TrustLayer | DATASHEET

Managed Change Service

TrustLayer policy and configuration changes, handled by TrustLayer experts.

The Managed Change Service gives you a practical way to manage regular changes across TrustLayer Email Security, Web Security, CASB and Security Awareness Training — without turning every change into a support issue or a separate professional-services project.

AT A GLANCE

What it is, at a glance.

Best for	Customers and MSPs with regular TrustLayer policy, rule or configuration change requests.
Products covered	Email Security, Web Security, CASB and Security Awareness Training.
Delivered by	TrustLayer engineers.
Includes	Request review, implementation, basic validation, documentation and monthly reporting.
Service hours	Monday to Friday, 09:00–17:00, excluding public holidays.
Out of hours	Available by prior agreement and may incur additional cost.

WHEN TO USE IT

The right tool for routine change.

Use it when an existing TrustLayer environment needs regular operational updates — policy and rule changes, exception handling, unblock requests, threat-protection tuning, reporting or SAT campaign updates. It is not for major redesigns, migrations, incident response or custom project work, which sit with support or professional services.

WHAT'S COVERED

Here for when you need help with:

- Filtering rule updates
- Safelist or deny list changes
- Unblock requests
- SSL/TLS inspection exceptions
- Application, category, user or group-based policy changes
- Agent profile updates
- Threat protection tuning
- Scheduled and ad-hoc activity reports
- SAT journeys, content packs, phishing simulations and landing pages

TrustLayer reviews the request, makes the change, checks it has applied as expected and records what was done.

COVERAGE

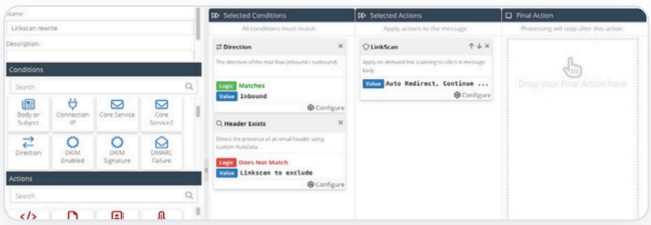
Across every layer you run.

Changes are handled per product, by engineers who know the platform.

TrustLayer Email MAIL

Keep filtering, threat protection and sender controls up to date without leaving every rule or safelist change to internal teams.

- Filtering rule updates
- Spam Safe and Deny list changes
- Business Email Compromise entries
- Nearby Domain detection entries
- LinkScan safelists and threat-protection tuning
- Activity reports
- Post-change checks and documentation

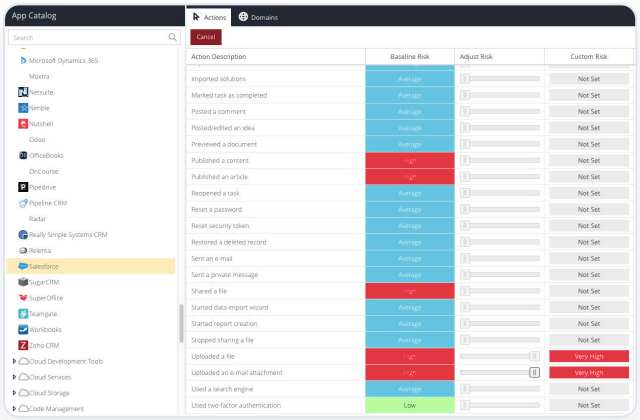


LinkScan and filtering rules kept current — conditions, matches and actions.

TrustLayer Browse BROWSE

For Web Security and CASB, the service supports changes that control how users access websites, cloud applications and online services.

