.
DECLARE @backupproducts_isnegated INT
DECLARE @servers_isnegated INT
DECLARE @clients_isnegated INT
DECLARE @from_date_time DATETIME
DECLARE @to_date_time DATETIME

SET @backupproducts_isnegated =
  (SELECT TOP 1 isnegated FROM #criteria
   WHERE criterioname = 'BackupProducts')
SET @servers_isnegated =
  (SELECT TOP 1 isnegated FROM #criteria
   WHERE criterioname = 'BackupServers')
SET @clients_isnegated =
  (SELECT TOP 1 isnegated FROM #criteria
   WHERE criterioname = 'BackupClients')
SET @from_date_time =
  (SELECT value_datetime FROM #criteria
   WHERE criterioname = 'FromDate')
SET @to_date_time =
  (SELECT value_datetime FROM #criteria
   WHERE criterioname = 'ToDate')
```

```

SELECT
    clients.clientfqname AS 'Client',
    clients.lastjobdatetime AS 'Last Backup Date Time',
    backupproducts.productname AS 'Backup Product',
    servers.serverfqname AS 'Server'
FROM clients
JOIN servers ON servers.server_id = clients.server_id
               AND servers.serverstatus <> 'delete'
JOIN backupproducts ON backupproducts.product_id = servers.product_id
WHERE clients.client_id > 0

-- Filter by user-selected date range; note that lastjobdatetime is in
UTC.
AND clients.lastjobdatetime IS NOT NULL
AND clients.lastjobdatetime >= @from_date_time
AND clients.lastjobdatetime < @to_date_time

-- Filter by user-selected backup product ids.
AND (@backupproducts_isnegated IS NULL
     OR @backupproducts_isnegated = 0
     AND servers.product_id IN
         (SELECT value_bigint FROM #criteria
          WHERE criterianame = 'BackupProducts')
     OR @backupproducts_isnegated = 1
     AND servers.product_id NOT IN
         (SELECT value_bigint FROM #criteria
          WHERE criterianame = 'BackupProducts'))

-- Filter by user-selected server ids.
AND (@servers_isnegated IS NULL
     OR @servers_isnegated = 0
     AND clients.server_id IN
         (SELECT value_bigint FROM #criteria
          WHERE criterianame = 'BackupServers')
     OR @servers_isnegated = 1
     AND clients.server_id NOT IN
         (SELECT value_bigint FROM #criteria
          WHERE criterianame = 'BackupServers'))

-- Filter by user-selected client ids.
AND (@clients_isnegated IS NULL
     OR @clients_isnegated = 0
     AND clients.client_id IN
         (SELECT value_bigint FROM #criteria
          WHERE criterianame = 'BackupClients')
     OR @clients_isnegated = 1
     AND clients.client_id NOT IN
         (SELECT value_bigint FROM #criteria
          WHERE criterianame = 'BackupClients'))

-- Implement zone security; this block is required for
-- all reports accessible to non-admins.
AND (@has_user_id = 0
     OR clients.client_id IN
         (SELECT DISTINCT clients.client_id
          FROM clients WITH (NOLOCK)

```

```

LEFT JOIN backupclientzone AS bcz WITH (NOLOCK)
    ON bcz.client_id = clients.client_id
LEFT JOIN zwebuserzone AS wuz WITH (NOLOCK)
    ON wuz.zone_id = bcz.zone_id
LEFT JOIN zwebusers AS wu WITH (NOLOCK)
    ON wu.user_id = wuz.user_id
LEFT JOIN #criteria ON #criteria.value_string = wu.sid
                    AND #criteria.criterianame = 'UserSid'
WHERE (#criteria.value_string IS NOT NULL
      OR bcz.client_id IS NULL)
      AND (@show_unzoned_clients = 1
          OR bcz.zone_id IS NOT NULL))

ORDER BY clients.lastjobdatetime DESC

```

Troubleshooting Limitations

You must name unnamed columns. For example:

```
SELECT 'myValue' AS 'myColumn'
```

Appendix D: Maintenance: Tables Pruned

This Appendix details which tables in the Bocada Database are affected by each type of control. Bocada database pruning is controlled within Administration > General Settings, on the Maintenance tab. Further information is available within the [General Settings](#) > [Maintenance](#) section of this guide.

