Default Reports

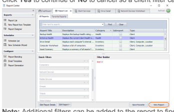
Overview

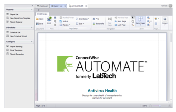
This page lists all of the default reports included with the Report Center solution and samples of each report.

Note: If you are running the report and you do not have full access to all clients (clients, computers, and locations) the report only shows information for what you have permission to access. Refer to Report Center Overview for additional required permissions.
Tip: Each sample report appears as a smaller thumbnail. Simply click on the image to expand to view the full-size sample report.

Preview Reports

Any of the reports can be manually generated, or scheduled to be generated at specific times. For more information on scheduling a report, please refer to Schedule Reports.
To manually preview a report:

1. From the **Control Center**, select **Tools** > **Report Center**.
2. In the **Reports** section of the sidebar, click **Report** List.
3. Double-click on the **Report** to preview it or select it and click the **View Report** button. If a client filter has not been specified for the report, a notification displays indicating that it might take several minutes for the report to display, depending on the amount of data. It is recommended to select a client from the **Quick Filters**. Click **Yes** to continue or **No** to cancel so a client filter can be added.

Note: Additional filters can be added to the report to fine-tune the data it returns using the **Quick Filters** or the **Filter Builder**. For more information on how to create your own filters using the **Filter Builder**, refer to Use the Filter Builder.
4. A **Print Preview** view of the report appears. Continue with the desired action (e.g., print the report).



Clients

This category is used for reports about services rendered to your clients. These can be used to show the value you add to your clients' business.

Client Services Report

The Client Services report shows a summary of a client's assets, service statistics, service time and service requests. The report can be run for all clients or by client.

Business Case

The CEO wants to provide clients with a high-level recap of services performed to show the value their company is providing to the client. The CEO runs the Client Services report on a monthly basis and gives to their clients to show a summary of their assets, service requests and service time.

Frequency

It is recommended the run this report monthly, but can be adjusted as desired.

Sample Report

Report Header	Displays the report name, company logo, and the date the report was generated.
Client Information	Displays the client name, address, country, telephone number, fax number, the number of locations associated with the client, the number of completed and open tickets, as well as the number of issued alerts and active monitor alerts.
Asset Analysis	Displays the total number of computer systems, and network devices. The computer systems are separated by two categories, servers, and workstations, which are further categorized by operating system.
Service Time	Displays the time, in minutes, that was spent on tickets by week.
Service Requests	Displays the total number of service requests per day for the past 30 days, separated by ticket types (e.g., New or Closed).
Report Footer	Displays on the last page of the report and explains the various parts of the report.

Client Performance Review Report

The Client Performance Review report displays a breakdown of CPU, RAM and drive space usage for each client.

Sample Report

Report Header	Displays the report name, company logo, and the date the report was generated.
Client Information	Displays the client name, address, country, telephone number, fax number, and the number of locations associated with the client.
Asset Analysis	Displays the total number of servers, workstations, and network devices. The computer systems are separated by two categories, servers and workstations, which are further categorized by operating system.
Computer Performance	Displays a breakdown for each computer including the location, operating system, IP address, CPU performance, RAM performance and Drive performance. The CPU and memory data are collected from the h_computerstatsdaily table of the database, while the drive data is collected from the drives and

	h_drivestats tables (and is only applicable to internal drives).
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Executive Summary Report

The Executive Summary report displays the current health status, recent asset analysis and includes list views of devices at risk for patch compliance, drive utilization and asset standards not met.

Note: The Executive Summary report is only available on Automate v12 and above.

Example Video

Media, iframe, embed and object tags are not supported inside of a PDF.

Sample Reports

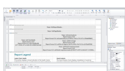
Report Header	Displays the report name, company logo and the date the report was generated at the top of the report.
Report Footer	Displays the date the report was run, the company name and the report page number at the bottom of each page of the report.
Report Legend	Displays details around each section of the report for reference on the last page of the report.

Latest Client Health	
Displays the overall health of the client. This is the combined average of all health checks in the Performance, Stability and Security categories. Additionally, the total counts for servers, workstations and network devices is displayed.	
Performance	Displays the rating for measurements of performance pertaining to CPU, memory, drive, drive fragmentation and NAS storage performance. The rating is displayed with a visual indication and overall percentage score. Additionally, each individual health check within the Performance category displays a visual indication and overall percentage score.
Stability	Displays the rating for measurements of stability pertaining to CPU, memory, drive, operating system and a variety of other stability checks.The rating is displayed with a visual indication and overall percentage score. Additionally, each individual health check within the Stability category displays a visual indication and overall percentage score.
Security	Displays the rating for measurements of security pertaining to antivirus and patch checks.The rating is displayed with a visual indication and overall percentage score. Additionally, each individual health check within the Security category displays a visual indication and overall percentage score.
Asset Analysis	
Assess and displays the percentage of servers and workstations using a Windows operating system and is broken down by supported, extended and end of life categories. Additionally, Mac and Linux system counts are recorded and assessed in the percentages.	
Server Drive Utilization: Top 5 At-Risk	
Displays the top five servers with the highest drive space utilization represented with a horizontal bar and percentage. The list includes location, computer name, volume name, size and percent of drive space utilized for each server.	
Workstation Drive Utilization: Top 5 At-Risk	
Displays the top five workstations with the highest drive space utilization represented with a horizontal bar and percentage. The list includes location, computer name, volume name, size and percent of drive space utilized for each workstation.	
Patch Compliance: Top 5 At-Risk	
Displays the bottom five systems as it relates to patch compliance scores of each server or workstation based on the patch policy set in Automate. Each workstation lists the associated location, computer, patch compliance, and patch status. The Patch Compliance for each workstation displays as a colored percentage bar (green, yellow, or red) based on patch policy settings. Additionally, the status of patches on devices is broken down by their status (I = Installed, NA = Not Attempted, and F = Failed). The Patch Status column displays the different compliance statuses based on the following risks: • OK: System is compliant and has no patch risks. • Missing Patches: The computer is missing one or more patches due to no installation attempt. • Pending Reboot: The computer may require a reboot in order to complete installation of patches. • Outdated Patch Inventory: The patch inventory has not been updated in the last 30 days. • Failed Patches: The computer is missing one or more patches due to one or more failed installation attempts. • Agent Offline: The computer has not been contacted within the last 15 days.	
Asset Standards At-Risk	

Displays the top five assets with the most failed standards as represented by a count of (Failed Standards / Total Standards).

