Omada

Extend Identity Governance and Access Workflows with Omada + ServiceNow

Leverage identity governance processes within ITSM tools
for fluid and secure access workflows, with full audit trail

Contents

An integrated identity governance and administration (IGA) and IT service management (ITSM) solution streamlines business processes, empowers business users and administrators alike, and improves the overall security posture of the organization. The combination of strong IGA and ITSM maximizes business output while ensuring strong security through seamless workflows for users to request access to related and approved business resources with full reporting capabilities for documentation and compliance.

Integrated IGA and ITSM

IGA and ITSM applications help organizations centralize all identity access rights, and ensure that people can request, review, and track access to the various applications that exist throughout hybrid, cloud and multi-cloud environments. This document outlines the standard use cases and covers different aspects of what organizations should expect from integrating Omada, the leader in modern identity governance, with ServiceNow, the leader in ITSM.

Omada and ServiceNow

Omada establishes guideposts and transparency of who is entitled to use which resources, for what reason and when, and controls access through efficient request and policy workflows – with audit-ready reporting capabilities for easy documentation of compliance. Omada also provides the ability to certify access and roles, govern access throughout the identity lifecycle, and ensure that toxic combinations are prevented by implementing separation of duties (SoD) controls.

Integrating Omada and ServiceNow allows joint customers to generate transparency of who has access to what, for what reason, and when, based on requests. Omada and ServiceNow provide customers with best-in-breed solutions that integrate seamlessly, with a unified platform for all access requests and reviews. Omada and ServiceNow provide customers with access to the Omada reference architecture that automatically runs policy violation checks to ensure SoD is being adhered to,access is being provisioned in real-time, and defining and implementing automated access rules and policies. The advanced governance and reporting capabilities of Omada enable customers to document accountability for auditors and authorities. These capabilities allow organizations to get in control of identities and their access rights throughout their entire lifecycle, from joining the organization, moving departments and roles, and eventually leaving the organization.

> "Omada and ServiceNow provide customers with best-in-breed solutions that integrate seamlessly, with a unified platform for all access requests and reviews."

Capabilities

The integration of ServiceNow and Omada Identity improves access management functionalities and capabilities including:

- Unified application for access requests within ServiceNow
- Enable all identities to request access to business resources and applications, whether on mobile, tablet, or desktop
- Eliminate the need for business users to be fluent in multiple tools for accessing specific resources
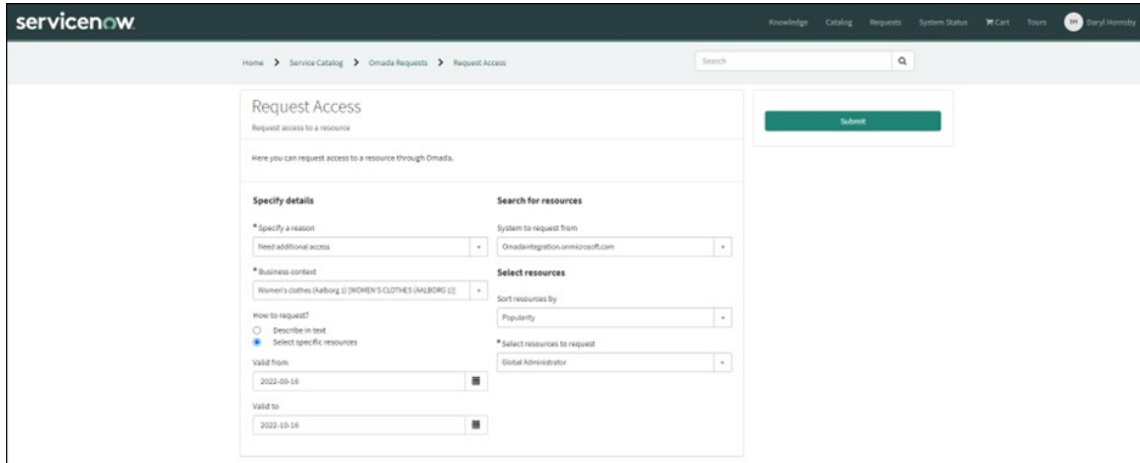
Figure 1: The Request Access portal within the ServiceNow application

There are three different types of integration options between Omada and ServiceNow. The technology offered within the two product offerings allows for rich configuration and adaptation based on organizational requirements. Below are examples of each of these, and the associated use cases:

