Get Started with CloudCheckr for AWS
Set Up for Success: Configuring Accounts and Utilizing Key Features
Contents

Configuring Accounts 3
Step 1: Log-On to CloudCheckr 4
Step 2: Prepare AWS Accounts 4
Step 3: Adding an Account in CloudCheckr 5
Step 4: Configuring an AWS Payer Account 6
Step 5: Access Management 7
Step 6: Customize Your CloudCheckr Experience 8
Step 7: Get a Platform Deep Dive from a CloudCheckr Technical Expert 8
Step 8: Get Access to CloudCheckr’s Learning Management System 9

Utilizing Key Features 10
Security 11
- Fix Security BPCs 11
- Setup Security Alerts 12
- Monitoring Changes 12
- Check Compliance 13
- Audit Compliance History with SnapBack 15

Cost 16
- Cleanup Idle, Unused, Misprovisioned, & Previous Generation Resources 16
- Setup Cost Alerts 17
- Setup Billing & Invoicing 18
- Manage Custom Charges and Credits 19
- Review Right Sizing Recommendations 19
- Review Reserved Instance Purchase Recommendations 20

Availability and Usage 21
- Best Practice Checks: Fix Availability 21
- Best Practice Checks: Fix Usage 22
- Review Heatmaps 22
- Configure EC2 Automation 23
Get Started

Configuring Accounts
Step 1 Log-On to Your CloudCheckr Account

CloudCheckr has a platform deployed in three regions. Direct your web browser to one of the following links and log-on using your existing CloudCheckr credentials:

app-us.cloudcheckr.com | app-eu.cloudcheckr.com | app-au.cloudcheckr.com

To sign up for a CloudCheckr account, get started here with a free trial.

Step 2 Prepare AWS Accounts

Before CloudCheckr can begin to monitor your AWS account, you must complete a series of actions in AWS to ensure your account is prepared.

Create a Cost and Usage Report

If the account is the master account for an Organization, create a Cost and Usage Report (CUR) in the Billing Dashboard. These steps can be skipped for any linked accounts, as the CUR is only available in the master account for the Organization. This should be completed at least 24 hours prior to the credentialing process for the best experience.

**Step A:** Enable at least one Cost Allocation Tag.

**Step B:** As a best practice, we recommend creating a new CUR with ‘ccr’ prefix so that it can be easily identified. Create a CUR report according to the specifications described here.

**Step C:** AWS will take a few hours to write the first report and the manifest that CloudCheckr needs to successfully ingest.

Enable CloudTrail Logs

If desired, CloudCheckr can ingest CloudTrail reports for alerting and historical auditing. This requires that your CloudTrail logs be written to an S3 bucket. Ensure that you complete the following steps:
**Step A:** Create a CloudTrail ‘Trail’ in your AWS account. This process is documented on the CloudCheckr Success Center [here](#).

**Step B:** Record the bucket to which the Trail is being written. It will be used later when configuring the Cross-Account Role (see Step 4).

---

### Step 3 Adding an Account in CloudCheckr

**Account Switcher**

CloudCheckr’s Account Switcher helps identify the account you are currently viewing and allows you to quickly switch to another account or a Multi-Account View (MAV) in your project.

You will find the Account Switcher in the Header bar on every page in the application, so you can change accounts or MAVs regardless of what report or feature you are using.

From the Account Switcher, you can navigate to the Account Hierarchy page by clicking the link in the upper right corner.

**Go to Account Hierarchy Page**

The Account Hierarchy page allows you to organize your accounts by account groups—CloudCheckr’s folder structure that simplifies account management. From this menu you can add new accounts, MAVs, and Attributes. Attributes are key/value pairs that help you organize and categorize your accounts.

**Adding an Account**

When you log-in to CloudCheckr for the first time your Account Hierarchy page will be pre-populated with a sample account. You can use this to look through the various CloudCheckr reports and functionality. You will want to add your own AWS accounts to get a full analysis of your environment.
**Step A:** Click + CREATE and select ‘Account.’

**Step B:** This will pop out a drawer on the right hand side of the UI.

**Step C:** Name the account and select AWS as the Cloud Provider. If applicable, select the appropriate Location for the new account in your account groups folder structure. Add any relevant Attributes for the account.

**Step D:** Click ‘Save.’

**Step E:** Click ‘Manage Credentials’ and complete the steps as directed in **Step 4** and **Step 5** below.

---

**Adding Multi-Account Views**

To configure a Multi-Account View, click + NEW MAV on the Account Hierarchy page on the ‘MAVs’ tab. Enter the name and cloud provider for the MAV in question. When creating the MAV, you will be prompted to add the accounts that should be included in the view. You have the option to add all accounts, or to filter by an Attribute, which allows you to add an entire subset of accounts at the same time.

