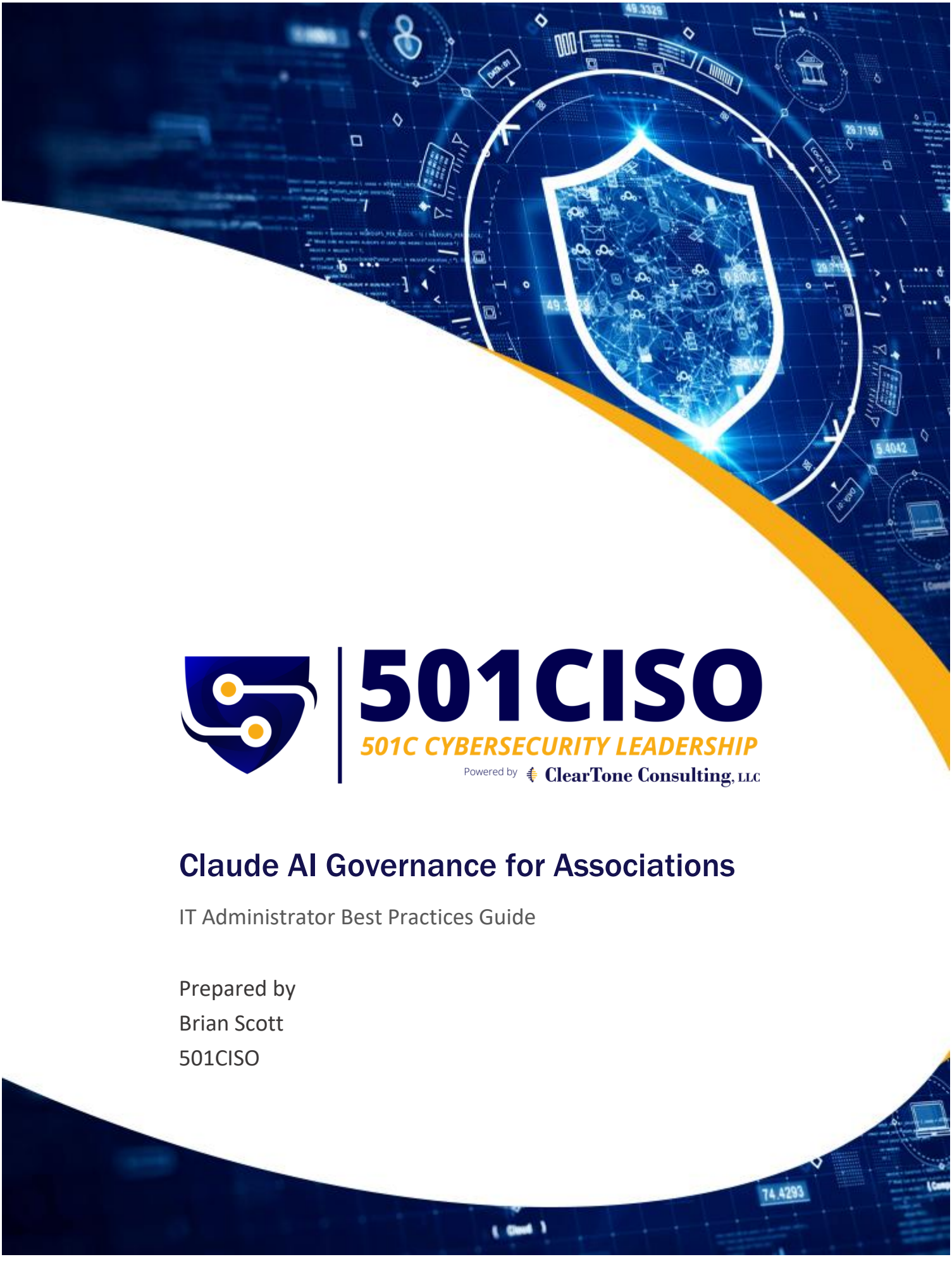

501CISO

501C CYBERSECURITY LEADERSHIP

Powered by ClearTone Consulting, LLC

Claude AI Governance for Associations

IT Administrator Best Practices Guide

Prepared by
Brian Scott
501CISO

ABOUT THIS GUIDE

This guide is designed for IT administrators and MSP technicians responsible for deploying and governing Claude AI at association organizations. It covers everything from initial account setup through ongoing security monitoring.

All guidance is calibrated for Claude Team plan (the standard choice for most associations) and is layered by M365 licensing tier so you can implement exactly what your licensing supports. Enterprise plan differences are noted where they unlock meaningfully stronger controls.

