Simplify Self-Service Application Workflow Orchestration for your Business

Control-M Role-based Administration & Centralized Connection Profiles

Save Time and Reduce Risk
Introduction

Is it possible to “shift left” without increasing risk? That’s a question a lot of IT professionals are asking as they’re under pressure to satisfy service requests while also delivering new innovation. Two-thirds of IT professionals say the manual work to create workflows is excessive, and 55 percent said workflow management responsibilities divert staff from strategic initiatives.

A common response is to shift service requests left by enabling self service for business users. This philosophy is solid, but execution can be problematic. There is a legitimate concern that any time IT saves by letting users do things themselves will be offset by time spent fixing what they’ve done and containing damage to other systems. Just shifting workflow development and other common service requests to business users isn’t enough – the tasks must also be simplified and error proofed through automation.

So back to the question. Is it possible to “shift left” without increasing risk? Yes. Automation is eliminating the need for IT or business users to take care of many service requests, and is taking so much risk and effort out of others that they can easily be done via self service. Control-M has been at the forefront of automating application workflows. Two new features – Role-based Administration and Centralized Connection Profiles – safely extend automation and self service in valuable new ways so IT can focus on higher-value activities.
What The Experts Say

“IT organizations under pressure to deliver faster are prioritizing self-service capabilities in the coming year. However, widely implemented automation tools have great power that needs to be wielded appropriately to prevent accidental misconfiguration. By having role-based access and views, organizations can right-size control to the automation tool while also promoting greater collaboration between IT and business users.”

Forrester Consulting
Face The Workflow Automation Gap Head On
July 2020 a commissioned study conducted by Forrester Consulting on behalf of BMC Software.
New Tools for Delegating and Error-proofing Workloads

Role-based Administration and Centralized Connection Profiles are new Control-M features that free IT operations from having to handle some of the most repetitive support functions and service requests. They safely give business users and development teams that may not have operations experience or focus the ability to connect Control-M to other applications to run their workloads, and to complete other workload tasks, without exposing critical systems or processes. Role-based Administration and Centralized Connection Profiles complement and enhance the development and self-service support enabled by Control-M Automation API and Application Integrator.

**Role-based Administration**
Control-M Role-based Administration gives developers and product teams full authority to manage their application artifacts without the fear of breaking other teams’ work or submitting service requests to IT. It provides access to new Control-M capabilities using modern API development methods through expanded Automation API functionality.

**Centralized Connection Profiles**
Centralized Connection Profiles simplify creating and maintaining the connection profiles that integrate Control-M with applications. Through automation, they essentially tell Control-M how to talk to applications. Once a connection between an application and Control-M is built, it can be reused repeatedly without having to be developed. Centralized Connection Profiles eliminate manual, time-consuming action when deploying or modifying applications, and speed disaster recovery, data migration and upgrades.
Role-based Administration was created to give users the ability to install, configure and monitor various assets, while providing strong guardrails to ensure enterprise standards are met and systems are not adversely affected. It builds on the powerful authorizations already in Control-M to provide more granular control for working with the assets listed below:

- Control-M agents
- Plug-ins
- Connection profiles
- Control-M web
- Control-M Automation API
- And more

By enabling self service for these activities, IT operations can delegate many common and repetitive service requests while allowing developers and other users to create their own workflows or make changes to existing ones.

For example, security credentials, passwords, client tokens and secrets are frequently embedded in Control-M objects that are normally administered by operations. Maintaining separation of duties has been significantly eased by delegating access to connection information to security teams. Additionally, installing agents and application plug-ins has become a far more common activity in dynamic infrastructure environments like cloud and containers. Granting product teams the ability to install and configure specific agents and plug-ins goes a long way to supporting agile approaches for those groups as they follow a DevOps approach to building and deploying new applications. Self service for agents, plug-ins and other assets is especially valuable as developers accelerate the rate at which short-lived hosts like containers and cloud instances are deployed and decommissioned in support of a CI/CD toolchain.