---

**Step 4  Configuring an AWS Payer Account**

**Create a Cross-Account Role with our CloudFormation Template**

Leverage our CloudFormation template for the quickest and easiest experience creating a Cross-Account Role in AWS.

**Step A:** Click + CREATE and select ‘Accounts’ to Create your Role using our CloudFormation template (linked in Step 2 of the on-screen instructions).

**Step B:** The stack creation process will prompt you for some additional information, including the bucket names for your CUR and CloudTrail buckets. This [detailed guide](#) walks you through the Role creation process step-by-step.

**Step C:** Save your Role ARN in the CloudCheckr ‘Manage Credentials’ page after successfully creating the Role in AWS.

**Complete the Billing and Usage Configuration Page**

Completing this page will provide CloudCheckr with the necessary information to
locate and ingest the Cost and Usage Report (CUR). This step can be skipped for any linked accounts in an Organization, as the CUR is only available in the master account for the Organization.

**Step A:** Navigate to the ‘Billing and Usage’ page under Account Configuration

**Step C:** Open the AWS Console to the page for your CUR created earlier in this process.

**Step D:** Use the guide here to fill out the required fields in this page, then save your settings with the **Save Configuration** button.

For more information on how to perform the above steps, see CloudCheckr Success Center: Onboarding Your AWS Account

Depending on the size of your AWS deployment, the initial report update could take anywhere from a few minutes to a few hours. As soon as your initial report update finishes CloudCheckr will send you an Inventory Summary, S3 Summary, and Best Practices Report email (if you entered an email address when configuring your account). Once your initial report update finishes, you can begin reviewing the data within your account. For more in-app information about CloudCheckr updates and other Account Notifications, navigate to the ‘Notifications’ icon () in the upper right hand corner of the screen.

**Step 5** **Access Management**

CloudCheckr customers have full control over provisioning and managing user access within their account(s). User access can be configured with specific permissions, rights, and visibility based on the needs and role of the user.

To configure users & permissions and create their policies, reference the following walkthrough: CloudCheckr Success Center: Access Management
Step 6  Customize Your CloudCheckr Experience

After the initial report update is completed, your account will be populated with detailed information about your AWS deployment, organized into many pre-built (and any custom created) reports. Each time a report update completes, CloudCheckr will create new reports that reflect the most recent state of your AWS account. Since CloudCheckr retains a history of your deployment, you can drill into historical information for any of CloudCheckr’s reports.

Step A: Start by configuring CloudCheckr email notifications by navigating to the upper right of the UI and selecting the stacked dots icon ( ⬤ ) and then navigating to Account Configuration > Email Settings. There are a number of pre-built options for daily, weekly, and monthly emails, including Daily Bill Fluctuation Alerts, Best Practice Check summaries, Change Monitoring reports, Automation task information, CloudTrail detail, and AWS Health notifications.

Step B: Second, navigate to the upper right of the UI and select the stacked dots icon ( ⬤ ) and then to System Management > Customization to access the CloudCheckr basic whitelabeling options. Users can add their own logo and page icon, change the colors of the navigation menus, and change the support site link to an internal site, if desired.

Step 7  Get a Platform Deep Dive from a CloudCheckr Technical Expert

To help you get up and running quickly, CloudCheckr can advise on how you can make the most of the recommendations in your initial report update. The goal of this deep dive is to have one of our subject matter experts provide you some initial suggestions on what features to leverage based on your data and use cases and help get any of your specific questions answered.
Step 8  Get Access to CloudCheckr’s Learning Management System

CloudCheckr provides our customers and partners with access to an online, on-demand course called CloudCheckr 101. To get access to our courseware, navigate to the CloudCheckr Success Center and click on ‘Training and Certification.