Section	What It Covers	Primary Audience
1 · Plan & Licensing	Plan tier differences, what each M365 license unlocks	IT Lead / MSP
2 · Initial Setup	Step-by-step Claude admin console configuration	MSP Technician
3 · Connector Governance	Connector catalog lockdown, per-action permissions	IT Admin
4 · Shadow AI Controls	Entra Conditional Access, SWG header injection	Security / MSP
5 · Visibility & Audit	Usage reporting, Compliance API, SIEM integration	IT Admin
6 · Entra ID Configuration	Conditional Access policies step-by-step	MSP Technician
7 · Ongoing Operations	Quarterly review checklist, incident response	IT Admin
8 · Acceptable Use Policy	Staff-facing policy template	IT / HR

CAUTION This guide reflects Claude product capabilities as of May 2026. Claude's admin controls evolve rapidly — verify current functionality at docs.anthropic.com before implementation.

SECTION 1: PLAN SELECTION & LICENSING TIERS

1.1 Claude Plan Tiers — What Admins Actually Get

Most associations will run Claude Team plan. The table below compares governance capabilities across Claude plans so you can assess whether your current plan provides adequate control — and where gaps exist.

Governance Capability	Free / Pro (Personal)	Team	Enterprise
Admin console	❌ None	☑ Owner controls	☑ Full admin console
Enable/disable connectors org-wide	❌	☑	☑
Per-action restrictions (read vs. write)	❌	☑	☑
Usage dashboard	❌	☑ Basic	☑ Full + API
Domain verification (block new personal accts)	❌	☑	☑
SSO / SAML 2.0 enforcement	❌	❌	☑
Domain capture (lock corp email to workspace)	❌	❌	☑
SCIM auto-provisioning / deprovisioning	❌	❌	☑
RBAC group-based connector scoping	❌	❌	⚠ Beta
Compliance API (programmatic audit log)	❌	☑ Basic	☑ Full

Governance Capability	Free / Pro (Personal)	Team	Enterprise
OpenTelemetry / SIEM integration	✗	☑	☑
Private inference (Bedrock / Vertex / Azure)	✗	✗	☑
Cowork MDM-managed deployment	✗	✗	☑

CRITICAL

Team plan has no SSO enforcement and no domain capture. A staff member with a personal Claude account on their corporate email address cannot be forced to use the organizational workspace on Team plan. This is the primary reason security-conscious organizations upgrade to Enterprise. See Section 4 for mitigation options.

1.2 M365 License Tier — What It Unlocks for Claude Governance

Claude's own admin controls are the same regardless of your M365 license. However, the M365 license tier determines which Entra ID, Purview, and Defender controls you can layer on top of Claude. The table below maps key security features to licensing tiers.

Security Control	Biz Basic/ Std	Business Premium	M365 E3	M365 E5
Entra ID Conditional Access (basic)	⚠ P1 add-on	☑ Included	☑ Included	☑ Included
Entra ID P2 (risk-based CA, Identity Protection)	✗	✗	✗	☑ Included
Microsoft Purview DLP (basic)	✗	⚠ Limited	⚠ Limited	☑ Full

Security Control	Biz Basic/ Std	Business Premium	M365 E3	M365 E5
Microsoft Purview Communication Compliance	✗	✗	✗	☑ Included
Defender for Cloud Apps (CASB)	✗	☑ Included	✗	☑ Included
Intune MDM (device compliance policies)	✗	☑ Included	⚠ Basic	☑ Full
Entra ID SCIM provisioning to 3rd-party apps	⚠ Limited	☑	☑	☑
Audit log retention (Purview)	90 days	90 days	180 days	365 days
Microsoft Sentinel (SIEM)	✗	✗	⚠ Add-on	⚠ Add-on

NOTE

Business Premium is the most common tier across associations and is the minimum recommended for Claude governance. It includes Conditional Access, Defender for Cloud Apps (CASB), and Intune — the three controls that matter most for governing Claude. Organizations on Business Basic or Standard should plan to add Entra ID P1 as a standalone add-on ($6/user/month) at minimum.

SECTION 2: INITIAL CLAUDE ADMIN SETUP

Complete these steps in order when standing up Claude Team for your organization. This section is written for the MSP technician performing the initial deployment.

