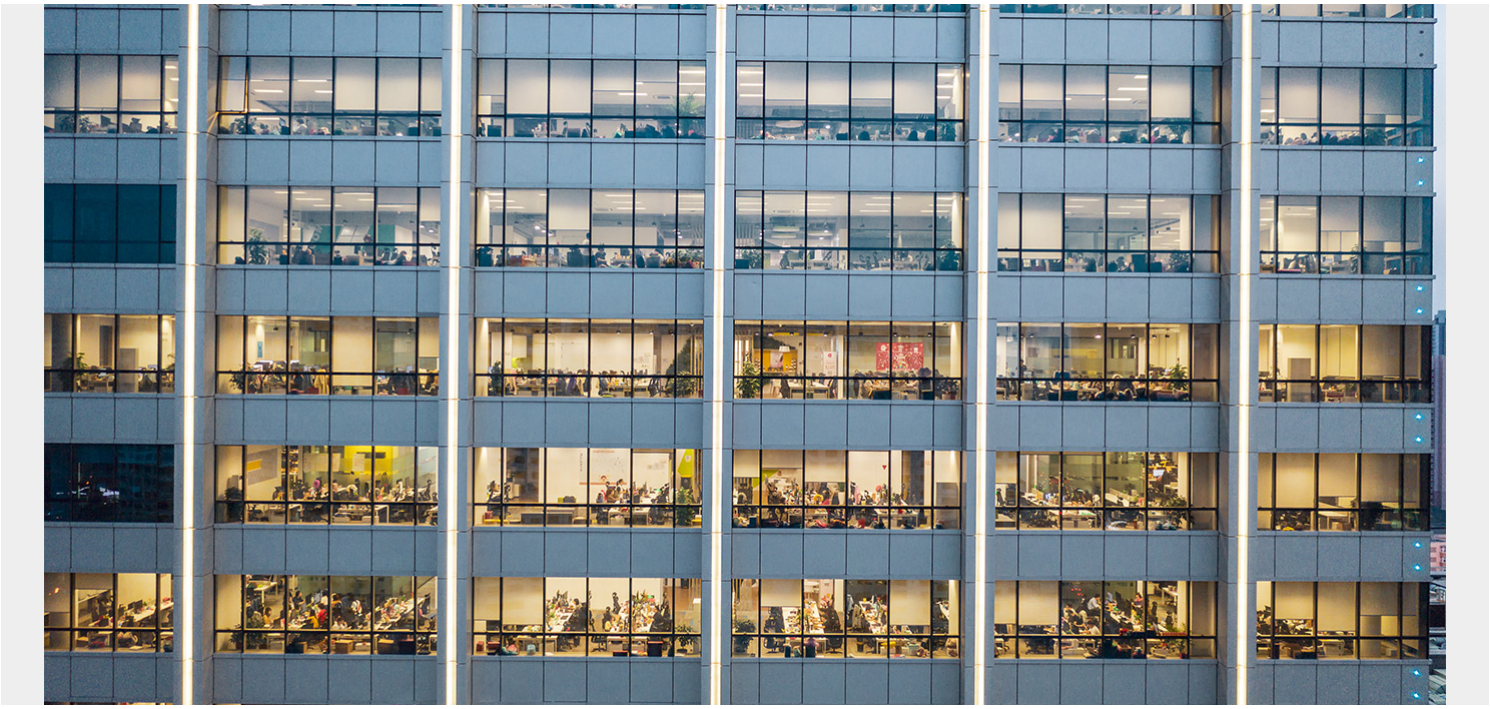
AUTONOMOUS DATA AND APPLICATION WORKFLOW ORCHESTRATION



Autonomous workflow orchestration lets IT teams manage their own data pipelines and application workflows without depending on a central administrator for every configuration change. Control-M from BMC delivers this autonomy through role-based administration and centralized connection profiles—empowering data engineers, application developers, and file transfer teams to work independently while maintaining controlled access across the organization.

New IT roles and responsibilities

IT roles have expanded significantly. Digital acceleration and multi-cloud adoption have brought IT closer to the business, transforming professionals into architects, data engineers, data scientists, DevOps engineers, and governance advisors.

As Gartner (2021) noted, each IT role now faces specific challenges—from supporting digital acceleration to integrating more strategically with the broader business.

The result is a workforce operating across a wider range of technologies and business functions than original role descriptions ever anticipated—doing substantially more, often with the same team size.

Why do enablement and empowerment strategies matter?

The more IT teams can autonomously access and leverage tools and technologies, the more effective they become at driving business value. Enablement and empowerment strategies also

compound over time: when more users can exploit capabilities beyond their traditional expertise, organizations accelerate both innovation and execution.

This shift reflects the broader democratization of technology—where capabilities that once required deep technical expertise are now accessible across roles. Self-service culture reinforces this expectation, as users throughout the organization increasingly expect autonomous access to the tools they need.

How does Control-M support autonomous workflow orchestration?