![Training and Certification](image)

Register for courseware and certifications

To get started with CloudCheckr’s learning management system, simply fill out the form linked on the ‘Training and Certification’ page. Our learning team will reach out with more details.
Get Started

Utilizing Key Features
Security

Fix Security BPCs

CloudCheckr has over 600 Best Practice Checks (BPCs), and most of those are focused on security. Because CloudCheckr Best Practice Checks run at least once a day, by Day 2, you should be able to begin analyzing configuration vulnerabilities. Each check will be marked in Red, Orange, Yellow, or Green, based on severity, and Blue, if the check is informational in nature. Many times, thanks to Automated Self-Healing, our Fix Now and Always Fix buttons can fix the underlying issue, even if you’re not actively using the platform. CloudCheckr automation capabilities provide self-healing governance at scale.
Setup Security Alerts

Leveraging CloudCheckr’s Security Best Practice Checks will help to get your accounts configuration in order, but that doesn’t mean another AWS user can’t undo those changes. CloudCheckr has more than 30 pre-built CloudTrail alerts that users can toggle on/off (as shown below) as well as the ability to create custom alerts, using any CloudTrail event or resource-level changes, with advanced filtration capabilities and automation via AWS Lambda. CloudCheckr has notification integrations to maximize our customers’ ability to integrate systems, and can push alerts via email, SNS, Syslog, PagerDuty, Slack, JIRA, and ServiceNow.

Monitoring Changes

CloudCheckr’s Change Monitoring report allows you to track the day-to-day configuration and resource changes that occur in your AWS account. CloudCheckr takes a daily snapshot of your AWS deployment and compares it against the previous day; if anything has been added, deleted, or modified, users will be notified – and are able to drill into event detail, as shown below – using this report.
The Change Monitoring report can also be delivered as a daily email, so you’ll always know when changes are made to your EC2 instances, AMIs, EBS volumes, ELBs, EIPs, IAM users, policies or groups, security groups, VPCs, and more!

### Check Compliance

CloudCheckr Total Compliance has more than 35 interactive compliance benchmarking reports to assist with cloud governance at scale in regulated industries and the Public Sector, including CIS Benchmarks, a variety of NIST standards, PCI-DSS, HIPAA, FISMA, and many more. Each report references our Best Practice Checks and helps make sure your organization is in compliance.

With handy graphs that showcase your top five frameworks, and our SnapBack History view, you can easily demonstrate that your organization has achieved and maintained compliance to your executive team, or provide read-only access to the CloudCheckr platform for auditors.
To ensure that you are meeting requirements for a specific standard, click on the compliance framework to expand the underlying cloud-based controls. For each, CloudCheckr’s corresponding Best Practice Check(s) are displayed underneath; if there is a green check mark next to the Best Practice Check, that portion of the control passes.

Users can establish approval workflows and add remediation comments detailing any actions taken, to easily keep supervisors apprised of any changes. Once all associated Best Practice Checks are resolved and display the green check mark, then the overall Control changes to ‘Set Correctly = Yes’, and your compliance percentages will rise accordingly.
Audit Compliance History with SnapBack

Finally, the SnapBack History feature at the top right allows you to re-run the Total Compliance report for a prior date, in either Daily or Weekly view. CloudCheckr keeps historical data for up to seven years to assist customers with compliance or regulatory requirements. These SnapBack Reports can be used during the attestation process by auditors to prove that your organization was compliant at a point in time or over time, and can be added, as is, to a Body of Evidence report.

For more information on how to perform the above steps, see [CloudCheckr Success Center: Total Compliance](#).
Cost

Cleanup Idle, Unused, Misprovisioned, & Previous Generation Resources

CloudCheckr can immediately help users to identify resources for which they are incurring cost, without seeing the value of that investment. Start by looking through our Cost Best Practice Checks, and identify the BPCs that include the words “unused,” “not utilized,” under-utilized,” and “unattached,” among others.
In addition, we have savings tools to analyze whether you could save money by upgrading to a newer generation resource, and the ability to scan for many common service provisioning issues. Users can reference either our ‘Savings’ page or the Cost BPCs for all cost optimization opportunities.

**Setup Cost Alerts**

CloudCheckr allows users to configure budget alerts based off of both absolute budget thresholds and relative cost spikes. You can add multiple thresholds at which to trigger an alert (as shown below), and alerts can be filtered by accounts, service, region, usage type, operation, and/or tag. Like our Security Alerts, CloudCheckr has notification integrations via email, SNS, Syslog, PagerDuty, Slack, JIRA, and ServiceNow.
Setup Billing & Invoicing

CloudCheckr can manage the entirety of the invoicing process from ingestion of the AWS billing reports, to sending invoices to customers/stakeholders through our invoice generator, to ad hoc profit reporting. We offer both pre-built and custom invoice formats and can generate customers’/stakeholders’ bills on a scheduled day each month or with the click of a button.

Our invoicing features help our partners and customers dramatically reduce time and expenses of the billing process. CloudCheckr users can create invoices, in PDF or CSV format, grouped by service, region, operation, usage type, and/or tag, for one or more accounts.