2.1 Pre-Deployment Checklist

Before enabling Claude for staff, complete all items in this checklist:

#	Pre-Deployment Task	Why It Matters
1	Identify the Claude Account Owner (typically the IT lead or a dedicated admin email address — not a personal account)	The Owner has full admin rights; losing access to this account locks you out
2	Confirm all staff will use their organizational email address (@yourorg.org) for Claude accounts	Required for domain verification to function
3	Inventory which SaaS connectors staff want to use (M365, Salesforce, AMS, etc.)	Allows you to build an approved connector allowlist before users start self-connecting
4	Review connector permissions available for each approved system (read vs. write actions)	Sets the basis for per-action restrictions configured in Step 2.4
5	Draft an Acceptable Use Policy (see Section 8 template)	Publish before first staff access — establishes expectations and legal coverage
6	Notify staff that organizational Claude accounts are being deployed and personal accounts should not be used for work tasks	Reduces shadow AI risk from day one

2.2 Admin Console Configuration — Step by Step

Step 1: Claim Your Organization and Verify Your Domain

- Log in to claude.ai with the designated Owner account
- Navigate to Organization Settings > Organization and Access
- Enter your organization name and primary email domain (e.g., yourorg.org)
- Complete DNS TXT record verification as prompted — this requires access to your DNS provider (typically your hosting provider or M365 DNS zone)
- Once verified, domain verification will block new personal Claude accounts from being created using your org's email domain

CAUTION	Domain verification only blocks NEW account creation. It does not affect personal accounts that already exist. To identify existing personal accounts on your domain, use the Domain Memberships report under Organization Settings after verification is complete.

Step 2: Provision Staff Accounts

- Navigate to Organization Settings > Members
- Invite staff by sending invitations to their organizational email addresses
- Assign roles: Owner (IT admin only), Admin (team leads if needed), Member (all staff)
- **Only 1–2 Owner accounts.** Owners have full connector admin rights and can make irreversible changes such as domain capture if you later upgrade to Enterprise.
- For departing staff: remove members manually from Organization Settings > Members. On Team plan there is no SCIM auto-deprovisioning — this must be a manual offboarding step tied to your HR process.

Step 3: Lock Down the Connector Catalog (Critical — Do This Before Staff Access)

- **Navigate to Organization Settings > Connectors**
- Enable the organizational connector restriction toggle. This shifts the catalog from open self-service (any user can add any connector) to managed mode (only admin-approved connectors are visible).
- **This toggle does not retroactively remove already-enabled connectors.** Review and remove all default-enabled connectors before granting staff access.

- Remove every default-enabled connector from the list
- Add back only connectors that are on your approved list (see Section 3)

CRITICAL	The connector catalog is OPEN by default. If you provision staff accounts before enabling the restriction toggle, users can connect any of the 50+ available connectors — including ones that read email, browse files, and post to project tools — without any IT approval. Enable the restriction toggle first, before any staff accounts are invited.

Step 4: Configure Per-Action Permissions for Each Approved Connector

For each connector you enable, configure the action permissions. The three permission states are:

Permission State	Behavior	Recommended Default
Always Allow	Claude can invoke this action automatically when relevant	Use for read/search actions on low-sensitivity systems
Needs Approval	Claude pauses and requests explicit user confirmation before acting	Use for write actions and any action that modifies records
Blocked	Claude cannot invoke this action regardless of user request	Use for delete, send, and admin actions on all systems

Recommended baseline permission settings by connector:

Connector	Recommended Allowed Actions	Set to Needs Approval	Block Entirely
Microsoft 365 (SharePoint / OneDrive)	Read files, search content	Edit, create new files	Delete, share permissions

Connector	Recommended Allowed Actions	Set to Needs Approval	Block Entirely
Microsoft 365 (Outlook)	Read / search email, summarize	None	Send email, create rules, delete
Microsoft 365 (Teams)	Read messages, search	None	Post messages, create channels
Salesforce / CRM	Read contacts, opportunities, account history	Create/update records	Delete records, change ownership
AMS (iMIS, Fonteva, etc.)	Read member records, event registrations	None — block writes entirely	All write/delete/admin actions
Asana / project tools	Read tasks, view status	Create tasks	Delete, reassign, close projects

TIP

For AMS systems that manage member PII (addresses, dues history, certifications), the default posture should be read-only with all write actions blocked. The risk of an AI-assisted workflow inadvertently modifying member records is not worth the productivity gain from write access.

Step 5: Enable Audit Logging and Verify Usage Dashboard Access

- Navigate to Organization Settings > Usage to confirm the usage dashboard is active
- Confirm that the Compliance API is accessible — this is available on Team plan for basic logging
- If using SIEM: configure the OpenTelemetry event stream (see Section 5 for full setup)
- Set a calendar reminder to review the usage dashboard monthly

SECTION 3: CONNECTOR GOVERNANCE

3.1 The Two-Layer Connector Model

All Claude connector access operates through two sequential gates. Understanding this model is essential for communicating Claude's data access scope to leadership and staff.

Layer	Controlled By	What It Does
Layer 1 — Org Enablement	IT Admin / Owner	Makes a connector available to the organization. Until enabled by an admin, no user can access the connector in the managed workspace.
Layer 2 — User Authentication	Individual Staff Member	Each user personally authenticates to the third-party service using their own credentials. Claude inherits only that user's existing permissions — it cannot access data the user cannot already access.