Tables Pruned by Maintenance Control Type

Bocada database pruning is controlled within Administration > General Settings, on the Maintenance tab.

Edit General Settings

Maintenance | Global Report Settings | User Error Categories | Email Settings | Application | License Keys | SLA

Collection | Web Server

Prune Outdated Updates

<input type="checkbox"/> Backup data:	365	days	<input type="checkbox"/> Weekly summaries:	52	weeks
<input type="checkbox"/> Storage data:	365	days	<input type="checkbox"/> Monthly summaries:	12	months
<input type="checkbox"/> Media data:	365	days	<input checked="" type="checkbox"/> Server messages:	90	days
<input type="checkbox"/> Policy data:	365	days	<input checked="" type="checkbox"/> Backup events:	2000	days

Prune Outdated Logs

Activity log retention: 888 days

Prune Outdated Backup Clients

☐ Clients retention: 365 days

Prune Orphan Assets

☐ Orphan Assets retention: 15 days

Prune Outdated Snapshot Files

Snapshot Retention: 7 days

Prune Auto Saved Reports

Auto Saved Reports retention: 24 hours

Prune Saved Reports

☐ Saved reports data: 45 days

Prune Outdated requests

☒ Requests: 35 days

Prune Database Maintenance Window

Maximum duration: 2 Hours

Maximum number of rows being pruned per attempt

Maximum rows per attempt: 1000 rows

Schedule to Update Weekly and Monthly Summary

Each day at 4:00 - [Edit Schedule](#)

Update Summary timeout: 300 minutes

Previous Next Finish Cancel

Backup Data Tables:

Backuplog
alertassetstate_backups
alertbackups
backuplog_groupsession
jobmessagelog
medialog
nbubackupjobs
sladetail
sladetails

Storage Data Tables:

mediavolumeinventory
mediapoolinventory
mediadeviceinventory
groupclientpoolinventory

Media Data Tables:

mediamount
mediaerror

Weekly Summaries Tables:

backuplog_week

Monthly Summaries Tables:

backuplog_month

Server Messages Tables:

servermessagelog

Backup Events Tables:

jobmessagelog

Activity Log Retention Tables:

zactivitylog

Clients Retention Tables:

clients
alertassetstate
asset
backupclientignore
backupclientzone
backupgrouptarget
backuplog
backuplog_groupsession
backuptargets
groupclientpoolinventory
medialog
nbubackupdest
nbubackupjobs
policy_client
policy_client_options
policy_nbu_clients
policy_target
policy_tsm_nodes
sladetail
sladetails
tsm_sessions
zclientruletoprocess
zrfx_annotations
ztargetgroups

Orphan Assets Retention Tables:

asset
alertassetstate
assignment
backuptargets
sladetail
sladetails
zassetstate

Auto Saved Reports Retention Tables:

zrfx_savedreport
zrfx_alertconfig
zrfx_savedreport_cache
zrfx_savedreport_reportset
zcommandrequestobjects

Saved Reports Data Tables:

zrfx_savedreport
zrfx_alertconfig
zrfx_savedreport_cache
zrfx_savedreport_reportset
zcommandrequestobjects

Outdated Requests Tables:

zrequests
alerts_data_collection_details
discoveredsubnet
subnet
zactivitylog
zperf
zrequestreport
zrequestserver
zsharedreport

Note: zactivitylog pruning is done per the *Activity Log Retention* setting. However, when pruning zrequests for *Outdated Requests* pruning, dependent entries in zactivitylog must be pruned first to allow zrequests pruning.

