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. Administrators can create seamless workflows to request access to related and approved business resources with full reporting capabilities for documentation and compliance. Furthermore, integrating IGA and ITSM enables all business requests to be performed from a single user interface, keeping users in applications that they're already comfortable with.

Introducing the Omada ServiceNow Application

Integrating IGA and ITSM applications helps organizations centralize all identity access rights, ensuring that employees can request, review, and track access to the various applications that exist throughout hybrid, cloud, and multi-cloud environments.

To streamline the access request process, Omada has created a ServiceNow application: Omada Service Catalog. By integrating Omada's comprehensive identity and access management solutions with the powerful capabilities of ServiceNow, the app enables seamless user lifecycle management, efficient access provisioning, and robust security protocols. This integration not only simplifies the user experience but also boosts productivity by centralizing access management tasks. By providing a unified interface for access requests and monitoring, the Omada ServiceNow app ensures a cohesive and intuitive user journey. This integration improves access management functionalities and capabilities including:

- Provide a native experience directly in ServiceNow for all business requests
- Enables all identities to request access to business resources and applications wherever they are, whether on mobile, tablet, or desktop
- Eliminates the need for users to be fluent in multiple tools for accessing specific resources

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

Integrating Omada and ServiceNow

The technology offered within Omada Identity Cloud and ServiceNow allows for rich configuration and adoption options based on your business needs. There are four different types of integration options:

- **Omada Service Catalog Application:** ServiceNow capabilities are provided out-of-the-box (OOTB) via the Omada Service Catalog application, no additional configuration is needed

- **Governance:** The governance and administration of ServiceNow accounts and entitlements are managed within Omada Identity Cloud

- **Indirect Provisioning:** Indirect provisioning of accounts and entitlements in ServiceNow is governed by Omada Identity Cloud

- **Additional Integrations:** Specific integrations from ServiceNow to Omada, utilizing the rich set of APIs provided for third-party integrations

In the sections below, we explain each integration type and give examples of the associated use cases.

Omada Service Catalog Application

Organizations looking to accelerate time-to-value can take advantage of the OOTB functionality provided by the Omada Service Catalog application. We provide the following functionality without any additional configuration necessary:

- Request for self

- Request on behalf of another identity

- Select context to request in (if configured in Omada Identity Cloud)

- Filter resources on a system

- Filter out already assigned resources

- Control which resources are available to be requested in ServiceNow (e.g. only expose business roles)

- Select validity

- See the status of an access request

Use Case
Using ServiceNow as the UI for all access requests while using Omada solely for provisioning and policy validation

- Omada functionality remains available to ensure continuous compliance within the organization.

Functionality

- ServiceNow is utilized as the end-user interface for access requests.
- The Omada OData API generates assignment records.
- Organizations leverage the Omada provisioning framework for target system provisioning.

Implementation

- Uses the Omada GraphQL API to retrieve contexts and entitlement catalog, including the configuration of who can request what and for whom.
- The integration is seamless for the end user as the logged-in user in ServiceNow is registered as the requestor in Omada Identity.
- Submit the entitlement for approvals, policy validation (e.g. Separation of Duties), provisioning, and reconciliation.

Governance and Administration of ServiceNow

In this integration option, Omada is used for the governance and administration of ServiceNow accounts. Entitlements for all ServiceNow accounts are based on policies or access requests, ensuring that the right identities (employees, contractors, interns, auditors, etc.) have access to the right resources.

Visibility is a crucial factor in ensuring effective IGA governance. Having a clear understanding of the compliance level of ServiceNow, and other onboarded applications and systems, is essential for maintaining a secure and well-managed environment. This is where the Omada Compliance Workbench comes into play. The Workbench offers a centralized dashboard that provides compelling insights into onboarded systems and the data they protect. Users can easily understand the compliance status through intuitive traffic light indicators, and the option to delve deeper into each view for more detailed information. What sets the

Omada Compliance Workbench apart is its flexibility and ability to take immediate action—it enables users to configure unique Key Performance Indicators (KPIs) tailored to their specific business needs, facilitating the monitoring of progress and highlighting potential areas of concern. The Workbench empowers administrators to take immediate remedial actions, ensuring that any issues are promptly addressed.