NOTE

This model narrows access — it never expands it. Claude cannot access SharePoint sites a user cannot access, records in Salesforce outside a user's permission set, or AMS data outside a user's role. The connector model is additive to — not a replacement for — your existing data permissions.

3.2 M365 Connector — Special Configuration Requirements

The Microsoft 365 connector requires additional setup beyond the Claude admin console and is available only on Team and Enterprise plans.

Requirement	Detail
Entra ID Global Administrator	A one-time consent grant from a Global Admin is required before individual users can authenticate to the M365 connector. This grants the Claude app access to read M365 data on behalf of authenticated users.
App Registration Review	After the admin consent is granted, verify the app permissions in Entra ID > Enterprise Applications > Claude. Confirm the granted permissions align with your approved connector actions.
Conditional Access Scope	Consider whether your Conditional Access policies should explicitly include the Claude Enterprise Application to enforce MFA and device compliance on Claude's M365 access (see Section 6).
SharePoint Permission Audit	Before enabling the M365 connector, audit SharePoint site permissions. Claude respects existing permissions, but overly broad SharePoint sharing means Claude can surface content users technically have access to but never expected to find easily.

3.3 AMS Connector Governance

Most AMS platforms (iMIS, Fonteva, Nimble AMS, Personify) do not have a native Claude connector in the connector directory. Organizations integrating Claude with their AMS typically do so via one of three methods:

- **Custom MCP Server:** A custom MCP server is built to expose specific AMS data (member records, event registrations, certification history) as read-only context for Claude. This requires development work and must be approved and security-reviewed by IT before deployment.
- **Manual data export + upload:** Staff export a CSV or report from the AMS and upload it directly to Claude for analysis. No persistent connector — data is session-scoped only.
- **Bedrock Agents (Enterprise path):** For organizations on Claude Enterprise, AWS Bedrock Agents can connect to AMS APIs via AWS native connectors.

CRITICAL Custom MCP servers for AMS systems must be internet-reachable from Anthropic's cloud infrastructure. An AMS on your private network cannot be

connected without allowlisting Anthropic's IP ranges at your firewall. Engage your AMS vendor and IT team before attempting this integration. Never expose AMS admin accounts through a custom MCP connector — use a dedicated read-only service account with the minimum required permissions.

3.4 Connector Governance Maintenance

Connectors are not set-and-forget. Ongoing governance requires:

Task	Frequency	Who
Review active connector list in Organization Settings > Connectors	Quarterly	IT Admin
Review per-action permissions for each active connector	Quarterly	IT Admin
Audit new connector additions or changes requested by staff	As requested	IT Admin
Review Entra ID Enterprise Applications for Claude app permissions	Semi-annually	IT Admin / MSP
Remove connectors for staff who have left the organization	Upon offboarding	IT Admin
Security review of any new custom MCP servers	Before production deployment	IT Admin + Vendor

SECTION 4: SHADOW AI CONTROLS

Shadow AI refers to staff using personal Free, Pro, or Max Claude accounts for work tasks outside of IT visibility and control. This is a real risk: any staff member who was using Claude personally before your org adopted it — or who simply prefers their personal account — can connect their organizational Google Drive, Outlook, or Salesforce credentials to a personal Claude account, completely bypassing your admin controls.

4.1 Risk Scenarios and Available Controls

Risk Scenario	Team Plan	Enterprise Plan	Network / Endpoint Layer
New personal accounts on org email domain	☑ Blocked by domain verification	☑ Blocked	N/A
Existing personal accounts on org email domain	❌ Cannot affect	☑ Domain capture + SSO	⚠️ Partial via Conditional Access
Personal accounts on non-org email (Gmail, Yahoo, etc.)	❌ No control	❌ No control	☑ SWG header injection
Personal accounts on unmanaged personal devices	❌ No control	❌ No control	⚠️ Policy only — no technical control
claude.ai access on non-compliant managed devices	❌ No control	❌ No control	☑ Intune / MDM + CA policy
Sensitive data uploaded to personal Claude session	❌ No control	❌ No control	☑ Defender for Cloud Apps DLP

NOTE	No combination of Claude plan and M365 controls can prevent a staff member from accessing claude.ai on a personal device on a personal network with a personal account. Policy, training, and employment agreements are the only available controls for that scenario. Focus technical controls on managed devices and managed networks, and use policy for everything else.

4.2 Immediate Actions — Team Plan (All M365 Tiers)

1. Enable domain verification in Organization Settings to block new personal accounts on your domain
2. Run the Domain Memberships report to identify existing personal accounts on your domain
3. Contact staff with existing personal accounts and request they migrate to the organizational workspace
4. Publish an Acceptable Use Policy that explicitly prohibits use of personal Claude accounts for work tasks
5. **Communicate clearly:** most staff using personal accounts are not doing so maliciously — they simply started using Claude before IT deployed it. A clear, non-punitive communication resolves most cases.