Beyond invoice itemization and filtering, there are many options to experiment with. For example, invoices can display multiple cost types, known as Blended, Unblended, or List Cost rates. List Cost is a CloudCheckr custom cost layer that gives users full power over the allocation of RI-related and volume-based discounting across the consolidated bill.
Invoice period is also editable. Users can choose a calendar month or a specific date range as the billing period, show precise values beyond 2 decimal places, and perform currency conversion.

**Manage Custom Charges and Credits**

In addition to saving money, CloudCheckr enables Managed Services Providers and Enterprises with an IT profit center to charge more for AWS consumption and build margin. You can create charges that are a percentage uplift, or a flat dollar amount, each with multiple tiering capabilities and advanced filters. Administrators can also reconfigure the consumption rate for any service in the AWS catalog, including CloudFront. Similarly, you can share cloud provider credits across accounts, if desired, and pass the savings on to your clients.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Start Date</th>
<th>End Date</th>
<th>Type</th>
<th>Charge Value</th>
<th>Account IDs / Families</th>
<th>Description</th>
<th>Region</th>
<th>Resource ID</th>
<th>Stack</th>
<th>Stack Order</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>01/01/2017</td>
<td></td>
<td>Monthly Discount</td>
<td>-7.00%</td>
<td>All Accounts</td>
<td>Discount for EC2 - Invoice #32127</td>
<td>All Regions</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>02/01/2018</td>
<td>02/28/2018</td>
<td>Monthly Premium</td>
<td>10.00%</td>
<td>All Accounts</td>
<td>Stack 2 Custom Charge Test</td>
<td>All Regions</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>02/01/2018</td>
<td>02/28/2018</td>
<td>Monthly Discount</td>
<td>-11.00%</td>
<td>All Accounts</td>
<td>Enterprise Discount Program</td>
<td>All Regions</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>02/01/2018</td>
<td>04/01/2018</td>
<td>Premium for all charges</td>
<td>7.00%</td>
<td>All Accounts</td>
<td>All The Stuff</td>
<td>All Regions</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Review Right Sizing Recommendations**

The EC2 Right Sizing report helps you optimize the sizing of your instance fleet by providing recommendations both within and across families and a ‘Request Fix’ (or ‘Fix Now,’ depending on your account permissions) button to make the necessary changes to the instance in question without leaving the CloudCheckr UI.
Users should wait until the later part of their evaluation to review the Right Sizing report, to ensure that CloudCheckr has a couple of weeks’ worth of utilization history to be able to make accurate recommendations; typically, we advise waiting to effectuate recommendations until the platform has the ability to use 30 day average CPU history. In many cases, right sizing is one of the places that CloudCheckr customers achieve the greatest cost savings.

<table>
<thead>
<tr>
<th>Request ID</th>
<th>Instance ID</th>
<th>Current Hourly Cost</th>
<th>Projected Hourly Cost</th>
<th>Possible Hourly Savings</th>
<th>Platform</th>
<th>Instance Type (Size)</th>
<th>Recommended 30 Day Avg CPU</th>
<th>30 Day Avg Memory</th>
<th>30 Day Avg Network In</th>
<th>30 Day Avg Network Out</th>
<th>30 Day Peak CPU</th>
<th>30 Day Peak Mem</th>
<th>Utilization Score %</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request 1</td>
<td>1234567890</td>
<td>$0.02</td>
<td>$0.01</td>
<td>$0.01</td>
<td>Other Linux</td>
<td>t3a.small</td>
<td>1.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>3.22%</td>
<td></td>
<td></td>
<td>25%</td>
<td>running</td>
</tr>
<tr>
<td>Request 2</td>
<td>2345678901</td>
<td>$0.01</td>
<td>$0.01</td>
<td>$0.01</td>
<td>Amazon Linux</td>
<td>t2.micro</td>
<td>0.11%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.12%</td>
<td></td>
<td></td>
<td>5%</td>
<td>running</td>
</tr>
<tr>
<td>Request 3</td>
<td>3456789012</td>
<td>$0.06</td>
<td>$0.06</td>
<td>$0.06</td>
<td>Windows</td>
<td>t2.large</td>
<td>0.48%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>14.94%</td>
<td></td>
<td></td>
<td>10%</td>
<td>running</td>
</tr>
<tr>
<td>Request 4</td>
<td>4567890123</td>
<td>$0.05</td>
<td>$0.04</td>
<td>$0.04</td>
<td>Amazon Linux</td>
<td>t2.medium</td>
<td>0.24%</td>
<td>0.01%</td>
<td>0.01%</td>
<td>0.28%</td>
<td></td>
<td></td>
<td>8%</td>
<td>running</td>
</tr>
<tr>
<td>Request 5</td>
<td>5678901234</td>
<td>$0.09</td>
<td>$0.09</td>
<td>$0.09</td>
<td>Amazon Linux</td>
<td>t2.large</td>
<td>0.26%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.30%</td>
<td></td>
<td></td>
<td>9%</td>
<td>running</td>
</tr>
</tbody>
</table>

