Omada

Administration

IdentityPROCESS+

An ongoing component of any Identity Security program is to ensure that as business requirements change - as new applications are introduced and new identities are created - that they are continuously secured. As new applications are introduced it is critical to integrate them into Omada so that identity access and provisioning can be automated and managed centrally. Administration processes provide workflows to allow organizations to effectively onboard new business systems and applications. They also provide the ability to tag applications with meaningful descriptions. This enables end users to find the resources they need when making self-service requests and administrators to know what they are granting access to. The Administration processes allow for the efficient onboarding of new business applications into Omada, ensuring that new applications are governed by global policies and making password reset management and password policies easier to enforce.

As part of Omada IdentityPROCESS+, there are several key components to Administration that are critical to follow best practices to ensure that business efficiency is optimized, security is tight, and compliance is met.

Managing Target Systems

Target system resource processes allow administrators to connect Omada to target systems so that Omada can read information such as current user access rights and write new access rights. Target system resources are read into Omada from the connected system via data collector interfaces. Each target resource requires enrichment to include data related to ownership, show/hide request access, status and validity, attributes, approval levels, delegation, exclusive management, and post validity. This is usually set via rules and policies at system level to minimize the manual effort.

Onboard Application

The Onboarding Application process enables the business to define roles and applications based on business requirements, instead of the technical resources and permissions that give users access in the target systems. System resources often have technical names that business users do not understand. Using the Application Onboarding process, IT and business users can collaborate to create roles and resources with business-friendly names and descriptions thereby reducing the time it takes to request access and to review the requests.

The process also allows organizations to create logical business applications that come from multiple target systems. For example, an application that uses AD for access control would consist of the application itself and AD. Applications often need access to multiple resources that do not need to be known by business users. This allows the user to quickly select a single application they need without getting lost in the technical details that are not relevant for their purposes.

100
The average number of passwords per person[1].

90%
Of internet users are worried about getting their passwords hacked[2].

23 Million
The number of accounts that use the password '123456'[2].

$70
On average, it costs an enterprise $70 for a single password reset[3].

Source[1]: NordPass
Source[2]: DataProt
Source[3]: BioConnect

Process Stakeholders

Within IGA processes, it is critical that multiple stakeholders are aligned and working together. For Identity Security Breach Management, the following teams must be involved in the following capacities:

IGA Team

- Manage target system resources in Omada and ensure connections are working properly
- Create the challenge questions

Business and Application System Owners

- Ensure that enrichment data is added to target systems
- Define which target system resources define end user applications

Business Users

- Interact with Omada to reset passwords

Password Management

Password management is increasingly critical, as passwords are routinely targeted by attackers, and are also very challenging for business users to keep track of. Within identity governance, this requires that the target business system is managed and enforced based on each system's required password strength. The Administration processes ensure that password generation within Omada creates passwords that are equal to (or stronger than) the requirements for the business systems. The password policy is described in simple terms, such as password length and complexity. Data administrators can easily create and update password policies in Omada to enforce minimum strength policy, and if necessary can make changes to the policy to maintain system security.

Unauthenticated Password Reset

Within IdentityPROCESS+, users that forget passwords are given easy workflows to allow them to reset passwords. This self-service process eliminates the need to contact the helpdesk. This process is designed so that the user answers pre-defined security questions and if necessary can create a new password themselves. The user can also be presented with several challenge questions, where - if completed - they can enter in a new password (assuming that the new password satisfies the password policy). Once a user enters their username into the self-service password portal, Omada checks to ensure that it is an active identity.

Password Reset Enrollment

The Administration process outlines how to allow the administrator to edit the challenge questions to the user, such as 'what is your mother's maiden name?' The administrator selects challenge questions within the Omada interface and can then edit those available to end users. Administrators can also set up other parameters such as the number of questions to be shown, the number of reset failures before the identity is locked, and notification parameters.

Authenticated Password Reset

Managers or operations administrators select whose passwords should be reset in Omada, and those users are presented with a list of identities, grouped by password policy, where the underlying system is enabled for a password reset. Omada then asks the user to enter their current and new password, checks that the new password satisfies the password policy and creates a provisioning request to perform synchronization.