

Telstra Cloud Sight Frequently asked question (FAQs)



Welcome to the Telstra Cloud Sight FAQs

Australian account holders

For sales, account set-up enquiries and technical support, contact your Telstra representative or visit the [Telstra Cloud Sight page](#) on our website where you'll find all our contact details, a pricing guide, user guide, feature descriptions, FAQs and Our Customer Terms.

Telstra Global account holders

For sales and account set-up enquiries, contact your Telstra Global representative or visit the [Telstra Global Cloud Sight page](#).

Conventions used in this guide

The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, email addresses and hyperlinks are shown in bold italics, for example [***www.cloud.telstra.com***](http://www.cloud.telstra.com).

Button names and titles/features on your computer screen are shown in italics.

User input is shown in typewriter font.

Telstra Cloud Sight User Guide, Version 3.0

© Telstra Limited (ABN 64 086 174 781). All rights reserved.

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, information contained within this manual cannot be used for any other purpose other than the purpose for which it was released. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the written permission of Telstra Corporation Limited.

Words mentioned in this book that are known to be trademarks, whether registered or unregistered, have been capitalised or use initial capitals.

What's Inside

Chapter 1 About Telstra Cloud Sight

Chapter 2 Access, users and roles

Chapter 3 Compliance

Chapter 4 Budget

Chapter 5 Charges and Billing

Chapter 6 Support

About Telstra Cloud Sight

What is the Telstra Cloud Sight platform?

The Telstra Cloud Sight service allows your organisation to manage compliance, budget, security and resources associated with your eligible cloud accounts via an online portal.

Import your existing eligible cloud accounts or add new eligible accounts to the Telstra Cloud Sight platform. You can then apply Telstra Cloud Sight features to those accounts.

What can I do on the Telstra Cloud Sight platform?

Once you add or import cloud accounts to the Telstra Cloud Sight platform, the following features can be applied:

- **Compliance** – apply a compliance blueprint to protect monitor and audit your cloud account. See more details [here](#).
- **Budget** – set up a monthly budget and email alerts. Alerts will be sent when a cloud account is forecast to exceed, and exceeds the set budget. See more details [here](#).

These features also offer a range of reports and alarms that allow you to keep track of of your cloud accounts. The Telstra Cloud Sight platform also offers centralised access to the management consoles of your cloud services – so you can easily make changes if you find something not to your liking.

What type of cloud accounts can I use with the Telstra Cloud Sight platform?

Currently you can use AWS accounts with the Telstra Cloud Sight platform.

How do I sign up for the Telstra Cloud Sight platform?

You can now register online at <https://getcs.telstra.com/register>.

I'm an international customer. Can I sign up?

Yes, please contact your Telstra representative or your local sales team. You can find their details at www.telstraglobal.com/contact.

Online registration is not yet available for international customers.

Are there any pre-requisites for signing up to the Telstra Cloud Sight platform?

You'll need the following before you sign up:

01. You need to be a Telstra Cloud customer with a Telstra online account.

- If you're not a Telstra Cloud customer yet or don't have Telstra online access:
 - a. Within Australia – [view our registration options](#) (to purchase any of our cloud services, you must have an [Australian Business Number](#))
 - b. Outside Australia – [contact us](#) or your Telstra representative

02. You'll need a Cloud Management Platform (CMP) account. If you don't already have one, your Telstra representative can help you sign up for the service.

What integrated services do I get access to when I sign up for the Telstra Cloud Sight platform?

Once sign-up is complete, you'll have access to:

- Telstra's Cloud Management Platform (CMP) powered by RightScale – performs all your cost and budget functions
- Dome9 – for all your compliance functions
- The management console of your cloud account – e.g. AWS management console

How do I create a new cloud account?

Follow the steps listed on the 'Adding a new cloud account' section on our [user guide](#).

Remember to use a unique email address for each cloud account you create.

How do I import a cloud account?

When you sign up for the Telstra Cloud Sight platform, you'll be asked to provide a list of cloud accounts you want transferred to Telstra. If you want to import an eligible cloud account after sign up, contact your Telstra representative who will guide you through the process.

Do I need a unique email address for every new account I create?

Yes. AWS uses this email address as the root identifier for your new account. For that reason it has to be unique among all your AWS accounts.

How do I cancel my Telstra Cloud Sight service?

Contact your Telstra representative or your local sales team.

If you're an international customer, you can find their details at www.telstraglobal.com/contact.

Access, users and roles

How do I log into the Telstra Cloud Sight platform?