Modifying the Executive Summary Report

The Executive Summary report takes advantage of subreports to deliver a combination of information. Each detail report in the Executive Summary is a subreport with its own data source and parameters that grab data from the master report. Since the sections are subreports, they can be reused in any other client-based report. Additionally, the Executive Summary report (or any report utilizing these subreports) can be further customized by adding calculated fields which give you the ability to hide or display some components and even change the number of items listed by changing the value of the expression. The image below is the Executive Summary in the Report Designer. You can see the location for each subreport and then use the table to make edits to the report (click the thumbnail image to expand the Report Designer example):

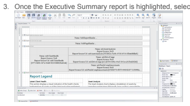


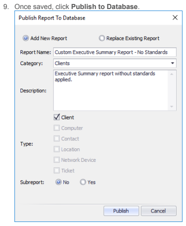
Subreport	Filter	Function	Default Value
subClientHealth	FilterShowHealthCategories	Set value to 0 to hide Health Categories Set value to 1 to show Health Categories	1
subClientHealth	FilterShowHealthChecks	Set value to 0 to hide Health Checks Set value to 1 to show Health Checks	1
subClientHealth	FilterShowStandards	Set value to 0 to hide Standards Set value to 1 to show Standards	1
subClientHealth	FilterStandardsCount	Set value to the number of standards rows to display Set value to 0 to show all standards (does NOT override FilterStandardsShowPassed)	5
subClientHealth	FilterStandardsShowPassed	Set value to 0 to hide standards with no failures Set value to 1 to show standards with no failures	0
subClientHealth	FilterStandardType	Set value to 1 to shows standards rows with counts of computers failed Set value to 2 to show computers rows with counts of standards failed	1
subDriveUsage	FilterDriveShowAtRiskOnly	Set value to 0 to show all drives Set value to 1 to show drives greater than 60% utilized (review or unhealthy only)	0
subDriveUsage	FilterDriveShowServers	Set value to 0 to hide Server drives (section) Set value to 1 to show Server drives (section)	1

Subreport	Filter	Function	Default Value
subDriveUsage	FilterDriveShowWorkstations	Set value to the number of drive rows to display Set value to 1 to show Workstation drives (section)	1
subDriveUsage	FilterDriveTopCount	Set value to the number of drive rows to display Set value to 0 to show all drives (this overrides at-risk settings)	5
subPatchComplianceAssets	FilterPatchMissingOnly	Set value to 0 to show all patch statuses Set value to 1 to show only computers with 1 or more patches that are Not Attempted	1
subPatchComplianceAssets	FilterPatchShowAll	Set value to 0 to show patches with risk statuses only Set value to 1 to show all patches (this overrides missing patch settings)	1
subPatchComplianceAssets	FilterPatchTopCount	Set value to the number of computer rows to display Set value to 0 to show all computer rows (does NOT override missing patch settings)	5

The following example walks you through the process of modifying the Executive Summary report by applying one filter to the report. This example can be utilized to apply any of the listed filters in the above table. The filters are applied by creating calculated fields with the exact name of the filter in the table and then changing the expression to the value necessary for the change. Parameters in the subreports bring these values in at run time and filter the output at print accordingly.

To modify the Executive Summary report:

1. From the **Control Center**, select **Tools** > **Report Center**.
2. Select **Report List** > **Executive Summary**.
Note: If you do not have the Executive Summary in your report list, then you must publish the report from a template. Please refer to Configuring Report Center for more information.
3. Once the Executive Summary report is highlighted, select **Edit Report** > **Modify Report**.

4. Click **Field List** to bring up a list of fields for the report. Then right-click on the **Clients** data source and select **Add Calculated Field**.
5. From the **Property Grid** section, change the entry of the **Name** field of the **Design** section, to **FilterShowStandards**.

6. Enter **0** as the **Expression**. This hides the standards from showing entirely when the report is run. This may be useful if you want to create a version of this report that goes to clients who do not want to see the standards information. You can still run the original version of this report for your techs and sales team to identify revenue-generating opportunities to bring out of standard devices within supportable standards.
7. Click **Print Preview** to confirm the changes have been applied.
8. Once the changes have been made, select **Save** to save the report locally.
9. Once saved, click **Publish to Database**.


10. Enter a unique name in the **Report Name** field.
11. Ensure that **Clients** are selected from the **Category** drop-down and a description is entered in the Description field.
12. Leave the **Type** set to **Client** and the **Subreport** radio button set to **No**.
13. Once all information has been added, click **Publish**. This custom report is now available from the **Report List** and can be run at any time from the **Report Center**.

Custom Reports

Includes two base reports that can be used to create your own computer and client based reports and represent a starting point to help you create a report from scratch. Additionally, you can save reports that you create on your own under this category to quickly find them in the report list.

Client Base Report

This report provides you with a simple starting point for developing custom client reports. This template features a fully functional client report with a short summary of client contact and asset information to get you started.

Displays Client Information to the left (name and contact information for the current client), with an Asset Analysis to the right (a summary of asset counts for the current client).

Computer Base Report

This report provides you with a simple starting point for developing custom computer reports. This template features a fully functional computer report with a short summary of computer information to get you started. Displays basic computer information to identify the asset.

Events

Reports in this category show information regarding specific events within your environment. For example, showing all remote access events initiated by Automate users.

Remote Access Audit Report

The Remote Access Audit report displays a history of remote connections for each computer. The purpose of the report is to give you the option to provide your clients with details of remote connections into their environment and bill accordingly. This report can be run for all computer, location, client or by all clients.

Business Case

The ConnectWise Automate Administrator needs to show what machines their technicians are accessing and the reason for access in order to ensure regulations are being adhered to.
The Automate Administrator can run the Remote Access Audit to view all remote connections, the reason for connection, and the duration of the connection.

Report Frequency

It is recommended to run this report monthly, but can be run, as needed.

Sample Report

Report Header	Displays the report name, company logo and the date the report was generated.
Identification	Displays identifying details about the computer, such as the client and location the computer is associated with, as well as the computer name, nickname, operating system, IP address, current status,

	current user, etc.
Remote Connection History	Displays the history of remote connections made to the computer. Each line details the connection type, the user that initiated the connection, time the connection started, duration of the connection and the reason for the connection.
Report Footer	Displays the date the report was run, the company name, and the report page number.

Remote Workforce Access Audit Report

The Remote Workforce Access Audit report displays a history of contact-initiated Control sessions. The purpose of the report is to give you the option to provide your clients with details of Control remote connections into their environment and bill accordingly. This report can be run for all computer, location, client or by all clients.

Report Frequency

It is recommended to run this report monthly, but can be run, as needed.

Sample Report

Report Header	Displays the report name, company logo and the date range of the report.
Identification	Displays identifying details about the client including the client name, address, country, phone and fax numbers (if applicable).
Remote Access Summary	Displays the total number of remote sessions, the duration of the sessions, the number of contacts that have initiated sessions and the total number of sessions by computer.
Remote Connection History	Displays the history of remote connections made to the computer. Each line details the location of the connection, the computer name, the connected time and the duration of the connection. The bottom of each column also displays totals for each one (computers, connections and connection duration).
Report Footer	Displays the date the report was run, the company name, and the report page number.

Health

High-level summarization regarding the overall health of an agent or client or the health of one or more specific categories. Health reports help technicians find problem areas and can also be used with Client reports to show the value you add to your clients' business.