The Control-M tools used to manage authorization (including a graphical administrative client and Automation API) have been enhanced to fully support managing the new privileges.
Centralized Connection Profiles Overview

Control-M manages business processes that need to connect with other applications and tools. For example, Control-M must connect to a relational database to execute an SQL query, a file transfer server to transfer a file, or to an Informatica environment to execute an Informatica workflow. In all these situations, Control-M needs information about the where that application resides, security credentials to authenticate itself to that application, and other such application-level parameters. This information is stored in a Connection Profile.

In a typical environment, the jobs that perform such tasks (and thus require a Connection Profile) execute on multiple agents, either due to volume requirements, load balancing and high-availability, ownership, or other requirements.

Centralized Connection Profiles provide a mechanism for defining all application characteristics in a single object that can then be accessed by all of the processes running on any agent host, anywhere in the enterprise.

With Centralized Connection Profiles, profiles are defined once and applied to all relevant agents. All profiles are stored centrally in the Control-M database. Any user’s workload that needs a specific connection (for example to automate a file transfer using Control-M Managed File Transfer) gets an up-to-date, centrally maintained instance from the database. Business users can easily find the predefined connectors they need in the database, and administrators can easily keep all instances up to date, without hunting through all the workflows and systems that use them.
Role-based Administration with Automation API will provide more freedom for customers to manage their connection to us. For example, users can update their passwords without sharing them with our team.

Role-based Administration and Centralized Connection Profiles both represent ways to give users more capabilities to create workflows while protecting systems and operations from unintended consequences. They support the spirit of DevOps by giving teams autonomy over their stack to install and configure components, while ensuring administrators keep controls in place. IT ops is still the gatekeeper, but now they can let business users do the heavy lifting of opening the gate to increased automation.

By giving developers and business users proven ways of executing file transfers and interactions with databases, Azure and other cloud resources, plug-ins, agents and more, IT frees itself from many of the high-volume, time-consuming tasks that take it away from more valuable work. Plus, Role-based Administration and Centralized Connection Profiles help extend automation to the cloud and other areas where many development and innovation efforts are happening.

**The Benefits:**
**Giving Users Self Service Frees IT Ops to do More**

"Role-based Administration with Automation API will provide more freedom for customers to manage their connection to us. For example, users can update their passwords without sharing them with our team."

**Johann Vermeulen**
*IT Operations Analyst: ESFT BMW Group South Africa*
The Benefits:

**Automation, Centralization**

**Save Time & Reduce Risk**

The fundamental benefits of automation and centralization are well understood, so here’s a recap of how these benefits relate specifically to Role-based Authorization and Centralized Connection Profiles.

- Role-based Administration allows Control-M administrators to delegate administrative tasks like installing, configuring and monitoring assets and assigning or changing permissions to dev teams and other users, while retaining control over how far they can go. It extends automation to more environments and Control-M capabilities while enabling modern, API-based development methods.

- Centralized Connection Profiles support for Control-M Managed File Transfer alone will save many enterprises a lot of time simply because of the sheer volume of file transfer jobs and associated service requests. Centralized profiles save time for users and IT operations teams alike by making profiles and agents easier to find, deploy and maintain. Centralization also means no connections embedded in workflows get missed if there is an update, which helps keep systems consistent and running smoothly.

- Besides giving business users and developers convenient access to connection profiles that have already been proven, centralized management provides a big boost to business continuity and disaster recovery. When connection profiles are stored and managed centrally, nothing gets missed when they’re updated.

- The web interface improves ease of use and opens up self-service connection profile management to a larger user base, including those with limited operational focus or experience.
What the Experts Say

“Done right, application workflow automation moves the burden of workflow execution from people to software, freeing up IT staff to work on strategic initiatives rather than babysitting technology. Seventy-nine percent of IT leaders believe application workflow automation would have a positive impact on their ability to meet their top IT priorities, and 49% describe the impact as significant.”

Forrester Consulting
Face The Workflow Automation Gap Head On July 2020 a commissioned study conducted by Forrester Consulting on behalf of BMC Software.
Contact BMC today to learn more about how you can take advantage of Role-based Authorization, Centralized Connection Profiles and all the other new features and capabilities available in Control-M 20. The enhancements help you get more out of Control-M and run it even more autonomously, so you can focus on creating and running a more agile, digital business.

Next Steps

Learn more at www.bmc.com/control-m