When you first sign up or are invited to use the Telstra Cloud Sight platform, you'll get an email with the following details:

- Domain ID
- Email address
- Create password button

Use the domain ID, the email address along with the password you create, to log into the Telstra Cloud Sight platform.

What roles can be assigned to users on the Telstra Cloud Sight platform?

There are three basic roles that can be assigned to users on the Telstra Cloud Sight platform:

- Service Admin
- Service Reader
- Cloud Account Admin

Service Admins can add users, assign roles and manage them across the Telstra Cloud Sight platform service. They can also add cloud accounts, add users to that cloud account and manage all cloud accounts on the service.

Service Readers can view the Telstra Cloud Sight platform service and cloud account details. A service reader may also be assigned administration rights for cloud accounts (Cloud Account Admin rights).

Cloud Account Admins can manage the cloud accounts to which they're assigned, including users on that account.

Do roles and permissions on the Telstra Cloud Sight platform extend to integrated services such as Dome9 and RightScale?

All Telstra Cloud Sight roles (Service Admin, Service Reader and Cloud Account Admin) have read access on integrated systems.

Is a user's access to an integrated service removed when that user is removed from the Telstra Cloud Sight platform?

No. If you want a user's access removed from an integrated service like Dome9 or RightScale, you must do so manually, from each individual service.

Can I access a record of user activity on my organisation's Telstra Cloud Sight account?

Yes. You can find a user activity log on the 'Manage user access' page.

What actions are recorded on the user activity log?

On the user activity log you'll find a record every time a user:

01. Signs in or out of Telstra Cloud Sight
02. Adds or removes a cloud account
03. Adds or removes a feature on a cloud account
04. Adds or removes a user
05. Modifies a user account
06. Updates system settings
07. Updates profile settings

What's Two-Factor Authentication (2FA)?

Two-Factor Authentication, or 2FA, is two step verification process that needs not only a username and password but also something that only a user has in his or her possession, like a physical token or a code sent to their mobile phone number.

The type of 2FA used on Cloud Sight requires an app to be downloaded on your mobile device. You'll find step-by-step directions on how to enable 2FA and log in with 2FA on the Telstra [our user guide](#).

Why do I need 2FA?

2FA gives your account an extra layer of security. Even if your password is compromised, attackers won't have the unique code, which is generated just for you and used only once.

How do I enable 2FA on my Telstra Cloud Sight account?

See Enabling Two-Factor Authentication under the '[Telstra Cloud Sight settings and profile](#)' section of our user guide for step-by-step directions.

After 2FA is activated, do I need to scan a QR code every time I log in?

No. You only need to do that the first time you log in. Every subsequent log in will need you to enter the authentication code on your mobile app in addition to the regular domain ID, email address and password combination.

Compliance

What is compliance?

The compliance feature allows you to select a blueprint of your choice and apply it to your eligible cloud account. The blueprint is used as a benchmark, each one offering a different set of measures to help keep your account compliant with industry regulations and best practices.

We currently offer three compliance blueprints:

01. Center for Internet Security (CIS) compliance. Learn more about CIS compliance [here](#).
02. Health Insurance Portability and Accountability Act (HIPAA) compliance. Learn more about HIPAA compliance [here](#).
03. Payment Card Industry (PCI) and Data Security Standard (DSS) compliance. Learn more about PCI DSS compliance [here](#).

There's another option if you don't want to choose the above blueprints

04. Keep AWS settings – this allows you to get reports on your cloud account without changing the default AWS configuration.

There are three ways to apply a blueprint to your cloud account:

01. Deploy the blueprint to your cloud account (new cloud accounts only)
02. Enable alarming on your cloud account – when you choose this option any changes to your cloud account will be tested against the blueprint. If changes breach compliance you'll immediately receive an alarm in you email.
03. Get reports on your cloud account's compliance status – there are two kinds of reports you can choose from:
 - a. Daily assessment reports – results of daily compliance tests. This includes details of all failures, in order of severity.
 - b. Hourly change reports – a list of all changes that occurred to the account within the past hour.

Please note that:

- A blueprint only contains a limited subset of the total number of recommendations within a specific compliance standard relevant to your eligible cloud services account;
- the blueprint does not address broader architectural build (e.g. connectivity) or processes and systems outside of your eligible cloud services account;
- the blueprint does not provide a certificate of compliance for the limited recommendations it supports;
- we do not guarantee end-to-end compliance with the industry standard and we do not and cannot assume your compliance obligations under all or any of the industry standards; and
- you remain responsible for your overall compliance with the applicable industry standards.

How do I add compliance to my cloud account?

You can add compliance via the Telstra Cloud Sight platform. See the '[Compliance](#)' section of our user guide for more details.