(Note: The following are not visible in Edit General Settings, but are pruned as part of regular maintenance)

Deleted Server Tables:

- servers
- alertassetstate
- backupgroupserver
- backupgrouptarget
- backuplog
- backuplog_groupsession
- backupserverzone
- backuptargets
- clients
- groupclientpoolinventory
- inventory_snapshots
- mediadeviceinventory
- mediaerror
- medialibrary
- medialog
- mediamount
- mediapool
- mediapoolinventory
- mediaserver
- mediavolume
- mediavolumeinventory
- nbubackupdest
- nbubackupjobs
- policy_nbu_policies_lut
- policy_tsm_domains_lut
- servermessagelog
- serverversions
- tsm_sessions
- zarchivedrepositories
- zrequestserver
- zscheduleserver
- ztargetgroups

Media Server with no associated media mount, media log, or media device inventory Tables:

- mediaserver

Deleted Alerts Tables:

- zrfx_alertconfig
- alertassetstate
- alerts
- alerts_data_collection

Policy Orphan data with no associated data in any table with FK dependency Tables:

policy_nbu_policies_lut
policy_tsm_policies_lut

Appendix E: Parameters in the Bocada Database:

There are features in Bocada which are not used often enough to incorporate into the UI of the Bocada Application, but which can be configured by adding / editing parameters directly in the Bocada Database.

Master Bocada Application Server

If you run more than one Bocada Application server the master application server will be the last one installed, unless you override using `zapplicationservers` database table. The master Application server will have a `dusstatus` of `master`. See screenshot below for example.

hostnode_id	hostname	installation_guid	dusstatus
1	demo.Testlab.com	2d29fb8b-b6de-4c36-9738-fa68c07a9da0	master

The below features are set in the table `zparams`

MaxReportDays:

Optional `zparam` 'MaxReportDays', when set to a value 'N', limits the data pulled from the Bocada database for any report to the most recent N days. This affects *all* users regardless of assigned user role.

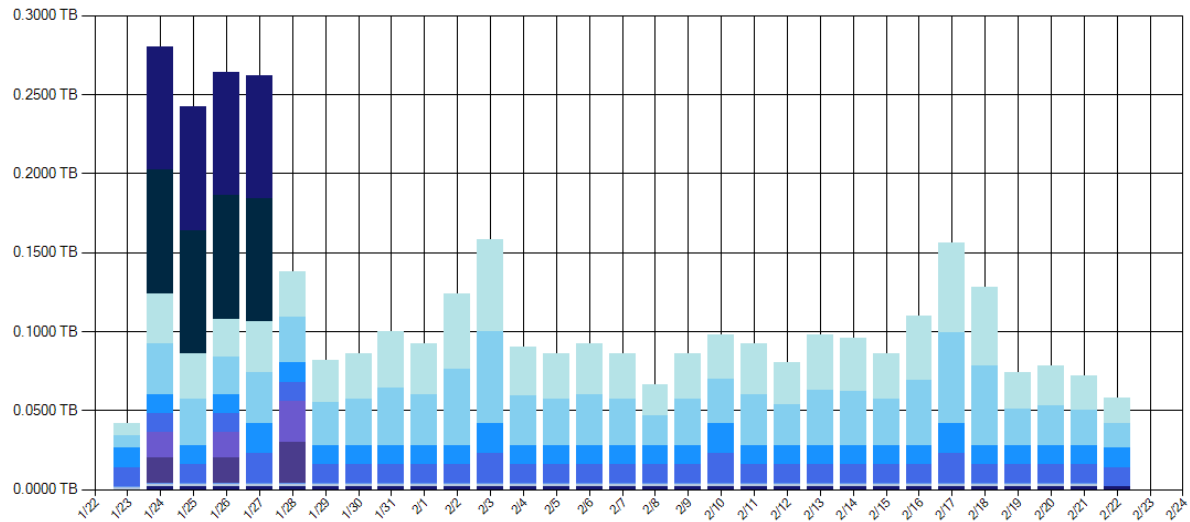
Usage: This `zparam` was included to allow administrators to limit the maximum date range that users could run a report for, to prevent users' report requests from putting too much load on the SQL Server at one time.