4.3 Conditional Access Policy for Claude (M365 Business Premium, E3, E5)

Conditional Access can restrict access to claude.ai on managed devices to compliant-only sessions. This does not prevent access to personal Claude accounts, but it ensures that staff accessing Claude on a managed device are doing so through a compliant configuration.

Full Conditional Access setup steps are in Section 6.

4.4 SWG Tenant Restriction Header Injection (Most Effective Shadow AI Control)

The most effective technical control for shadow AI is Secure Web Gateway (SWG) header injection. Supported SWG and CASB vendors can inject an HTTP header into all outbound traffic to claude.ai. Anthropic's infrastructure reads this header and blocks

any Claude session that is not authenticated to your approved organizational workspace.

This means: a staff member on a corporate device attempting to use a personal Free/Pro account on claude.ai will see an IT administrator block message, regardless of which email address they used to register that account.

Vendor / Approach	M365 License Required	What It Blocks
Defender for Cloud Apps (CASB) — Microsoft native	Business Premium or E5	Content DLP inspection; session policy enforcement; can block uploads to personal Claude sessions
Zscaler Internet Access	Any (3rd party)	Full tenant restriction header injection; blocks all non-org Claude sessions on managed devices/networks
Netskope	Any (3rd party)	Full tenant restriction header injection + content DLP
dope.security	Any (3rd party)	Tenant restriction header injection; lightweight option for smaller orgs
DNS / Firewall block of claude.ai	Any	Blocks all Claude access on managed network — use only if combined with allowlist for managed devices

TIP

For Business Premium organizations: Defender for Cloud Apps is already included in your license and should be the first control deployed. It provides content DLP inspection for claude.ai uploads (including member PII and financial data detection) without requiring a third-party SWG vendor. See Section 6 for Defender for Cloud Apps configuration steps.

SECTION 5: VISIBILITY & AUDIT

Equal-weight governance means visibility into what staff are doing is as important as controlling what they can do. This section covers all available reporting and logging capabilities by licensing tier.

5.1 Claude Native Usage Dashboard

Available on Team and Enterprise plans at Organization Settings > Usage. Provides:

- Total messages sent by the organization per day / week / month
- Per-user message volume (identify power users and unusual activity)
- Connector usage — which connectors are being invoked and by whom
- Model usage breakdown (Opus / Sonnet / Haiku)

Limitations of the native dashboard:

- Does not show the content of conversations
- Does not provide alerting or anomaly detection
- Retention period is limited — export regularly if you need historical trend data
- Does not track connector actions (read vs. write invocations) separately

5.2 Compliance API

Available on Team plan (basic) and Enterprise plan (full). The Compliance API provides programmatic access to usage data for integration with external audit systems.

Capability	Team Plan	Enterprise Plan
Message volume and per-user counts	☑	☑
Connector invocation logs	☑	☑
Conversation metadata (timestamp, model, token count)	☑	☑

Capability	Team Plan	Enterprise Plan
Conversation content access	❌	☑
Real-time event streaming	❌	☑
Cowork tool call logs	☑ Basic	☑ Full (OpenTelemetry)

5.3 OpenTelemetry / SIEM Integration

Claude (Team and Enterprise) emits OpenTelemetry events for connector calls and Cowork tool invocations. These events can be piped into your SIEM for correlation and alerting.

SIEM Platform	Integration Method	M365 License Notes
Microsoft Sentinel	OpenTelemetry connector + custom data connector (Log Analytics workspace)	E3/E5 — Sentinel is an add-on at all tiers; included workspace logs available at no extra charge
Splunk	OpenTelemetry HTTP Event Collector (HEC)	Any — Splunk is third-party; no M365 license dependency
Cribl Stream	OpenTelemetry pipeline — Anthropic-documented integration	Any — acts as pipeline between Claude events and any downstream SIEM
Microsoft Defender XDR	Not a native integration — Claude events must be routed via Sentinel or Splunk first	E5 only

NOTE For most associations on Business Premium without Sentinel, the recommended starting point is: (1) export Claude usage data via the Compliance API weekly into a SharePoint list or Excel file for manual review,

and (2) configure Defender for Cloud Apps activity policies to alert on anomalous claude.ai usage (bulk file access, unusual upload volume). Full SIEM integration is a more advanced step for organizations with dedicated IT resources.