Can I add compliance later (after I've added a new cloud account)?

Most compliance features – selecting your blueprint, adding alarming and reporting – can be added after you create a new account. Blueprint deployment, however, can't be carried out after account creation (A blueprint can only be deployed as a new account is created).

Can I change a blueprint once it's applied?

No. The selection can't be modified after it's applied to your cloud account. Only alarming and reporting settings can be changed after you've configured an account.

Can I add compliance to an imported account?

You can apply most compliance features – selecting your blueprint, adding alarming and reporting – to an imported account. Blueprint deployment, however, can't be carried out on imported accounts (A blueprint can only be deployed as a new account is created).

Can I apply more than one blueprint?

No. You can only apply one blueprint per cloud account.

Do I have to deploy the blueprint?

If you don't want to change the standard configuration of a cloud account, you can choose to not deploy the blueprint. You can instead enable alarming and/or get reports on your account to keep it compliant with your chosen blueprint.

Remember, blueprint deployment can only be done when an account is being created.

What happens when I choose 'Keep AWS settings' instead of a blueprint?

Your cloud account is created with standard AWS settings and compliance measures such as deployment and alarming are no longer applicable. You can, however, request reporting on your account.

What's the difference between alarming and reports?

When you enable alarming on your cloud account, you'll receive an email whenever a change on your account breaches compliance.

Reporting is a periodic function. You can choose between a daily and an hourly report, or both.

- 01. Daily assessment reports** are results of daily compliance tests. This includes details of all failures, in order of severity.
- 02. Hourly change reports** are a list of all changes that occurred to the account within the past hour. This is similar to an alarm, although it lists all changes on the cloud account, not just those that breach compliance.

Can I change my alarming or reporting preferences later?

Yes. Alarming and reporting preferences can be modified.

Where can I find details on how my cloud accounts are performing (in terms of compliance)?

Account level compliance details can be found under the Compliance details tab when you select an account from the landing page.

The 'Compliance' page, which can be accessed from the navigation bar on the left, provides a view of performance across all your cloud accounts.

Both these pages have a more details link that takes you to Dome9 where more detailed statistics of your account's compliance can be found.

See the ['Compliance'](#) section of our user guide for further details, including screenshots.

What do the 'passed' and 'failed' percentages on the compliance pages mean?

The 'passed' percentage represents the ratio of compliance recommendations that have passed testing on your cloud account. Likewise, the 'failed' percentage represents the failed recommendations. Recommendations are particular to the blueprint you've selected for each of your cloud accounts.

Tests are run to validate each recommendation across every relevant resource linked to your cloud account. If even a single resource fails to comply with a recommendation, that recommendation is marked as a failure. The same test can fail multiple times across many resources but only contribute to one rule failure.

The 'passed' or 'failed' percentages are a proportion of the number of recommendations on a blueprint. They do not indicate the rate of success or failure at an resource level.

How often are the compliance tests run?

Dome9 runs hourly compliance tests.

What do the severity values indicate?

Each compliance recommendation has a severity grading of high, medium or low. Each time a recommendation associated with your cloud account fails a test, that failure is recorded against the severity of the rule.

Severity numbers are not proportional to recommendations 'passed' and 'failed' rates.

We recommend all high-severity failures be remediated as soon as possible.

What's the General Data Protection Regulation (GDPR)?

The GDPR is a regulation in European Union law that makes organisations responsible for maintaining best practices to secure EU data anywhere it resides.

Does the GDPR apply to me?

If your organisation holds data belonging to individuals living within the European Union (EU), the GDPR could apply to you.

How does Telstra Cloud Sight help me prepare for GDPR?

When you select the Include **General Data Protection Regulations (GDPR)** readiness recommendations option, you'll get a report from Dome9 detailing results of tests that were run against your eligible cloud accounts, assessing your readiness for the GDPR.

Entities/resources including your compute instances, databases, storage, security groups and IAM within your eligible cloud accounts will be tested for compliance with certain security requirements within the GDPR such as encryption, monitoring, reporting and access control where appropriate. Failures will be highlighted by severity.

You'll receive this report along with your compliance blueprint report at your chosen reporting frequency.

Budget

What does the budget feature offer me?

This feature allows you to set a monthly budget and enable alerts. Alerts are sent to you when your budget is forecast to exceed, and exceeds your budget.

You can choose to be alerted daily, weekly, fortnightly or monthly.

How do I create a budget?

Follow the steps listed in the [‘Costs’](#) section of the user guide.

Do I have to set the budget figure in US dollars?