Patch Compliance Report

The Patch Compliance report draws from data gathered from the Patch Manager, and displays up-to-date information about the current patch health of your managed systems, detailing each device and patch that is non-compliant. This report can be run for all clients or by a specific client. The patch compliance calculations do not include third party patches.

Important: The Patch Compliance report is only available when you enable the latest Patch Manager within v11.
Important: The Patch Compliance report performs calculations on a nightly basis. If the report data is missing or inaccurate, the report displays incorrect information. To resolve, go to the **Control Center** > **Help** > **Server Status** and click the **Do Patch Report Calculations** button. Once the command completes, rerun the report.

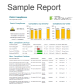
Business Case

The ConnectWise Automate Administrator needs to make sure that their company is meeting their SLAs with their client. The Automate Administrator runs the Patch Compliance report to verify the patch health across their client base, provide compliance scores, and list non-compliant devices.

Report Frequency

It is recommended to run this report weekly; however, you can adjust the frequency to be more or less frequent in order to meet your obligations to your clients.

Sample Report



Report Header	Displays the report name, company logo and the date the report was generated.
Client	Displays the patch compliance score as a colored icon based on the scoring method used by the Patch

Patch Compliance	Manager in Automate. The patch compliance score for the client is calculated based on the number of successfully installed patches out of the total number of approved patches. Additionally, this section displays the number of total assets in patch management and the number of assets that are considered at risk.		
Patch Compliance by Severity	Displays a chart of the recent history of patches that have been installed as compared to patches that have not been installed for the client on the basis of severity (as categorized by Microsoft). The graph displays percentages for Critical, Important, Moderate, Low and Unspecified. Compliance percentages are calculated as the number of Approved and Installed patches over Approved patches.		
Patch Compliance by CVSS	Displays a chart of the recent history of patches that have been installed as compared to patches that have not been installed for the client on the basis of severity (as categorized by Microsoft). The graph displays percentages for Critical, Important, Moderate, Low and Unspecified. Compliance percentages are calculated as the number of Approved and Installed patches over Approved patches.		
Non-Compliant Devices	Displays a list of devices that are at risk due to a non-compliant configuration. The list is sorted by the I / NA / F column, specifically on the values for NA and F, in descending order. Each device displays the following information:		
	Location or Computer	Displays the name of the location and computer.	
	Operating System	Displays the operating system of the device.	
	Patch Compliance	Displays the patch compliance percentage per device as well as a bar graph that represents the given percentage by color.	
	I / NA / F	Displays the total installed, total not attempted and the total failed patches. Values are displayed as integer counts (e.g., 90 / 10 / 30)	
	Last Patched	Displays the month, day, and year of the last patch.	
	Last Scanned	Displays the month, day, and year of the last scan.	
	Patch Status	Displays the current patch status **Note:** If multiple statues exist for a patch, the row expands and stack each applicable status under it.	
		OK	The computer is not at risk due to a non-compliant configuration. This computer is filtered from the list, by default.
		Outdated Patch Inventory	The patch inventory has not been updated in the last 30 days.
		Pending Reboot	The computer may require a reboot in order to complete the patch install.
		Failed Patches	The computer is missing one or more patches that were approved but an install was not attempted.
		Missing Patches	The computer is missing one or more patches that were approved but an install was not attempted.
		Agent Offline	The computer has not been contacted within the last 15 days and may require patches to be installed.

Non-Compliant Patches	Displays a list of patches that are not fully distributed to approved devices. The list is sorted by the F and NA columns, in descending order. Each patch displays the following information:	
	Patch Title & KB Article	Displays the title and KB Article ID for the patch.
	Operating System	Displays the operating system that the patch applies to.
	Category	Displays Microsoft's patch category for the patch.
	Severity	Displays Microsoft's severity level for the patch.
	CVSS	Displays NIST's CVSS score level for the patch.
	Release Date	Displays the date that the patch was released.
	F	Displays the number of devices that have failed to install the patch.
	NA	Displays the number of devices that have not attempted to install the patch.
Report Footer	displays the date the report was run, the company name, and the report page number.	
Report Legend	Displays on the last page of the report and explains the various parts of the report.	

Computer Health Standards Report

The Computer Health Standards report displays details about the latest standards and health checks, for each computer. This allows you to view which client assets are non-compliant with your standards so that you can show your client opportunities for improvement. The report displays the latest health score by category, as well as the list of standards that are applied to each computer, with the percentage passed. This report can be run for all computers, location, client, or by all clients.

Sample Report

Report Header	Displays the report name, company logo and the date the report was generated.	
Identification	Displays information that identifies the current computer: client and location the computer is associated with, friendly name of the computer, its current status, the date it was added to Automate, nickname, the last contact with the server and its operating system. Status is based on computer uptime (e.g., Shutdown, Standby/Hibernate, Service Updating, Disconnected (if the last contact is more than 15 minutes ago) and Running).	
Latest Computer Health	Displays a simplified health score by category. Green indicates healthy, yellow indicates that it needs review, red indicates that it is unhealthy and gray indicates that it has not been evaluated.	
Applied Standards	Displays the list of standards that are applied to this computer and their latest score.	
	Calculation	Displayed as [StandardsPassed] passed / [StandardsApplied] evaluated = [StandardsPassed] / [StandardsApplied]%
	[Standards Passed]	The sum of all standards where the standard is enabled, is passed and is not ignored.
	[Standards Applied]	The sum of standards where the standard is enabled and is not ignored.
Latest Health Check	Displays the list of health checks that are applied to this computer and their latest score. Calculation is displayed as [HealthCheckScore] / [HealthCheckScoreMax].	
Report Footer	Displays the date the report was run, the company name, and the report page number.	

Client Health Standards Report

The Client Health Standards report lists a summary of your current health status, recent asset activity, and a short asset analysis. The Client Health Standards report includes a graph of devices that are currently within standards. This report can be run for all clients or by a specific client. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Important: The Client Health Standards report is only available in the **Report Center** when the Standards and Health Plugin is installed and enabled.

Business Case

The Automate Administrator wants to check the overall health of their clients' systems.
They run the Client Health Standards Report to check on ticket and patch activity for the past seven days, as well as to check on the overall health, which is based on health and standards checks that were put in place.

Report Frequency

It is recommended to run this report on a weekly basis.

Sample Report

Report Header	Displays the report name, company logo and the date the report was generated.	
Latest Client Health	This section is broken down into three areas:	
	Performance	Displays the rating for measurements of performance pertaining to CPU, memory, drive, drive fragmentation and NAS storage performance.
	Stability	Displays the rating for measurements of stability pertaining to CPU, memory, drive, operating system and a variety of other stability checks.
	Security	Displays the rating for measurements of security pertaining to antivirus and patch checks.
Asset Analysis	The Asset Analysis section displays the number of servers, workstations, and network devices. Additionally, the section assesses the percentage of servers and workstations using a Windows operating system and other operating systems.	
Device Standards	Displays a chart of the percentage of devices within the standard and those failing to meet the standard.	