Governance

Governance and administration of ServiceNow accounts and entitlements within Omada

Provisioning

Indirect provisioning of accounts and entitlements in ServiceNow governed by Omada

Integration

Specific integrations from ServiceNow to Omada, utilizing the rich set of APIs provided to third-party integrations

Governance and Administration of ServiceNow

Omada is used for governance and administration of ServiceNow accounts and entitlements to the entire workforce based on policies or access requests, and ensures that the right identities (employees, contractors, interns, auditors, etc.) have access to the provided functionality

The Omada Compliance Workbench renders compelling insights about systems and protected data, visualizing the compliance level for each application and system. It provides a high-level overview with traffic light indicators and the ability to drill down into detailed access, and the ability to easily configure unique KPIs to monitor progress. With a single click, it is possible to instantly execute remediation activities for critical findings.

Use Case

1. An organization wants to assign a ServiceNow account for all employees, including a standard set of roles and groups.
2. An assignment policy is created and the account with permissions is calculated and provisioned automatically as part of the onboarding process for employees.
3. The organization wants to perform yearly access reviews of ServiceNow access to ensure compliance. Access review surveys are launched and completed within Omada Identity and any removed/revoked entitlements are automatically deprovisioned from ServiceNow.

Functionality

- Collector to import ServiceNow accounts, resources and assignments.
- Connector to provision ServiceNow accounts, resources and assignments
- All objects exposed in the ServiceNow REST API are supported and can be configured by customers to match requirements.
- Enable all business users to request access to additional resources or data from a unified platform.

Implementation

- Standard collector with default queries and mappings for ServiceNow.
- Standard connector with default data model and task mappings for ServiceNow.

Indirect Provisioning

If an organization is manually provisioning accounts or entitlements to a target system, the basis for this decision might be related to the complexity, security, or integration options of the system. Using Omada, it is possible to determine the provisioning need and create associated tickets in ServiceNow for agents to fulfill.
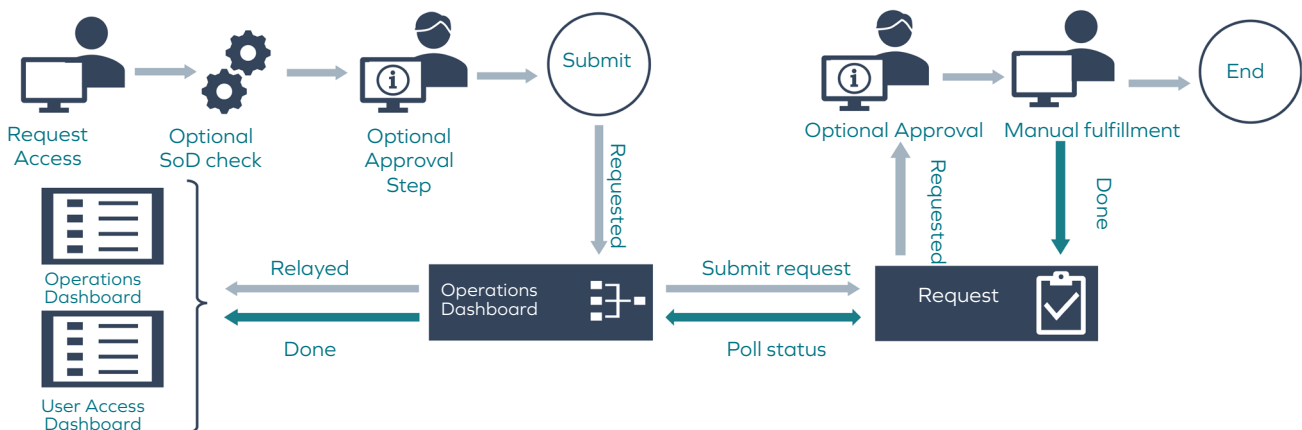
Use Case

1. An end user has submitted a request for an access within either Omada or ServiceNow, and it has been approved accordingly.
2. The requested entitlement belongs to a system that is manually provisioned. As the organization already has provisioning processes in place in ServiceNow, they want to use these processes for all manual provisioning tasks. Omada Identity sends a task to ServiceNow via the ServiceNow relayed provisioning connector.
3. When the ServiceNow ticket has been processed, the status of the task is updated in Omada Identity and reconciliation can take place.