- Filtering rule updates
- User, group, device or OS-based policy updates
- SSL/TLS inspection exceptions
- Application and category controls
- Custom URL groups, bypasses and exceptions
- Agent profile updates
- Threat-protection tuning and unblock requests
- MIME type configuration
- Activity reports and documentation

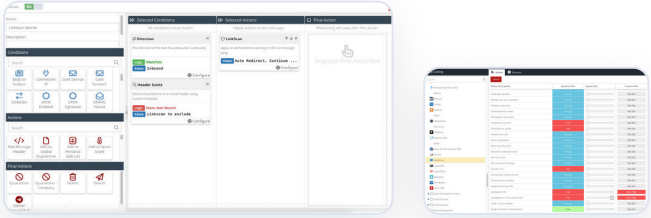


Web and cloud-app policy — categories, apps and action-level risk.

TrustLayer Users USERS

For Security Awareness Training, TrustLayer helps keep training journeys, phishing simulations and campaign assets current as user needs and risks change.

- Journey content updates
- On-demand content sends
- Content pack management
- Phishing simulations
- Landing page customisation
- Branding updates
- Scheduled or ad-hoc reports
- Post-change checks and documentation



HOW IT WORKS

Request to record, in seven steps.

1. Request	The customer or MSP submits the change request with the information TrustLayer needs to review it.
2. Review	TrustLayer checks the request for detail, risk, impact and possible policy conflicts.
3. Approval	The nominated customer contact confirms the change can go ahead.
4. Change	A TrustLayer engineer makes the change.
5. Check	TrustLayer carries out basic validation to confirm the change has applied as expected.
6. Record	The work is documented, including implementation notes and verification details.
7. Report	Monthly reporting summarises change activity, service-target performance and recurring themes.

ONBOARDING & REPORTING

Health-checked in, reported on throughout.

Before the service begins, TrustLayer may health-check your environment — configuration, policies, alerts and operational health — and outline any remediation needed first.

Monthly reporting summarises submitted, completed and pending requests, service-target performance, recurring themes, policy-hygiene recommendations, notable security improvements or gaps, and remaining service credit. Change records include request details, approval logs, implementation notes and post-change verification.

SERVICE TARGETS

Clear response and completion targets.

Targets apply during standard business hours, Monday to Friday, 09:00–17:00, excluding public holidays. Out-of-hours or weekend changes must be agreed in advance and may incur additional cost.

REQUEST TYPE	INITIAL RESPONSE	COMPLETION TARGET
Standard change	Within 4 business hours	Within 1 business day
Moderate change	Within 8 business hours	Within 2 business days after approval
Emergency change	Within 1 hour	Within 4 hours, subject to approval
Planned major change	Within 1 business day	Based on agreed maintenance window

MANAGED CHANGE SERVICE VS SUPPORT

Two services, one platform.

Managed Change Service is separate from standard TrustLayer support. Support handles faults, service issues, degradation and general technical queries. Managed Change Service handles operational changes — policy updates, rule changes, exceptions, safelist updates, unblock requests and reporting changes.

ONE PLATFORM

Every layer, kept current.

Browse

Web
Stop web threats and filter distractions with a proxy-less agent or gateway.

CASB
Discover, analyse and control user interaction with cloud applications.

Posture

CSPM
Continuous misconfiguration checks across AWS, Azure and GCP.

SSPM
Posture management across SaaS apps like Microsoft 365 and Salesforce.

Mail

Email
Stop known, unknown and emerging email threats before the inbox.

Archiving
Compliant, searchable storage for eDiscovery and continuity.

Users

SAT
Reduce human risk with engaging, automated security training.

MFA
Stop stolen passwords being useful with adaptive authentication.

WHY IT WORKS

One stack, under control.

Go direct
No proxies. No slowdowns. Just protection at full speed.

Get layered
Start with what you need, and scale as your business evolves.

Deploy fast
Live in minutes, not months, with prebuilt templates and zero fuss.

Stay quiet
Become invisible to users, but invaluable to your security team.

TRUSTLAYER LTD

4.2 Belvedere House, Basing View, Basingstoke, Hampshire RG21 4HG

Phone: +44 (0) 845 230 9590

trustlayer.co.uk

ONE PLATFORM

Managed Change Service keeps your whole TrustLayer stack current — mail, web, user and SaaS security that actually works together. No patchwork, no platform fatigue.