Control-M — BMC's leading platform for autonomous workflow orchestration — has evolved to support enablement, empowerment, and self-service across data, cloud, and AppDev teams.

Today, business users, data teams, cloud teams, and AppDev teams all benefit from autonomous access to workflow orchestration. Data engineers use Control-M to integrate, automate, and orchestrate data pipelines—from ingestion through analytics—to produce reliable, actionable insights. Application developers integrate Control-M via Jobs-as-Code in their CI/CD toolchains, delivering high-quality applications to production while meeting governance, risk, and compliance requirements.

Two key features drive this autonomous model: role-based administration and centralized connection profiles.

> *"… role-based administration and Automation API will provide more freedom for customers to manage their connection (e.g.bank users can update passwords without sharing it with our team)"* – **Johann Vermeulen, IT Operations Analyst, BMW South Africa.**

Role-based administration: how does it enable team autonomy?

Role-based administration gives product teams the ability to manage their own workflow orchestration environments without submitting ticket requests to a central Control-M administrator.

Previously, data engineers who wanted to use Control-M had to rely on a central administrator for setup, configuration, and user management—creating bottlenecks that slowed execution. Role-based administration eliminates this dependency by delegating administrative privileges directly to product teams.

With role-based administration, teams can independently perform tasks including:

- **Deploying Control-M agents and application plug-ins**—prerequisites to integrating data pipeline technologies across all servers
- **Managing connection profiles and user definitions**—prerequisites to securely accessing and running data technologies and applications

As Johann Vermeulen, IT Operations Analyst at BMW South Africa, explains: role-based administration and the Automation API provide customers more freedom to manage their own connections—for example, allowing bank users to update passwords without involving the Control-M team.

How does controlled access prevent conflicts between teams?

Multiple teams—data engineers, file transfer teams, and others—may all use Control-M simultaneously. Each team needs full autonomy over its own environment while being prevented from affecting other teams' configurations.

Control-M administrators address this through tags and authorization granularity. For example, a file transfer team can be granted access only to agents whose names begin with *mft**, specific application plug-ins, and connection profiles prefixed with *connmft**. Teams can also be assigned browse, update, or full authorization levels on their resources.

The result: when a member of the file transfer team logs in to Control-M, they see and manage only their own resources—data engineering environments remain fully separate, and vice versa.

> *"As technology changes are constant, we continue to see that BMC Software is aligning Control-M to meet these fast-paced demands. We are excited to roll out more Application Integrator solutions and utilize role-based administration to empower our internal customers with more control over their batch workflows"* – **A Fortune 500 benefits company.**

Centralized connection profiles: what changes with the latest release?

Prior to Control-M's latest release, connection profiles were bound to individual agents. Users had to create a separate connection profile for each agent where their applications ran—a time-consuming process that scaled poorly as environments grew.

Centralized connection profiles decouple this relationship. A single connection profile now works across all available agents in Control-M.

In practice, the file transfer team can add a new agent to their environment by tagging it with *mft**. The team can immediately begin running tasks on that agent using the connection profile already in place for their existing plug-ins—no additional configuration required.

Conclusion

As Gartner's Top Strategic Technology Trends (2021) observed: organizations accelerating digital business strategy need increasing autonomy and democratization across the business to react quickly rather than be slowed by inefficient processes.

As the landscape evolves toward agentic workflow orchestration, BMC continues to evolve Control-M to support democratization of technology — empowering teams throughout the organization to benefit autonomously from application workflow orchestration. Role-based administration and centralized connection profiles are two concrete steps in that direction.

Click here to learn about the newest Control-M features.

Frequently asked questions

What is autonomous workflow orchestration?

Autonomous workflow orchestration is the ability for individual teams—such as data engineers or application developers—to independently define, schedule, and manage their own workflows without relying on a central IT administrator. Platforms like Control-M enable this through role-based administration and delegated access controls.

How does role-based administration work in Control-M?

Role-based administration in Control-M lets organizations delegate administrative privileges to specific product teams. Each team can manage its own agents, connection profiles, and user definitions within a controlled scope, eliminating central administrator involvement in routine configuration tasks.

What are centralized connection profiles in Control-M?

Centralized connection profiles allow a single connection profile to be shared across all available Control-M agents, rather than requiring a separate profile per agent. This simplifies configuration and allows teams to onboard new agents quickly by tagging them appropriately.

Who benefits from autonomous workflow orchestration?

Data engineers, application developers, file transfer teams, and business users all benefit from autonomous workflow orchestration. Each team gains the ability to manage its own workflows independently, while administrators retain oversight through tag-based access controls and authorization levels.

How does Control-M prevent teams from interfering with each other's environments?

Control-M uses tags and authorization granularity to restrict each team's access to its own defined resources. Administrators configure which agents, plug-ins, and connection profiles each team can access, ensuring teams operate independently without risk of cross-team interference.

The views and opinions expressed in this post are those of the author and do not necessarily reflect the official position of BMC.