Severs by Operating System	Displays a chart of the percentage of servers by the operating system.
Recent Activity	Displays the number of new tickets created, tickets closed, the number of files transferred, programs installed and patches installed, within the range of the last seven days.
Workstations by Operating System	Displays a chart of the percentage of workstations by the operating system.
Report Footer	Displays the date the report was run, the company name, and the report page number.

Backup Health Report

The Backup Health report displays the backup health rating for each client, with results over the last 30 days. Detailed results are grouped by location, failed backups, and systems without backups installed. This report can be run for all clients or by a specific client. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Business Case

The Automate Administrator needs visibility into systems where backups fail frequently or systems that do not have backup software installed. They run the Backup Health Report to verify the backup of their clients' systems.

Report Frequency

It is recommended that this report should be run monthly. However, the report frequency should be based on your obligation to your client, so adjust as needed.

Sample Report

Report Header	Displays the report name, company logo and date range for the report.
Client Backup Health	Displays the backup health for the client, the rate of success of the backup jobs, the total number of managed servers and workstations and the total number of at-risk assets. The backup health is calculated by comparing the number of successful backup jobs against the total number of backup jobs.managed servers and workstations and the total number of at-risk assets. The backup health is calculated by comparing the number of successful backup jobs against the total number of backup jobs.
Backup Health History	Displays a graphical history of completed and failed backup instances over the last 30 days. Completed backup instances are shown as green and failed jobs as red. If there is no backup data available, the chart is replaced with No Backup History Found.
Backup Health By Location	Displays a breakdown of installed servers and workstations with backups scheduled by location and the percentage of successful backups over several time periods (less than 1 day, 1 day to 7 days, 7 days to 15 days and 15 days to 30 days). These scores are non-cumulative.
At-Risk Assets	This section is broken down into two sections:
	No Scheduled Backups: Displays the computer/location, IP address, operating system and the date the agent was added for any agents that do not have a backup scheduled.
	Failed Backups: Displays the computer, backup schedule, the success of the last backup job that was run and the total number of successful and failed backup jobs compared to the total for several time periods (less than 1 day, 1 day to 7 days, 7 days to 15 days and 15 days to 30 days).
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Antivirus Health Report

The Antivirus Health report draws from data gathered from the Standards and Health plugin and displays the current health of managed antivirus scanners for each client. This report is designed to help you monitor the antivirus scanner health of your managed systems.
This report can be run for all clients or by a specific client.

Note: The Antivirus Health report is only available in the Report Center when the Standards and Health plugin is installed and enabled.

Business Case

The Technician reviews the Antivirus Health Report to monitor the antivirus scanner health of their clients' managed systems. The Technician can quickly determine what assets are at risk due to out-of-date definitions, antivirus not being installed, antivirus is disabled, and any threats that have occurred.

Report Frequency

It is recommended to run the report monthly but should be adjusted, as needed.

Sample Antivirus Health Report

The Antivirus Health report gives a detailed look at the client's overall antivirus health leveraging the client history, with the average definition file age, the total managed assets, and the total assets at risk. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Report	Displays the report name, company logo, and date the report was generated.

Header	
Client Antivirus Health	Displays the antivirus health score as a colored icon based on the scoring method used by the Standards and Health plugin in Automate. Additionally, this section displays the average antivirus definition age in days, the number of managed assets, and the number of assets that are considered at risk.
Antivirus Health History	Displays a chart of recent antivirus health scores for the client. The antivirus health score value is based on the score reported in the Client Antivirus Health section.
Scanner Disabled	Displays the location, computer name, operating system, and the antivirus solution of the computers that are at-risk, when antivirus is detected as disabled, as well as a total count of the number of assets at risk.
Scanner Missing	Displays the location, computer name, operating system, and the added date of the computers that are at-risk, when antivirus is not detected, as well as a total count of the number of assets at risk.
Scanner Out of Date	Displays the location, computer name, antivirus solution, and the days since the antivirus definitions were last updated, as well as a total count of the number of assets at risk.
Recent Threat Activity	Displays information about recent threat activity to include the date the event occurred, computer affected, name of the threat, severity rating, action taken, time elapsed, and a total count of the number of threats detected.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Inventory

Includes reports that detail the hardware and assets in your clients' networks. You can utilize these reports to track changes to any managed devices.

Hardware Change Audit Report

The Hardware Change Audit report displays each computer's acquired and retired assets for the client, and hardware change events within a specific date range for each computer.

Sample Report

Report Header	Displays the report name, company logo and date the report was generated.
Client	Displays the name of the pertinent client at the top of the page.
Identification	Displays the client, location, computer, computer nickname, domain name, IP address and operating system associated with the computer.
Asset Analysis - Last 30 Days	Displays a breakdown of servers, workstations and network devices that have been added or removed within the last 30 days.
Acquired Assets	Displays a list of asset that have been added within the range and includes the asset name, assigned location, the date the asset was acquired, the type of asset and any relevant notes.
Retired Assets	Displays a list of assets that have been retired within the range and includes the asset name, location, date of retirement, the type of asset and the reason for the retirement.
Asset Changes	Displays a list of assets that have been changed/modified within the range and includes the date of the change, the asset that was affected, the change that was made and a description of the change.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Drive Detail Report

The Drive Detail report displays each computer's internal drive details, including drive usage over time, drive fragmentation, and SMART status. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Sample Report

Report Header	Displays the report name, company logo, and date the report was generated.
Computer	Displays the name of the pertinent computer at the top of the page.
Identification	Displays the client, location, computer, computer nickname, domain name, IP address, and operating system associated with the computer.
Drive Summary	Displays the number of internal drives, optical drives, other drives, network shares, and drives that need to be reviewed. Additionally, the section displays the amount of space used on the drives both in terms of bytes and as a percentage.
Drive Detail	Displays the name of the drive, the volume name, assigned drive letter, model, drive type, file system designation, drive size, the amount of the drive that is used, the amount of the drive that is available, the fragmentation percentage, and any drive risks (which display in red text if items need attention). The section also contains a line graph that provides a visual indication of drive use percentage over time.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Asset Summary Report

The Asset Summary report shows a breakdown summary of all assets for each client per location, followed by a detailed list of computers and network devices for each location. The report can be run for all clients or for a specific client. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

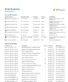
Business Case

The Automate Administrator wants to provide a monthly report to their clients with an accurate count of computers and network devices being monitored. They run the Asset Summary report on a monthly basis so clients can reconcile their records.

Report Frequency

It is recommended to run this report monthly. Adjust schedule, as needed.