5.4 Defender for Cloud Apps — Claude Activity Monitoring

For Business Premium and E5 organizations, Defender for Cloud Apps (MCAS) provides the most practical visibility layer. Once claude.ai is configured as a monitored app:

- Activity logs show all authenticated sessions to claude.ai from managed devices
- Upload volume monitoring flags unusual bulk uploads (potential data exfiltration)
- Session policies can block download / upload of files containing sensitive data patterns (member PII, financial data)
- Alerts can be configured for access from non-compliant devices or outside normal hours

5.5 Monthly Review Checklist — Visibility Tasks

Task	Where	Flag If...
Review per-user message volume	Claude Usage Dashboard	Any user with dramatically higher volume than peers
Review connector invocation logs	Claude Compliance API / Dashboard	Unexpected connectors appearing, or write actions being invoked
Review Defender for Cloud Apps alerts for claude.ai	Defender portal > Alerts	Any DLP policy match, access from unknown device, bulk upload
Check for new personal account activity	Claude Domain Memberships report	Any accounts on org domain not in the managed workspace
Review member offboarding — Claude access revoked	Claude org member list vs. HR offboarding list	Any former staff still listed as members

SECTION 6: ENTRA ID & M365 SECURITY CONFIGURATION

This section provides step-by-step configuration guidance for Entra ID Conditional Access and Defender for Cloud Apps as they apply to Claude governance. Steps are marked by the license tier required.

6.1 Register Claude as an Enterprise Application in Entra ID

Before you can apply Conditional Access to claude.ai, you need the app represented in your Entra ID tenant. There are two paths:

Path A — M365 Connector Admin Consent (Required for M365 Connector)

6. Sign in to the Azure portal (portal.azure.com) with a Global Administrator account
7. Navigate to Entra ID > Enterprise Applications > New Application
8. Search for 'Claude' — if listed in the gallery, add it. If not, proceed with the OAuth consent flow triggered when an admin first connects the M365 connector in the Claude admin console
9. After consent is granted, navigate to Entra ID > Enterprise Applications > Claude (or Anthropic)
10. Review the Permissions tab — confirm only the permissions required for the approved connector actions are present
11. Under Properties, confirm 'User assignment required' is set to Yes — this restricts which users can authenticate to Claude via M365 SSO

Path B — Named App in Conditional Access (For Session and Device Controls)

12. In Entra ID, navigate to Protection > Conditional Access > Named Locations
13. Claude may need to be targeted by URL (claude.ai) in a Conditional Access policy if it is not automatically detected as a Cloud App. Use the 'All cloud apps' scope in CA policies and exclude any apps you do not want included

NOTE	As of May 2026, claude.ai may not appear as a named cloud app in the Entra CA gallery. Contact your MSP to confirm current status. If not listed, target using Defender for Cloud Apps session policy on the URL instead.

6.2 Conditional Access Policy — Require MFA for Claude Access

License Requirement: Business Premium, E3, or E5 (Entra ID P1 required)

14. Navigate to Entra ID > Protection > Conditional Access > New Policy
15. **Name:** Require MFA for Claude AI
16. **Assignments > Users:** All users (or a specific group if rolling out gradually)
17. **Target Resources:** Cloud apps — select Claude if listed, or use 'All cloud apps' with exclusions
18. **Conditions:** Leave default (applies to all platforms and locations)
19. **Access Controls > Grant:** Require multi-factor authentication
20. Set policy to Report-only first to assess impact, then enable after 2 weeks

TIP	If you have an existing MFA Conditional Access policy covering 'All cloud apps', Claude is already covered. Verify by checking the Sign-in logs in Entra ID for claude.ai sessions and confirming MFA is recorded.

6.3 Conditional Access Policy — Require Compliant Device for Claude Access

License Requirement: Business Premium or E5 (requires Intune MDM enrollment)

21. Ensure all staff devices are Intune-enrolled and compliance policies are configured
22. Navigate to Entra ID > Conditional Access > New Policy
23. **Name:** Require Compliant Device for Claude AI
24. **Assignments > Users:** All users
25. **Target Resources:** Cloud apps — Claude or All cloud apps
26. **Access Controls > Grant:** Require device to be marked as compliant (Intune)
27. Enable in Report-only mode initially — non-enrolled personal devices will show as non-compliant, giving you visibility before enforcement

CAUTION	Enforcing device compliance for Claude blocks personal devices from accessing claude.ai unless they are Intune-enrolled. For staff who use personal devices for work, this may be disruptive. Communicate clearly before enabling enforcement mode. Consider a grace period with a 'Bring Your Own Device' enrollment path if needed.

6.4 Conditional Access Policy — Block Non-Compliant Claude Sessions (Advanced)

License Requirement: Business Premium or E5 (requires Defender for Cloud Apps)

This policy routes claude.ai sessions through Defender for Cloud Apps for real-time inspection, enabling content DLP, session controls, and anomaly alerts.