Implementation: Run the following SQL:

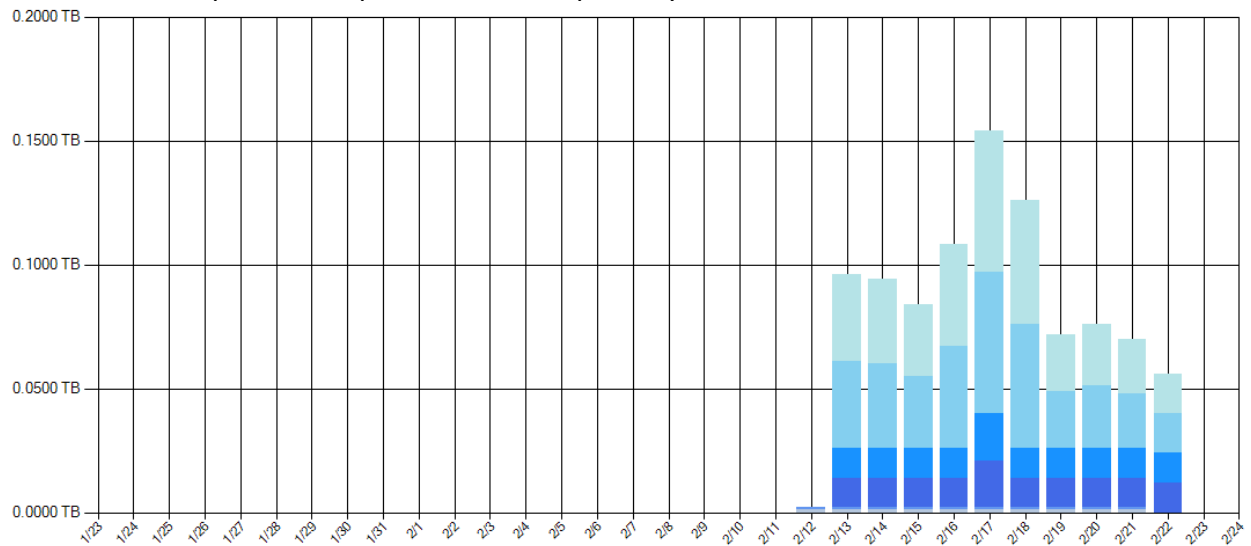
```
INSERT INTO zparams (paramname, paramvalue, hostnode_id)
VALUES ('MaxReportDays', 10, NULL);
```

Results:

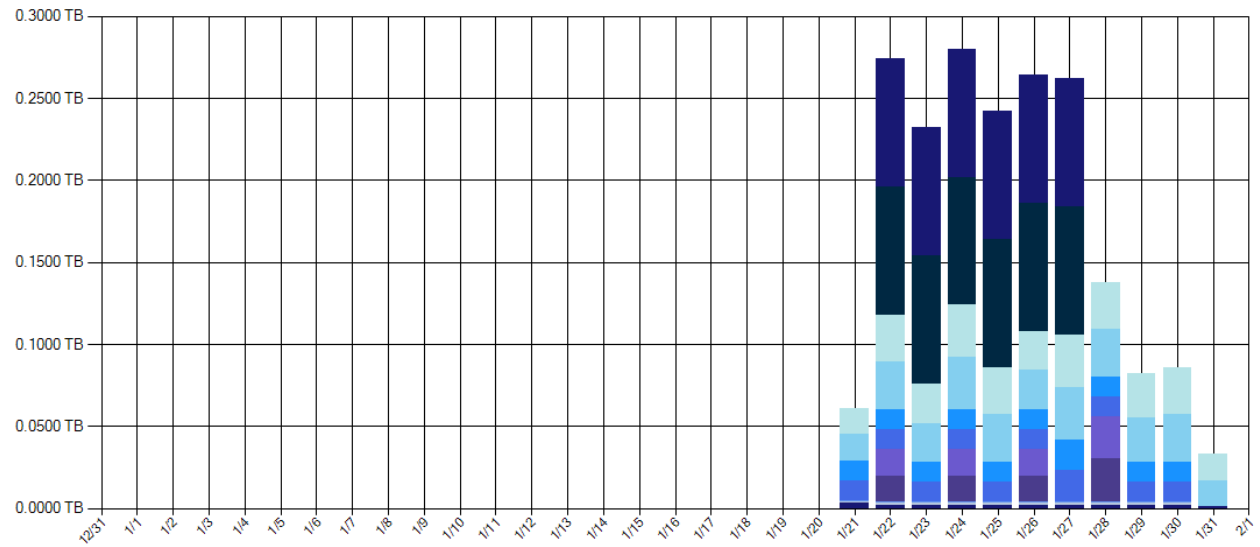
Report not limited by MaxReportDays (here, a Backup Trends report for 31 days):



The same Backup Trends report with MaxReportDays set to 10:



This range remains the same for *all* users (not just standard users) and will always display results for only the last N days (where MaxReportDays = 'N'). Here is the same report run for the days in January:



MaxReportDays also limits the results returned for reports in other formats (such as Job Trends or any tabular reports).