Sample Report

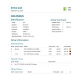


Report Header	Displays the report name, company logo, and date the report was generated.
Client Information	Displays the client name, address, country, phone number, fax number, and the number of locations for the client.
Asset Analysis	Displays the total number of servers, workstations, and network devices as well as the operating system for both servers and workstations (e.g., Windows or Other).
Assets by Location	Displays the total number of computers (servers and workstations) and network devices by location in separate pie charts.
Deployment History	Displays the number of devices deployed over a period of time. Each device type is color-coded (blue = server, red = workstations, green = network devices).
Server Roles	Displays the number of detected server roles by type, using a bar chart.
Computer Assets	Displays the Location\Machine, Operating System, IP Address, Domain, and the Make\Model of the computer.
Network Device	Displays the Location\Device, Description, Online status, IP Address, and MAC Address of the device.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Drive List Report

The Drive List report shows each computer's detected drives, separated by drive type.

Sample Report



Report Header	Displays the report name, company logo and the date the report was generated.
Identification	Displays the client, location of the computer, computer name, computer friendly name, the domain the computer is associated with, IP address and the operating system.
Drive Summary	Displays the number of internal, optical and other drives (e.g., USB and other portable drives, as well as any network shares. Drives to Review indicates the number of drives with SMART errors.
Drive Information	Lists all of the drives by drive type, the associated drive letter, volume name, model, file system, size, drive space, the percentage of drive space used and the current SMART health of the drive. SMART calculation is only provided for internal physical drives.

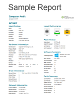
Computer Audit Report

The Computer Audit report shows a detailed overview of a computer. The report can be run for all computer, location, client or by all clients.

Report Frequency

This report should be run, as needed.

Sample Report



Report Header	Displays the report name, company logo and the date the report was generated.
Computer Name	Displays the name of the computer that is being audited.
Identification	Displays the client and location the computer is associated with, as well as the computer name,

	nickname, domain, the last login ID and the asset tag.
Hardware Information	Displays the computer hardware information, to include the manufacturer, product model, chassis type, processor, memory, video, monitors, devices, network cards, sensors and printers.
Drive Information	Displays the drive information, to include the total number of internal drives (and percentage of total used), optical drives, other drives (and percentage of total used), network shares and drives to review.
Network Information	Displays the network information for the computer, to include the local IP address, router address, gateway address, and MAC address.
Latest Performance	Displays the processor, memory and hard drive performance at the time of the report generation.
Service History	Displays the service history for the computer, to include the date/time the computer was added, the date/time the operating system was installed, the last startup date/time and the date/time the computer was last contacted.
Software Summary	Displays the software summary for the computer, to include the operating system, build version, .NET Framework version and the total number of apps installed, unclassified apps, blacklisted apps, startup items, services and processes.
Patch Summary	Displays the patch summary for the computer, to include the patch schedule, the date/time of the last scan, the date/time of the last patch, and the patch status (e.g., missing, approved, pushed or failed).
Report Footer	Displays the date the report was run, the company name, and the report page number.
Serial Number	Displays the ComputerSerial number.

Contact Assets Report

The Contact Assets report displays a list of assets, grouped by their contact assignment. The report includes detailed listings of assigned assets, assets with contacts and assets without contacts. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Sample Report

Report Header	Displays the report name, company logo, and date the report was generated.
Client Information	Displays the name of the client, the address of the client, the country associated, and the phone/fax numbers of the client. Additionally, the section lists the number of locations and contacts associated with the client.
Asset Analysis	Displays the number of servers, workstations, and network devices associated with the client.
Assigned Assets	Displays a list of assets, sorted by their contact. Each row displays the contact's first and last name, the asset's location and computer name, the local IP address, operating system, and last time the asset was contacted by the main server.
Assets without Contacts	Displays a list of assets that are not assigned a contact. Each asset displays the asset's location and computer name, date asset was first assigned an agent, the local IP address, operating system, and last time the asset was contacted by the main server.
Contacts without Assets	Displays a list of contacts that are not assigned to an asset. Each contact displays their first and last name, City and state, email address, primary phone, and mobile phone.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Monitors

Client Failed Monitor Summary Report

The Client Failed Monitor Summary report lists a summary of monitor configuration, current monitor failures, and any outstanding alerts for each client. This report can be run for all clients or by a specific client. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Sample Report

Report Header	Displays the report name, company logo, and date the report was generated.
Client	Displays the name of the specific client that the report was run for is displayed at the top of the report
Identification	Displays the address, country, phone number, and fax number of the client, if available.
Monitor Summary	Displays the applied internal monitors, system monitors, remote monitors and data collection monitors. Additionally, this section displays the current monitor statuses in terms of number of failed monitors and outstanding alerts.
Current Monitor Failures	Displays a detailed list of all current monitors that have failed for the client and includes a specific computer, location, name of the monitor, and date/time of the failure.
Outstanding Alerts	Displays a detailed list of all current outstanding alerts for the client and includes a date/time of the alert, the source, and the alert message.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Monitor Summary Report

The Monitor Summary report displays a summary of monitors installed, failed monitor history for the last 30 days, and any outstanding alerts for each computer. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Sample Report

Report Header	Displays the report name, company logo, and date the report was generated.
Computer	Displays the name of the pertinent computer at the top of the page.
Identification	Displays the client, location, computer, computer nickname, domain name, IP address, and operating system associated with the computer.
Monitor Summary	Displays the date/time of the last check-in, the number of internal monitors, the number of system monitors, the number of remote monitors, and the number of data collection monitors for the computer. Additionally, the number of failed monitors and outstanding alerts associated with the computer are displayed in this section, if applicable.
Current Monitor Failures	Displays a list of failed monitors and includes the date/time of the failure, the type of monitor, the name of the monitor, any available failure details, and the interval of the failed monitor.
Outstanding Alerts	Displays a detailed list of all current outstanding alerts for the computer and includes a date/time of the alert, the source, and the alert message.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Networking

Network Device List Report

The Network Device List report displays the list of network devices and a brief summary of each asset for the selected client.

Sample

Report Header	Displays the report name, company logo and the date the report was generated.	
Client Details	Displays the following client information:	
	Address	Displays the address of the client.
	Country	Displays the country of the client.
	Phone	Displays the phone number of the client.
	Fax	Displays the fax number of the client.
	Locations	Displays the number of locations within the client.
	Total Devices	Displays the total number of devices for the client.
Network Devices by Type	Displays a pie chart representing each type of device and the percentage amount that they make up of the total inventory of devices.	
Network Device	Displays the following device information:	
	Location\ Device	Displays the location name, IP address, and the device ID number.
	Description	Displays a description or name of the device.
	Online	Displays the status of online or offline represented by either a green checkmark or red X.
	IP Address	Displays the IP Address of the device.
	MAC Address	Displays the MAC address of the device.
Report Footer	Displays the date the report was run, the company name, and the report page number.	
Report Legend	Displays on the last page of the report and explains the various parts of the report.	

Performance

Includes reports that display key performance indicators of managed devices (e.g., the CPU utilization of an agent). Performance indicators can be used to uncover issues on an agent or opportunities to upgrade aging and inadequate hardware.