Users are often concerned about permissions to make right sizing decisions. Lower level users do not have the requisite permissions to ‘Fix Now,’ and instead will see the ‘Request Fix’ button, as shown above. In general, requesting a fix opens a ‘Workflow.’ Users with the ‘Admin Workflow’ permission can approve/reject requests, while users with the ‘Open Workflow’ permission are only allowed to make a request. Users who do not have either of these workflow permissions (i.e. read-only users) cannot make requests at all.

**Review Reserved Instance Purchase Recommendations**

By the end of the evaluation period, users should have enough data to assess CloudCheckr’s recommendations for purchasing Reserved Instances (RIs). These come with a discount, which is higher the more you pay upfront. CloudCheckr will display the recommended configuration, and give you the cost breakdown for different purchasing scenarios. CloudCheckr can look back at usage over the prior 30, 60, 90, or 180 days to make these recommendations, and users can filter and
view the recommended RIs by Instance or by Frequency, for static and dynamic environments, respectively.

---

**Discuss Savings Plan Recommendations**

Savings Plans are another way to purchase reserved capacity and get discounts off of on-demand pricing. CloudCheckr’s team of technical experts is able to assist you in evaluating your compute usage and the potential for Savings Plan purchases. Contact your CloudCheckr account representative if you would like to take advantage of this consultation.
Availability and Usage

Fix Availability

CloudCheckr has dozens of Best Practice Checks (BPCs) focused on High Availability. Use these to make sure that you have backups and snapshots, that you are using multiple zones and load balancers, and that your resources have passed various health checks.

- **31 EBS Volumes Without A Snapshot**
- **11 RDS Instances Configured To Retain Backups For Fewer Than 30 Days**
- **4 SES Domains With Failure Status**
- **2 SES Email Addresses With Failure Status**
- **6 Auto Scaling Groups Not Utilizing Multiple Availability Zones**
- **43 EBS Volumes With No Recent Snapshots (30 days)**
- **30 EC2 Instances Not Utilizing Termination Protection**
- **2 Elastic Load Balancers Not Utilizing Multiple Availability Zones**

Fix Usage

Similar to our Security, Cost and Availability Best Practice Checks, click on the Usage tab and look for under and over-utilized resources. Parameters to determine what constitute adequate utilization are fully editable by the individual user by clicking the gear symbol.

Review Heatmaps

CloudCheckr Utilization Heatmaps span five resource types – EC2, RDS, Elasticache, Redshift, and DynamoDB, and display the average utilization, by hour, over the last 7 days. The colors on the heatmap shift from blue, indicating less utilization, to white, to red, indicating more utilization. In addition to seeing the heatmap for ALL of a particular resource, you can use the instance dropdown to view the heatmap for
individual instances, or grouped resources by a tag. Selecting ‘Absolute’ will display the map ranging from 0% to 100%, while selecting ‘Relative’ will display the map using the lowest and highest utilization percentages, as shown below.

**Configure EC2 Automation**

CloudCheckr has seven automation tasks designed for ease of governance of EC2 instances at scale: Cleanup Security Groups, Cleanup Snapshots, Cleanup Volumes, Terminate Idle EC2 Instances, Stop EC2 Instances, Start EC2 Instances, and Copy Tags to Volumes.
Each task allows you to filter down by various criteria to manage different groupings of instances, and make decisions about how and when the automation will run. Users have the option to manually select the items to be processed from within the UI, receive an email notification when new resources are detected that fit the parameters of the automated task, or simply have CloudCheckr process any non-ignored resources that fit the task parameters.
About CloudCheckr

We deliver total visibility—across multiple public clouds and hybrid workloads—making the most complex cloud infrastructures easy to manage. From government agencies to large enterprise and managed service providers, CloudCheckr customers deploy our SaaS solution to secure, manage, and govern the most sensitive environments in the world. Our industry-leading cloud management includes cost savings, billing & invoicing, cloud security & compliance, resource optimization, and automation available in CloudCheckr CMx, CMx High Security for regulated industries, CMx Federal for FedRAMP Ready procurement, and CloudCheckr Finance Manager for IT cost management across hybrid cloud.