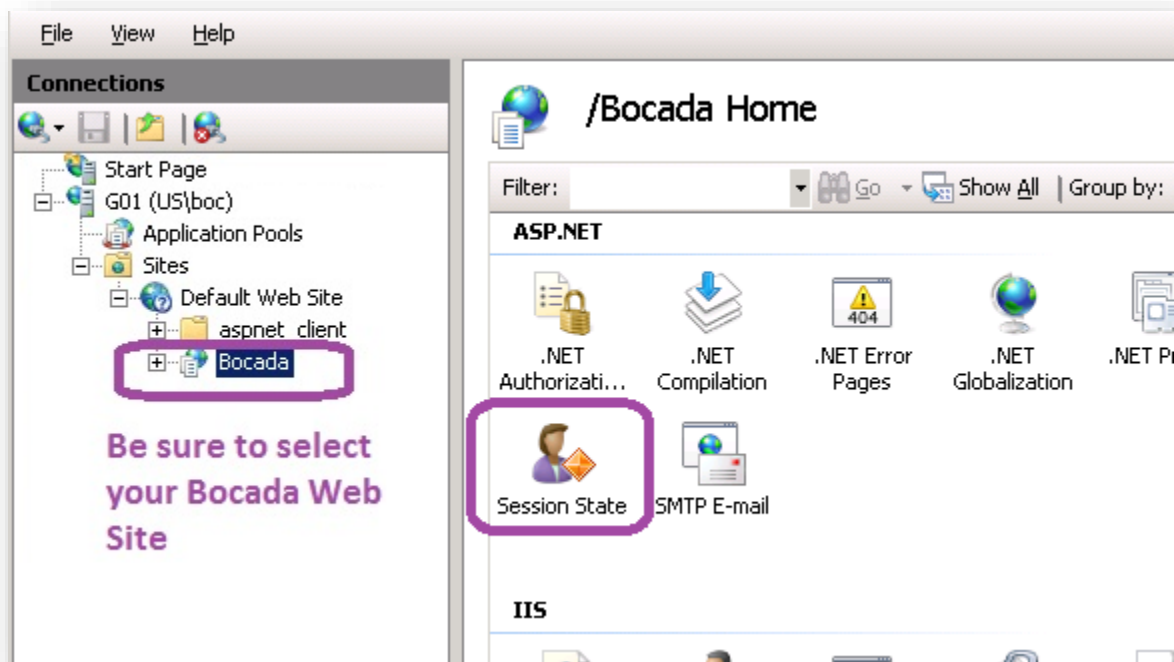
Appendix F: Bocada Website IIS Timeout Settings

By default, the Bocada Application will time out after 120 minutes, but Administrators may choose to change this. The Web UI Time-out setting is found in IIS Manager, and there are 2 setting that you must change: Session State timeout and Application Pools idle time out.

1. Open IIS Manager on the Bocada IIS Application server.



2. Expand the left-side until you get to the Bocada web, and select it.



3. Double-click on "Session State" icon to open.