Performance Review Report

The Performance Review report displays a single page summary of each computer and its corresponding performance history. This report can be run for all clients or by a specific client. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Report Frequency

This report should only be run as needed.

Sample Report

Report Header	Displays the report name, company logo, and the date the report was generated.
Identification	Displays the names of the client and location, the name and nickname of the computer, the domain name, and operating system of the computer.
Hardware Information	Displays the manufacturer, product model, chassis type, processor, memory, the number of internal drives, asset tag, and percentage of space available on the computer.
Asset History	Displays the date the asset was added, the date the operating system was installed, the date and time of the last startup, the date and time of the last contact, and the current status of the computer (e.g., disconnected, connected, etc.).
Drive Usage	Displays a graphical representation of the current drive usage. The bar graph depicts each of the currently detected drives and their usage percentage as compared to the predefined warning and critical levels.
Resource Usage - Last 24 Hours	Displays a graphical representation of the CPU and memory usage over the last 24 hours.
Resource Usage - Last 30 Days	Displays the CPU, memory, and drive usage average percentages over the last 30 days as compared to predefined warning and critical thresholds.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

Software

Software reports provide information regarding software inventory on agents as well as results of application

patching.

Patch Stats Summary Report

The Patch Stats Summary Report presents a summary of client and location patching statistics so that you can quickly review and address non-compliant devices.

Important: The Patch Stats Summary report performs calculations on a nightly basis. If the report data is missing or inaccurate, the report displays incorrect information. To resolve, go to the **Control Center** > **Help** > **Server Status** and click the **Do Patch Report Calculations** button. Once the command completes, rerun the report.

Sample Report

Report Header	Displays the report name, company logo, and the date the report was generated.	
Patch Stats Summary	Displays a list of Client or Location names, sorted by default, in ascending order by the lowest compliance score followed by the Client/Location name. You can expand the client or location name by double-click on it. The following table provides further details regarding the information displayed on the Patch Stats Summary table.	
	Compliance %	Represents the percentage of the number of patches installed on all systems vs. the number of patches approved for installation based on patch policies, for the specified client or location.
	Servers / Workstations	Displays a count of managed servers or workstations for the specified client or location.
	Patched > 30d	Represents the number of devices that have not been patched for over 30 days.
	Scanned > 15d	Represents the number of devices that have not been scanned for over 15 days.
	Contacted > 15d	Represents the number of devices that have not been contacted for over 15 days.
	Reboot Pending	Represents the number of devices that have a pending reboot.
	No Patch Inventory	Represents the number of devices that have an empty patch inventory.
Report Footer	Displays the date the report was run, the company name, and the report page number.	
Report Legend	Displays on the last page of the report and explains the various parts of the report.	

Patch Audit Report

The Patch Audit report displays a detailed breakdown of all approved patches and the corresponding installed or not installed state. The information is grouped by each client\location\computer structure. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Important: The Patch Audit report is only available when you enable the latest Patch Manager within v11.
Important: The Patch Audit report performs calculations on a nightly basis. If the report data is missing or inaccurate, the report displays incorrect information. To resolve, go to the **Control Center** > **Help** > **Server Status** and click the **Do Patch Report Calculations** button. Once the command completes, rerun the report.

Sample Report

Report Header	Displays the report name, company logo and the date the report was generated.	
Computer Details	Displays the following computer details:	
	Client	Displays the name of the client.
	(Client) Patch Compliance %	Displays the compliance score of the client. This is calculated as Approved & Installed / Approved.
	Location	Displays the name of the location.
	(Location) Patch Compliance %	Displays the compliance score of the location. This is calculated as Approved & Installed / Approved.
	Computer	Displays the name of the computer.
	(Computer) Patch Compliance %	Displays the compliance score of the computer. This is calculated as Approved & Installed / Approved.
	Total Missing Patches	Displays the count of patches that are missing (approved and not installed).

	Domain	Displays the name of the domain that the computer belongs to.
	Operating System	Displays the operating system of the computer.
	Last Login	Displays the user name of the last login for the computer.
	Asset Tag	Displays the asset tag assigned to the computer.
Patch Details	Displays the following patch list details for each computer:	
	KB ID	Displays the Microsoft KB number for the patch.
	Bulletin	Displays the Microsoft bulletin number for the patch.
	Description	Displays the Microsoft bulletin number for the patch.
	Discovered	Displays the title description of the patch.
	Installed	Displays the date that the patch was discovered.
	Install Date	Displays the date that the patch was installed, if applicable.
Report Footer	Displays the date the report was run, the company name, and the report page number.	
Report Legend	Displays on the last page of the report and explains the various parts of the report.	

Patch History Audit Report

The Patch History Audit Report presents a list of the patch history for each device at any client or location.

Sample Report

Report Header	Displays the report name, company logo and the date the report was generated.
Identification	Displays details regarding the client, location and computer for which this report was run.

	Client	Displays the name of the client.	
	Location	Displays the name of the location.	
	Computer	Displays the name of the computer.	
	Nickname	Displays the nickname associated with the computer.	
	Domain	Displays the domain name.	
	IP Address	Displays the IP Address associated with the computer.	
	Asset Tag	Displays the asset tag name.	
	Operating System	Displays the operating system name.	
Patch Summary	Displays details regarding the status of installed and/or uninstalled patches.		
	Patches Installed or Patches Uninstalled	The following statuses are applicable to both installed or uninstalled patches:	
		Success	Displays when either the patch was successfully installed or uninstalled.
		Failed	Displays when either the patch has failed to install or uninstall successfully.
		Success w/ Error	Displays when either the patch has successfully installed or uninstalled but encountered an error in doing so.
		Aborted	Displays when either the patch was aborted during installation or uninstallation.
		In Progress	Displays whether the patch is still being installed.
Patching History	Displays details regarding the last patch jobs to run.		
	Date	Displays the date the patch job was run.	
	Patch Title	Displays the name of the patch.	
	Source	Displays where the patch came from (e.g., Automate or Other).	
	Action	Displays the action performed on the patch (e.g., Install or Uninstall).	
	Result	Displays the outcome of the report (e.g., In Progress, Success, or Failed).	
Report Footer	Displays the date the report was run, the company name, and the report page number.		
Report Legend	Displays on the last page of the report and explains the various parts of the report.		

Third Party Patch Audit Report

The Third Party Patch Audit report displays a detailed breakdown of all third-party approved patches and the corresponding installed or not installed state. The information is grouped by each client\location\computer structure. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Important: The Third Party Patch Audit report is only available when you enable the latest Patch Manager within v11.
Important: The Third Party Patch Audit report performs calculations on a nightly basis. If the report data is missing or inaccurate, the report displays incorrect information. To resolve, go to the **Control Center** > **Help** > **Server Status** and click the **Do Patch Report Calculations** button. Once the command completes, rerun the report.