Yes, all AWS costs are currently in US dollars. You can use the [Reuters exchange rates page](#) for the latest conversion rates.

What are forecast costs?

The forecast cost is a prediction of what your total cost would be at the end of the month.

The forecasts are based on:

- Publicly available information; and
- The fee information for the eligible cloud services that you choose to manage through the Telstra Cloud Sight platform and that may be obtained from your cloud account bill or from the third party provider.

Accordingly, forecasts:

- May not be accurate or complete;
- May be in another currency and require you to convert the forecast to Australian dollars, which will introduce variability due to currency fluctuations;
- May not take into account all options and discounts;
- May not take into account the specifics of your agreed pricing with us or third providers (although you may be able to apply mark-ups or mark-downs within the Telstra Cloud Sight platform to adjust the standard pricing); and
- May not reflect the actual price at which you may be able to purchase the cloud service (whether from us or another supplier).

What are actual costs?

The actual cost is what you've spent to-date from the beginning of the month.

The actual costs are based on:

- Publicly available information; and
- The fee information for the eligible cloud services that you choose to manage through the Telstra Cloud Sight platform and that may be obtained from your cloud account bill or from the third party provider.

Accordingly, forecasts:

- May not be accurate or complete;
- May be in another currency and require you to convert the forecast to Australian dollars, which will introduce variability due to currency fluctuations;
- May not take into account all options and discounts;
- May not take into account the specifics of your agreed pricing with us or third providers (although you may be able to apply mark-ups or mark-downs within the Telstra Cloud Sight platform to adjust the standard pricing); and
- May not reflect the actual price at which you may be able to purchase the cloud service (whether from us or another supplier).

How is a forecast cost calculated?

The forecast cost is calculated using the average daily cost to-date, multiplied by the number of days in the month.

Where can I find details on how my cloud accounts are performing (in terms of costs)?

Account level cost details can be found under the **Cost details** tab when you select an account from the landing page.

The 'Costs' page, which can be accessed from the navigation bar on the left, provides a view of performance across all your cloud accounts.

Both these pages have a more details link that takes you to RightScale Optima, which is part of the the Cloud Management Platform (CMP) powered by RightScale – a Telstra Cloud Sight platform integrated service.

See the ['Costs'](#) section of our user guide for further details, including screenshots.

What's RightScale Optima?

RightScale Optima is part of the Cloud Management Platform (CMP) service we use to help you manage and optimise your cloud costs. [Learn more.](#)

Charges and billing

Where can I find prices?

Details of fees for Telstra Cloud Sight services can be found on our [pricing guide](#).

When does charging start?

You'll begin to be charged when your service is provisioned.

How will I be billed?

All charges, additional usage and any applicable add-on fees will be charged to your Telstra account.

How does billing work if I have multiple accounts?

If you have multiple Telstra billing IDs, you can select the ID you want your services charged to when you make your first purchase.

Read the [Account Management User Guide](#) to find out how you can separate your billing.

Support

I've just applied for a Telstra Cloud Sight service. Who do I contact for a progress update?

The typical time to activate a Telstra Cloud Sight account is 3 business days. This time may vary, depending on whether you've completed your service activations (RightScale, Dome9 etc.) and/or eligible cloud account transfers.

You can contact our concierge team for status update, via email: concierge@telstracloudpremiumservices.zendesk.com.

Where can I find more information on how to use the Telstra Cloud Sight platform?

Try our [user guide](#). You can also contact our support team via CloudServicesSupport@online.telstra.com.au.

See below FAQ for help with advanced technical questions.

Who do I contact for help with advanced technical questions about the Telstra Cloud Sight platform?

Cloud Advanced Services provides flexible, on-demand technical expertise when you need it. Different sized packages are available to meet your requirements so you only pay for what you need.

For further details please contact your Telstra representative.

How do I log any faults I find on the Telstra Cloud Sight platform?

You can contact our support team via CloudServicesSupport@online.telstra.com.au. Please include the following information in your email:

- Your name
- Domain ID
- AWS subscription ID
- Email address
- Phone number
- Organisation name
- Category: "Fault"
- Describe the fault, including any investigations and troubleshooting steps already performed to resolve or isolate the fault. Attach screen shots.
- Date fault occurred (include time of fault if known).

I have billing questions. Who do I contact?

For all billing enquiries please send an email to CloudServicesSupport@online.telstra.com.au.

Please include the following information in your email:

- Customer contact name
- Domain ID
- Customer's AWS subscription ID
- Customer contact email
- Customer contact phone
- Customer company name
- Category: "Enquiry"
- Billing period
- A short description of your enquiry