4. Change Cookie Setting “Time-out (in minutes)” to any desired number, e.g. 1500 minutes is 25 hours.

Session State

Session State Mode Settings

☐ Not enabled

☒ In process

☐ Custom

☐ State Server

Connection string:
tcpip=loopback:42424 [Create...](#)

Time-out (in seconds):
10

☐ SQL Server

Connection string:
data source=localhost;Integrated Security=SSPI [Create...](#)

Time-out (in seconds):
30

☐ Enable custom database

Cookie Settings

Mode:
Use Cookies

Name:
ASP.NET_SessionId

Time-out (in minutes):
1500

☐ Regenerate expired session ID

☒ Use hosting identity for impersonation

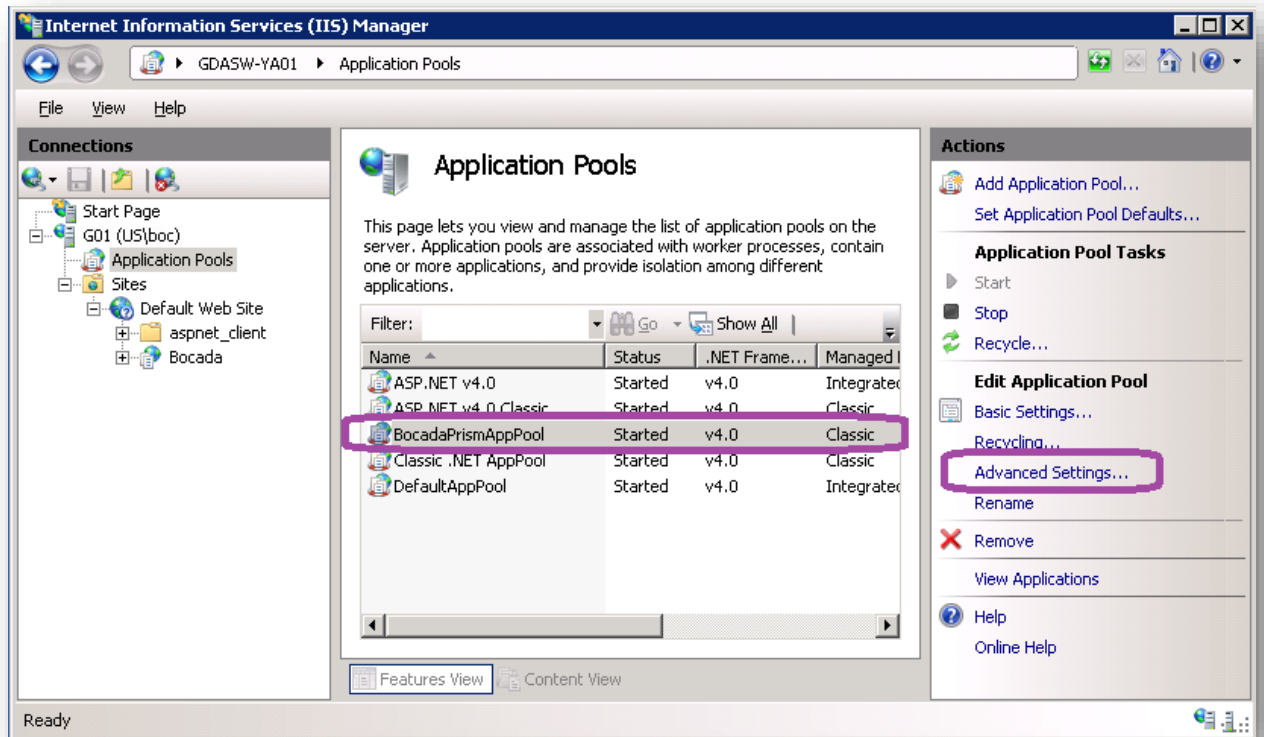
Features View Content View

a:\web.config

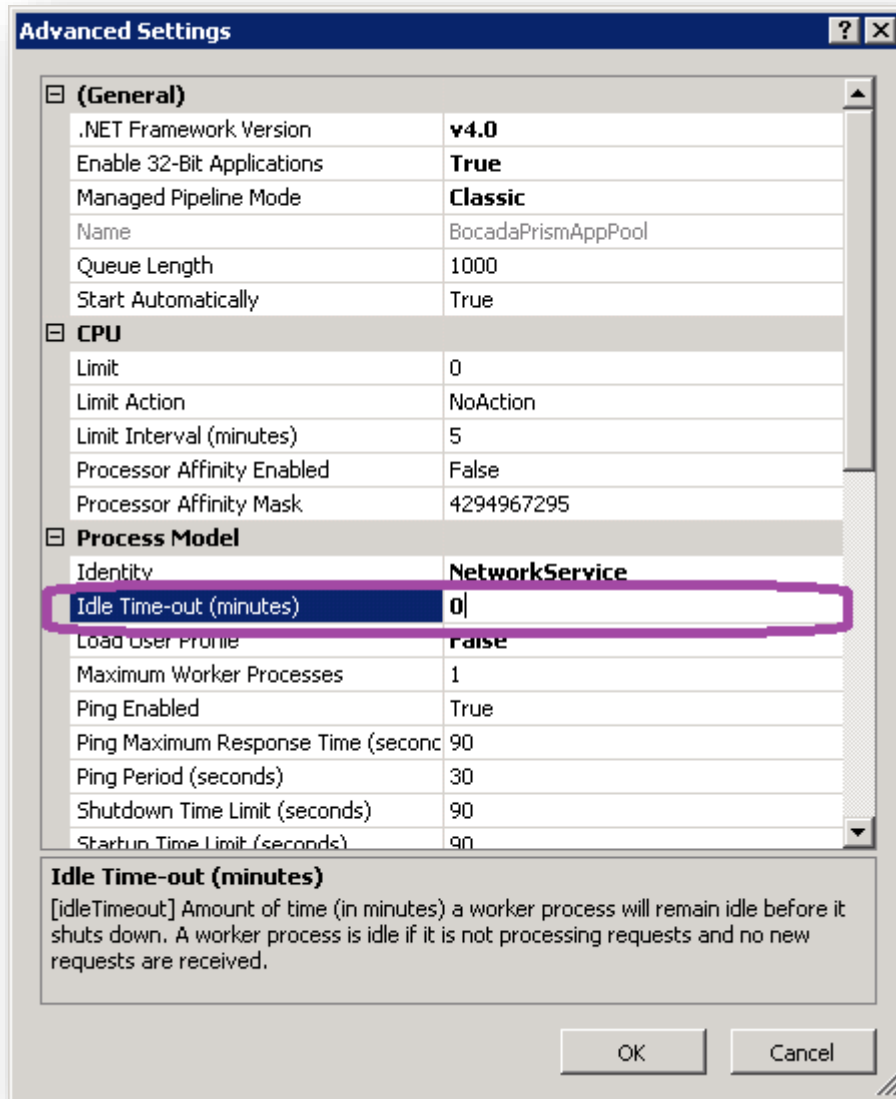
- a.
5. Select “Apply” in the far-right pane to save this setting.