Sample Report

Report Date	Displays the date the report was generated.
Identification	Displays a list of information used to identify this specific computer: Client Name, Location Name, Computer Name, Friendly/Nickname, Domain assigned, local IP Address, and Asset Tag.
Managed Product List	Displays the list of third-party applications managed for this computer. Each record displays the name of the application, the date, and version installed on the computer, the approved version for this computer, and the latest version available for installation. The icons to the left indicate whether or not the application meets the approved version requirements for this computer.
Third-Party Patch Summary	Displays a summary of patch configuration for this computer. Details include: Operating System installed; Date the computer was last contacted; Date the last time a third-party update was installed; A count of managed third-party products applied to this computer; and a count of managed third-party products that are compliant on this system (with a percentage).

Backup History Report

The Backup History report displays a historical view of backup jobs performed on each computer, with detailed information for each job instance. A backup job is considered historical if it has a status other than Scheduled, Paused, or Running. The Report Legend appears on the last page of the report and explains a high-level overview of the key areas of the report.

Report Frequency

It is recommended that this report should be run weekly. However, the report frequency should be based on your obligation to your client, so adjust as needed.

Report Criteria

Parameter	Description
Clients	Limits the report results to a specific client.
Locations	Limits the report results to a specific client location.
Computers	Limits the report results to a specific client computer..

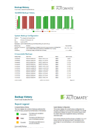
Report Fields

Report Field	Description
Report Header	
Report Name	Displays the report name.
Company	Displays the company name.
Location	Displays the location name associated with the company.
Backup History	
Successful Job Rate	Displays the managed computer's backup history (completed, failed, canceled) for the last 30 days.
System Backup Configuration	
Product	Displays the full product name of the detected definition vendor.
OS	Displays the operating system of the computer.
Source	Displays the source volume of the backup job (e.g., C:, G:, etc.)
Destination	Displays the destination path of the backup job (e.g., \\MYDRIVE\SPBackup\SERVER\SERVER_VOL-b001-i215.spi
Backup Type	Displays the backup type (e.g., full, continuous incremental, etc.).
Schedule	Displays the computer's current backup schedule.
Success Rate	Displays the current definition schedule's success rate calculation and value.
Unsuccessful Backups	
Displays any unsuccessful backups completed in the last 30 days for this computer.	Displays any unsuccessful backups completed in the last 30 days for this computer.
Backup Type	Displays the backup type (e.g., full, continuous incremental, etc.).
Start Time	Displays the start time of the backup job.
End Time	Displays the date and time the job started.
Status	Displays the date and time the job ended.
Next Success	Displays the time difference between the current failed backup job and the next successful backup.

Report Calculations

Calculation	Description
Successful Backup Jobs	Successful backup jobs is the count of backup jobs with a backup job status of 'Completed', used to calculate Success Rate.
Valid Backup Jobs	Valid backup jobs is the count of backup jobs with a backup job status of 'Completed' or 'Failed', used to calculate Success Rate.
Success Rate	Job Success Rate is calculated by dividing the successful backup job count by the valid backup job count and multiplying that value by 100. [Successful Backup Jobs] / [Valid Backup Jobs]*100

Sample Report



Report Header	Displays the report name, client name, location name, and company logo.
Computer Backup History	Displays a graphical history of completed, failed, and canceled backup jobs over different weeks. Completed backup jobs are displayed in green, failed jobs as red, and canceled jobs as yellow.
System Backup Configuration	Displays the backup job product and icon, the operating system, the source path, the destination path, the type of backup job, the backup job schedules, and the number of successful jobs compared to the number of total jobs.
Unsuccessful Backups	Displays the backup type, date and time the backup was started and ended, status of the backup, and the amount of time until the next successful backup in the schedule.
Signature Block	Displays signature and date lines for the technician and client to indicate that the backup jobs were completed to their satisfaction.
Report Footer	Displays the page number, title of the report, and the date the report ran.
Report	Displays on the last page of the report and explains the various parts of the report.

Legend	

Software List Report

The Software List Report displays a list of applications installed on each computer. This report can be run by Client, Location, Computer or all clients.

Sample Report

Report Header	displays the report name, company logo and the date the report was generated.	
Identification	displays the client, location of the computer, computer name, computer friendly name, the domain the computer is associated with, and the IP address.	
Software Summary	displays the operating system installed on the computer, the number of applications installed, the number of unclassified applications of the total number installed, the number of blacklisted applications and the total amount of space all applications are using.	
Installed Applications	lists all of the applications, version number, file location, the date the application was installed and the size of the application. Each application is also designated by its classification icon:	
	Unclassified	Indicates that the installed application has not been classified as good (whitelisted) or bad (blacklisted).
	Blacklisted	Indicates that the installed application has been classified as bad.
	Whitelisted	Indicates that the installed application has been classified as good.

Software Distribution Report

The Software Distribution report provides a list of the most common software installed at the selected level (e.g., all clients, specific client, location or contact).

Sample Report

Report Header	Displays the report name, date the report was run, and company logo.
Client/Location/Computer/Contact Information	Displays information for the client/location/computer/contact based on what level the report was run on. Information may include the name of the client/location/contact, address, email address, country, phone number and fax number.
Software Distribution	Displays a list of the most commonly installed software including the name of the application, version, installed size of the application, and number of assets that have the software installed.
Report Footer	Displays the page number, company name, and the date the report ran.
Report Legend	Displays on the last page of the report and explains the various parts of the report.

SubReports

Includes reports that can be added into other reports. Useful for creating consistent report components that can be used on all reports. For example, the two default SubReports are the report and page headers for all other default reports.

SubReportHeader

This subreport is used throughout the default Automate reports to generate a globally used report header page.

Important: Modifying this SubReport modifies all reports that use it.

Displays the first page of every report using the following format:

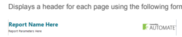
Report Logo	Displays the logo of your company or the default Automate logo.
Report Name	Displays the name of the report you run.
Report Description	Displays a brief description of the information that is included in the report.
Company Name	Displays the name of your company.

SubPageHeader

This SubReport is used throughout the default Automate reports to generate a globally used header page.

Important: Modifying this SubReport modifies all reports that use it.

Displays a header for each page using the following format:



Report Name	Displays the name of the report that was generated.
Report Parameters	Displays the date range that the report was generated.
Report Logo	Displays the logo of your company or the default Automate logo.

SubPageFooter

This SubReport is used throughout the default Automate reports to generate a globally used footer page.

Important: Modifying this SubReport modifies all reports that use it.

Displays a footer for each page using the following format:

Date	Displays the date the report was run.
Company Name	Displays the name of your company.
Page Count out of the Total Pages in the Report	Displays the number of the page in the report you are viewing out of the total number of pages (e.g., Page 2 of 3).

Ticketing

Includes reports that detail information about ticketing and time within Automate. These reports currently work on Automate ticketing and do not pull ticket information from a Manage server.

Ticket Summary Report

The Ticket Summary report displays client ticket statistics for the past 30 days, followed by a list of service tickets for each computer.
This report can be run for all clients or by a specific client.