28. In Defender for Cloud Apps portal (security.microsoft.com > Cloud Apps), navigate to Settings > Connected Apps > Conditional Access App Control
29. Add claude.ai as a monitored app (or 'Any app' with URL = claude.ai if not listed)
30. In Entra ID Conditional Access, create a new policy targeting Claude
31. **Session Controls:** Use Conditional Access App Control > Use custom policy (Defender for Cloud Apps)
32. In Defender for Cloud Apps, create a Session Policy:
    - Activity type: File upload
    - Filter: Sensitive information type — configure patterns for Member PII (names + addresses), financial account numbers
    - Action: Block upload and alert admin
33. Test with a synthetic file containing obviously fake PII before enabling in production

6.5 Entra ID Sign-In Risk Policy (E5 Only — Entra ID P2)

License Requirement: M365 E5 or Entra ID P2 add-on

For E5 organizations, Identity Protection can automatically require step-up authentication or block Claude access when Entra detects anomalous sign-in risk (impossible travel, leaked credentials, etc.).

34. Navigate to Entra ID > Protection > Identity Protection > Sign-in risk policy
35. Set sign-in risk level: Medium and above
36. Target: All users or a Claude-specific group
37. Access control: Require multi-factor authentication
38. This policy applies globally — it does not require Claude-specific configuration — but ensure it is active

6.6 Entra ID SCIM Provisioning to Claude (Enterprise Plan Only)

SCIM auto-deprovisioning is only available on Claude Enterprise plan. On Team plan, user lifecycle management must be handled manually. Build the following into your HR offboarding process:

Offboarding Step	Who Does It	Timing
Disable Entra ID / M365 account	IT / MSP	Day of departure
Revoke MFA devices in Entra ID	IT / MSP	Day of departure
Remove user from Claude organizational workspace	IT Admin in Claude admin console	Day of departure
Review and revoke any personal connector authentications associated with the user	IT Admin	Within 1 week — user's OAuth tokens in connected systems should be revoked
Archive or transfer any Claude projects owned by departing user	Manager / IT	Within 2 weeks

SECTION 7: ONGOING OPERATIONS & INCIDENT RESPONSE

7.1 Quarterly Governance Review

Assign a named owner for Claude governance (typically the IT lead or MSP account manager). Complete the following quarterly:

Review Area	Tasks	Escalate If...
Connector Inventory	Review all enabled connectors; remove unused; verify per-action permissions	Any connector enabled that is not on the approved list
User Access	Reconcile Claude member list against current staff roster; remove departed staff	Any accounts for users who have left the organization
Personal Account Audit	Re-run Domain Memberships report; follow up with any new personal accounts found on org domain	Staff with known work-related usage on personal accounts
Usage Anomalies	Review per-user message volumes; investigate outliers	Any user with >5x average usage, or bulk connector invocations in a short period
Connector Permission Changes	Review any per-action permission changes since last review	Any escalation of write/delete permissions that was not formally approved
M365 App Permissions	Review Claude app in Entra ID Enterprise Applications; confirm permissions unchanged	Any permission scope additions that were not intentionally granted

7.2 AI Incident Classification and Response

Define what constitutes a Claude-related security incident so your team knows when to escalate. The following are the most likely incident types for association organizations:

Incident Type	Example	Immediate Response
Unauthorized data access via connector	Staff member connected an AMS or Salesforce connector on a personal account and accessed member PII	1. Remove user from org workspace or disable personal account access. 2. Audit connector invocation logs. 3. Notify members if PII was accessed outside organizational controls per your privacy policy.
Prompt injection via document	Staff asked Claude to summarize a document that contained embedded instructions causing unexpected actions	1. Review what actions were taken. 2. Revoke any connector tokens that may have been used. 3. Report to Anthropic if data was exfiltrated.
Sensitive data uploaded to personal Claude session	DLP alert fires for member PII upload to claude.ai from a personal account session	1. Block session via Defender for Cloud Apps if active. 2. Speak with staff member. 3. Assess whether data was retained — check Anthropic's data handling terms for personal plan.
Credential exposed in Claude conversation	Staff pasted an API key or password into Claude chat	1. Rotate the exposed credential immediately. 2. Review what systems the credential accessed. 3. Add DLP rule to detect credential patterns in future sessions.
Unauthorized agent/workflow action	Cowork or an agentic Claude session took a write action the user did not intend	1. Review action logs in Cowork / connector audit log. 2. Reverse any unintended changes in the target system. 3. Tighten per-action permissions for the affected connector.

7.3 New Staff Onboarding — Claude-Specific Steps

- Add to Claude organizational workspace at time of M365 account provisioning
- Include Claude Acceptable Use Policy in new hire documentation (see Section 8)
- Communicate approved connectors and how to connect them
- Confirm staff are not migrating from a personal Claude account — if they are, coordinate with IT to transition projects and history
- Include Claude governance in security awareness training

SECTION 8: ACCEPTABLE USE POLICY TEMPLATE

The following is a template Acceptable Use Policy for Claude AI. Customize with your organization's name, IT contact, and any specific restrictions relevant to your operations. This template is designed to be accessible to non-technical staff.