Functionality

- Integrate to ServiceNow for indirect/manual provisioning (i.e. create tickets in ServiceNow)

- Ticket status retrieved from ServiceNow for provisioning claim.

Implementation

- ServiceNow relayed connector in the Omada Provisioning Service is used to submit jobs to ServiceNow.
- The connector uses ServiceNow's REST API to create tickets (e.g. requests or incidents) in ServiceNow.
- Status of tickets in ServiceNow polled at regular intervals - visible in Omada Identity dashboards
- ServiceNow processing of the tickets per ServiceNow workflow definitions.
- Provisioning claim created once tickets are completed in ServiceNow.

Integration

Organizations that use the development and configurability options in ServiceNow to build applications which mimic company specific processes can also use the rich set of APIs exposed by Omada to make access requests, retrieve relevant identity, account, and entitlement data.

Use Case 1

1. An organization wishes to implement a simplified access request process in ServiceNow, using Omada solely for policy validation and provisioning by leveraging the rich API functionality provided.
2. Omada functionality, like access review surveys, remains available to ensure continuous compliance within the organization.

Functionality

- Utilize ServiceNow as an end user interface to render access request UI / workflow.

- Omada Web Service to generate assignment records.
- Leverage Omada provisioning framework for target system provisioning.

Implementation

- Omada Data API to retrieve contexts and entitlement catalogue.
- User credentials must be provided with the request. The API supports basic authentication and integrated security for enforcing access controls.
- Submit entitlement for policy validation (e.g. SoD), provisioning and reconciliation.

Use Case 2

1. An end user has submitted an access request but has not received a confirmation that the request has been fulfilled. The user opens ServiceNow to verify the status of the request.
2. Data is returned from Omada which shows the access requests, approval and fulfillment status for the end users requests. The specific request is awaiting approval by the user's manager. End user acts accordingly.
3. Above functionality could also exists for managers being able to see overview of organizational requests or ServiceDesk for end user support.

Functionality

- Utilize ServiceNow as an end user interface to display status of Omada.

- Omada Web Services for Access Request, Approvals and Fulfillment Status for an identity is called from ServiceNow.

Implementation

- Omada Data API for Access Request Overview for user/identity.
- User credentials must be provided with the request. The API supports basic authentication and integrated security for enforcing access controls.
- Lookup for specified user (or manager/ServiceDesk officers) to see status of requests.
- Data displayed in ServiceNow via e.g. a dashboard widget based on configuration or development done.

Use Case 3

1. An end user is unsure if they have access to an application and before submitting an access request the user calls the ServiceDesk to verify if he still has the access.
2. The ServiceNow administrator navigates to the implemented assignments dashboard and searches for the user.
3. Data is returned from Omada that shows the current assignments/access rights for the identity. Access to the application is not assigned to the identity and the user can submit a new request.

Functionality

- Utilize ServiceNow as an end user interface to display status of Omada assignments.

- Omada web service to retrieve assignment overview for an identity and display in ServiceNow.

Implementation

- Omada Data API for assignment overview for user/identity.
- User credentials must be provided with the request. The API supports basic authentication and integrated security for enforcing access controls.
- Lookup for specified user to allow ServiceDesk officers to see status on behalf of a user.
- Data displayed in ServiceNow via e.g. a dashboard widget based on configuration and/or development done.

Improving Security, Compliance, and Efficiency

The benefits of integrating ServiceNow with Omada include streamlining business services, empowering end users, and delivering a general improvement of the overall security posture. While ServiceNow focuses on service-oriented standards such as ITIL and standards such as ISO 20000 "Requirements for IT Service Management Processes," Omada also offers a focus on automation and IT security standards such as ISO 27001 which covers "Requirements for an Information Security Management System ".

Key Features of the integration between Omada and ServiceNow include:

- Business users being able to request access
- Business users selecting contexts to request in
- Filter resources on system
- Filter out already assigned resources
- Control which resources are available to be requested in ServiceNow
- Select validity
- See the status of access request

Key Benefits of integrating Omada and ServiceNow include:

- Enable all identities to request access to business resources and applications whether on mobile, tablet, or desktop, within a single interface
- Provide a native experience directly in ServiceNow for all business requests
- Eliminate the need to have business users be fluent in multiple tools for accessing specific resources

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.