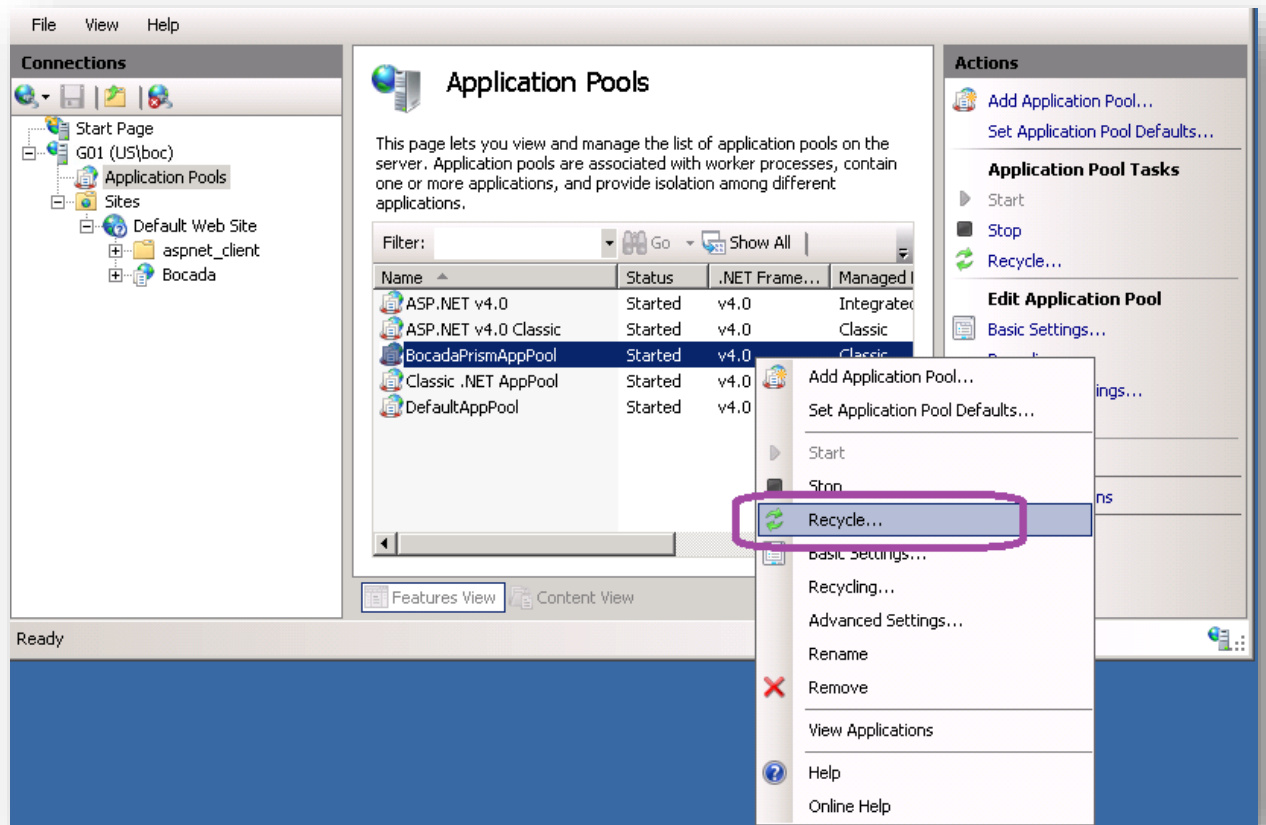
6. Next, select "Application Pools".
7. Right-click on "BocadaPrismAppPool", then select "Advanced Settings".



8. Under "Process Model", change the setting for "Idle Time-out (minutes)". This defaults to 1200 but can be set as high as you like. NOTE: Cannot be set higher than the advanced setting "Regular Time Interval (minutes)" under Recycling, but setting "Idle Time-out (minutes)" to zero removes the timeout altogether.



- Restart the BocadaPrismAppPool by right-clicking and choosing Recycle.



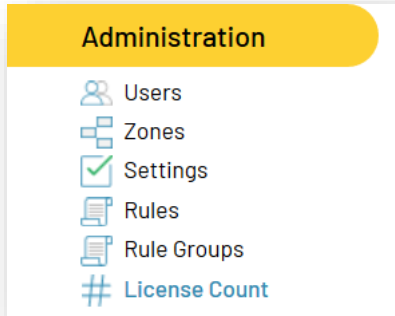
- In **Services**, restart the Bocada Service.

Appendix G: Bocada License Unit Count

If you receive a request for a License Unit Count, this is how to generate the report requested.

Steps to generate the report:

1. Log into Bocada and click on the **Administration** module.



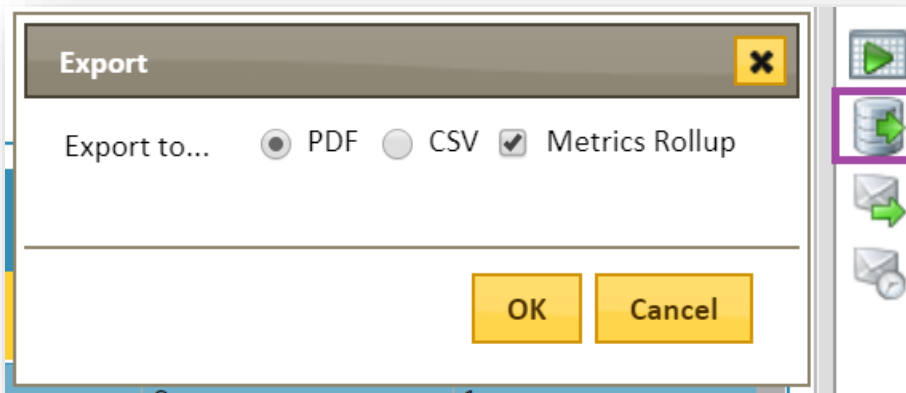
2. Select the item **License Count**.

Administration : License Count

(Drag column here to group by it)					
Product Name	Product Version	Total Unit Count	Client Units	Target Units	Server Units
Avamar	18.2.100-134	6	5	0	1
Avamar	7.4.101-58	2	1	0	1
AWS Backup		89	88	0	1
Azure Cloud		9	6	0	3
Licensed: 100000 Units		Total Units in Use: 1113	Client Units: 1071	Target Units: 7	Server Units: 29

View 1 - 27 of 27

3. Export the report in PDF format.



4. Email the results as an attachment to whomever requested the report.