[ORGANIZATION NAME]

Acceptable Use Policy: Claude AI

Purpose

[Organization Name] provides access to Claude AI to help staff work more efficiently. This policy defines how Claude may be used and what data may be shared with it.

Approved Use

Staff may use Claude for:

- Drafting, editing, and summarizing documents and communications
- Researching topics relevant to your role
- Analyzing data from approved organizational systems via approved connectors
- Automating repetitive tasks in approved systems

Prohibited Use

Staff may NOT:

- Use personal Claude accounts (Free, Pro, or Max) for any work task involving organizational data
- Upload, paste, or share member personal information (names, addresses, dues history, certification records) into any AI platform not approved by IT
- Share passwords, API keys, or system credentials in Claude conversations
- Connect Claude to any SaaS system not on the IT-approved connector list
- Treat Claude outputs as factual or legally reliable without human review

Your Organizational Account

You must use your [Organization Name] email address to access Claude. Your organizational Claude account is monitored for usage volume and connector

activity by IT. Conversation content is not routinely reviewed, but may be accessed in the course of a security investigation in accordance with our IT policies.

AI Outputs Are Not Authoritative

Claude can produce confident-sounding but incorrect information. Any Claude output used in official communications, member-facing content, legal documents, or financial reports must be reviewed and verified by a qualified staff member before use.

Questions or Incidents

Contact [IT Contact / MSP Name] at [email/phone] for questions about approved connectors, to report unexpected Claude behavior, or if you believe organizational data may have been inadvertently shared in a personal Claude session.

By using Claude through your organizational account, you agree to this policy.

APPENDIX A: MSP DEPLOYMENT QUICK REFERENCE

Use this checklist for new Claude Team plan deployments. Each item maps to a section in this guide for full detail.

#	Task	Section	Done
1	Identify Owner account; do NOT use a personal email	2.1	☐
2	Staff using org email addresses for all accounts	2.1	☐
3	Domain verified via DNS TXT record	2.2 Step 1	☐
4	Domain Memberships report run; personal accounts identified and addressed	2.2 Step 1	☐
5	Connector restriction toggle ENABLED before any staff access	2.2 Step 3	☐
6	All default connectors removed from the catalog	2.2 Step 3	☐
7	Approved connectors added back with per-action permissions configured	2.2 Step 4	☐
8	M365 connector admin consent granted by Global Admin (if M365 connector approved)	3.2	☐
9	SharePoint permission audit completed before M365 connector enabled	3.2	☐
10	Entra ID CA policy: Require MFA for Claude (Business Premium / E3 / E5)	6.2	☐
11	Entra ID CA policy: Require compliant device for Claude (Business Premium / E5)	6.3	☐

#	Task	Section	Done
12	Defender for Cloud Apps: claude.ai added as monitored app (Business Premium / E5)	6.4	☐
13	Usage dashboard reviewed; monthly review calendar reminder set	5.1	☐
14	Acceptable Use Policy published and distributed to all staff	Section 8	☐
15	Offboarding process updated to include Claude account removal	6.6	☐
16	Quarterly governance review scheduled	7.1	☐

APPENDIX B: FEATURE AVAILABILITY SUMMARY

Goal	Minimum Requirement	Notes
Connector governance (enable/disable, per-action)	Claude Team plan	No M365 license dependency
Block new personal accounts on org domain	Claude Team plan + domain verification	Does not affect existing accounts
Require MFA for Claude access	Entra ID P1 (Business Premium / E3 / E5)	Business Basic: purchase P1 add-on (~$6/user/mo)
Require compliant device for Claude access	Business Premium or E5 + Intune enrollment	Requires devices to be Intune-managed
Content DLP on Claude uploads (member PII detection)	Business Premium or E5 (Defender for Cloud Apps)	Most cost-effective option for most associations
Full shadow AI blocking via SWG header injection	Third-party SWG (Zscaler, Netskope) OR Business Premium CASB	CASB provides partial control; full header injection needs SWG vendor
Auto-deprovisioning when staff leave	Claude Enterprise plan + SCIM	Team plan requires manual offboarding
SSO enforcement / domain capture	Claude Enterprise plan	Team plan has no SSO enforcement
Conversation content access for investigations	Claude Enterprise plan (Compliance API full)	Team plan provides metadata only

This guide reflects Claude and M365 capabilities as of May 2026. Both platforms evolve rapidly — verify current feature availability with Anthropic (docs.anthropic.com) and Microsoft (learn.microsoft.com)