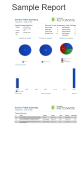
Business Case

The Automate Administrator wants to provide a report to their clients for an accurate assessment of time worked. They run the Service Ticket Summary report to show ticket statistics for the past 30 days to the client.

Report Frequency

It is recommended to run the report monthly but can be adjusted as desired.

Sample Report



Report Header	Displays the report name, company logo and the date the report was generated.
Client Information	Displays the client name, address, country, telephone number and fax number of the client.
Service Ticket	Displays the ticket summary for the last 30 days for the number of tickets that have been created,

Summary: Last 30 Days	opened, closed, overdue, unopened, resolved, combined, billed and the average number of days to close those tickets.
Tickets by Status	Displays a graphical breakdown of tickets on the basis of their current status in the form of a pie chart.
Tickets by Severity	Displays a graphical breakdown of tickets on the basis of their current severity level in the form of a pie chart.
Tickets by Category	Displays a graphical breakdown of tickets based on their category in the form of a pie chart.
Ticket Volume	Displays a graphical representation of the new tickets over the course of the last 30 days.
Report Footer	Displays the date the report was run, the company name, and the report page number.
Ticket Activity	Displays the ticket number, subject, category, priority, status, the date the ticket was received and the number of days since the ticket was last updated.

Timesheet Report

The Timesheet report gives a detailed look at the total amount of work time that has been added to tickets. The information provided includes client, ticket number, ticket time creation, ticket description, technician and if the time has been marked billed. This report can be run for all clients or by client or ticket ID.

Business Case

XYZ Computers has asked the Automate Administrator for a detailed list of work time for services rendered. The Automate Administrator runs the Timesheet Report for the client to show the number of billable hours and the corresponding tickets for the past 30 days.

Report Frequency

It is recommended to run the report monthly, but frequency can be adjusted, if needed.

Sample Report

Report Header	Displays the report name, company logo, and the date the report was generated.
Timesheet	Displays the client name, ticket number, the date the timeslip was created, the description, the technician that entered the timeslip, the timeslip category, and the amount of time that was entered on the timeslip, calculated as a fraction of hours.
Client Total	Displays the total number of timeslips, tickets and time, for the specific client.
Report Footer	Displays on the last page of the report and explains the various parts of the report.
Grand Total	Displays the total number of timeslips, tickets, and time.

Tickets Report

The Tickets report displays a detailed printout of up to 5,000 Automate tickets from the last 30 days and their associated ticket data items, excluding ticket comments. This report includes a signature block that is intended for technicians and clients to "sign-off", indicating its completion. This report can be run for computers, tickets, ticket status, clients or by a specific client.

Important: This report template by default collects a large amount of data from the Automate database. It is highly recommended that this report template is filtered too suit your needs. For more information about setting up filters, please refer to Use Filter Builder.

Business Case

The Service Manager wants to have insight into the efficiency of their team of technicians to determine if additional training is necessary. They run the Ticket report to see a list of all Automate tickets and the time spent working on the tickets.

Report Frequency

Recommended to run weekly.

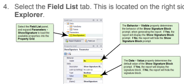
Configure Signature Block Defaults

By default, the Tickets report appears with a signature block. In order to schedule the report, a default setting to

show or hide the signature block must be selected, and the ShowSignature parameter must be set to Visible = No. If you would prefer to remove the signature block or return the signature block to the report, it can be toggled using the settings available to the ShowSignature parameter.

To configure signature block defaults:

1. From the **Control Center**, select **Tools** > **Report Center**.
2. From the **Reports** section of the sidebar, click **Report List**.
3. Select the **Tickets** report and then click **Edit Report** > **Modify Report** (located at the bottom of the window). The **Report Designer** tab displays.
4. Select the **Field List** tab. This is located on the right side of the window, sharing the same pod as **Report Explorer**.



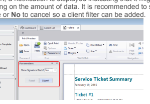
5. Expand the **Parameters** list and then select **ShowSignature**. The **Property Grid** pod is populated.
6. From the **Property Grid** pod, select the desired option from the **Behavior** > **Visible** drop-down. If **Yes** is selected, the report displays the **Show Signature Block** prompt when the report generates. If **No** is selected, the report hides the **Show Signature Block** prompt.
7. Select the desired option from the **Data** > **Value** drop-down. If **Yes** is selected, the report displays the signature block. If **No** is selected, the report hides the signature block.
8. From the toolbar, expand the **Save** option and select **Save As...**.
9. Specify the location and file name for the saved copy and click **Save**.
10. From the toolbar, click **Publish to Database**.
11. Select the applicable radio button. If the report is added as a new report, select **Add New Report**. If the changes you have made are to replace a report that is already being used, select **Replace Existing Report**.
12. Select or enter the name of the report to set the **Report Name**.
13. If needed, select the category from the **Category** drop-down.
14. If needed, select the contents of the **Description** field.
15. If needed, select or deselect the **Sub-Report** checkbox.
16. Click **Publish** to replace the report or **Cancel** to discard changes and return to the **Dashboard**.
17. Once the report opens in the **Report Designer**, you can make additional changes to the design, or you can close the **Report Designer** tab, and return to the **Dashboard**. After returning to the **Dashboard**, you can find your report using the **Report List** option.

Use the Signature Block

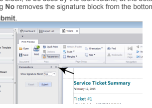
If the Signature Block is configured to appear when the report is generated, you must submit the value to display the signature block manually, when prompted.

To respond to the Show Signature Block prompt:

1. From the **Control Center**, select **Tools** > **Report Center**.
2. Click **Report List**.
3. Select and double-click the **Tickets Report** or click **View Report**. If a client filter has not been specified for the report, a notification is displayed indicating that it might take several minutes for the report to display, depending on the amount of data. It is recommended to select a client from the **Quick Filters**. Click **Yes** to continue or **No** to cancel so a client filter can be added.



4. Select the desired parameter from the **Show Signature Block?** drop-down. Selecting **Yes** displays a signature block, to be used by the technicians, at the bottom of each page of service ticket information. Selecting **No** removes the signature block from the bottom of each page of service ticket information.
5. Click **Submit**.



6. Click the **X** to close the **Parameters** panel.

Sample Report

Report Header	Displays the report name, company logo, and the date the report was generated.
Ticket Information	Displays the ticket number, the date/time the ticket was started, the date/time of the last contact pertaining to the ticket, ticket status, priority, category, and level.

Contact Information	Displays the contact information the ticket is associated with, to include the company, location, address, contact name, and telephone number.
Computer Information	Displays the computer information the ticket is associated with, to include the computer name, MAC address, local address, router address and operating system.
Ticket Activity	Displays all ticket details, to include the summary, description, date/time of when the ticket was created/completed, requester, and other pertinent ticket information.
Signature Block	Displays signature lines for the technician and the client to sign to indicate that the ticket was completed to their satisfaction. By default, the signature block displays; however, if the signature block does not display it has been configured to not display.