Use Case

Using Omada to create a ServiceNow account with a standard set of roles and groups for all employees

- An assignment policy is created within Omada Identity Cloud for an account in ServiceNow. As part of the employee onboarding process, a ServiceNow account is automatically provisioned with correct permissions based on an employee's role.
- The organization wants to perform yearly access reviews of ServiceNow access to ensure compliance. Access review surveys are launched and completed within Omada Identity Cloud. Any removed/revoked entitlements are automatically de-provisioned from ServiceNow.

Functionality

- The ServiceNow collector imports all ServiceNow accounts, resources, and assignments.

- The Omada connector provisions ServiceNow accounts, resources, and assignments.
- All objects that are exposed within the ServiceNow REST API are supported. Customers can configure these objects to meet business requirements.
- This integration option enables all business users to request access to additional ServiceNow resources or data from a unified platform.

Implementation

- Deploy a standard collector with default queries and mappings for ServiceNow.
- Deploy a standard connector with a default data model and task mappings for ServiceNow.

Indirect Provisioning

Complexity, security, or integration limitations may require organizations to provision accounts or entitlements to certain systems manually. Omada's ServiceNow integration helps streamline this process. In Omada Identity Cloud, users can request access to a target system. After the access request has been approved, a ServiceNow ticket is automatically created and routed to the target system's owner(s) to grant access.
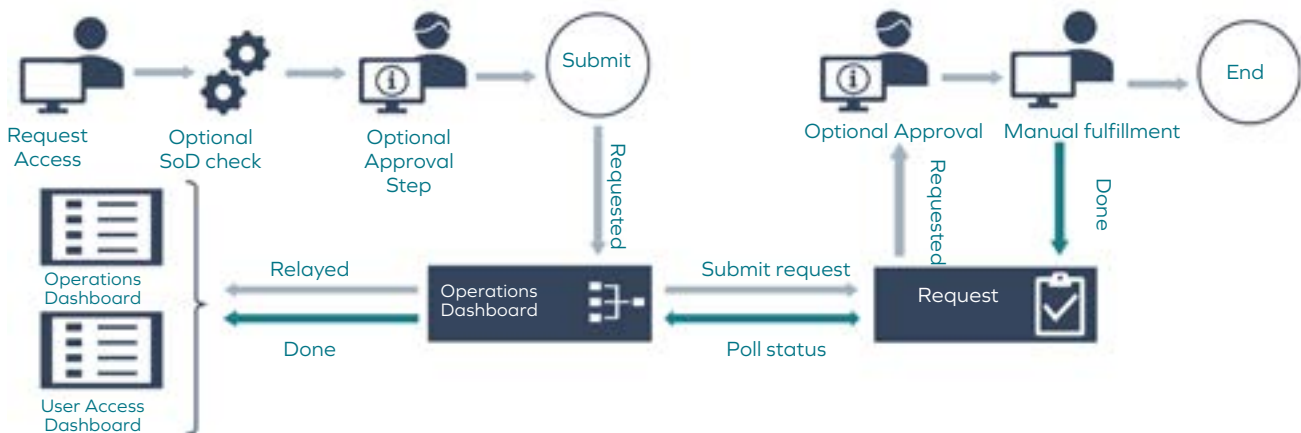
Use Case

Using Omada and ServiceNow to request access to a system that requires indirect provisioning

- An end-user has submitted an access request within Omada Identity Cloud, and it has been approved.
- The requested entitlement belongs to a system that requires manual provisioning. Since the organization already has provisioning processes in place within ServiceNow, they want to use a similar process for all manual provisioning tasks. Omada Identity Cloud sends a task to ServiceNow via the ServiceNow relayed provisioning connector; this task creates a ServiceNow ticket and routes it to the target system's owner(s) to manually approve access.
- When the ServiceNow ticket has been closed, the status of the task within Omada Identity Cloud is updated. Reconciliation takes place.

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

- Ticket status is retrieved from ServiceNow for provisioning claim in Omada Identity Cloud.

Implementation
- The ServiceNow relayed connector in the Omada Provisioning Service is used to submit jobs to ServiceNow.
- This connector uses ServiceNow's REST API to create tickets (e.g. requests or incidents) within ServiceNow.
- The status of ServiceNow tickets is polled at regular intervals and is visible in Omada Identity Cloud dashboards.
- ServiceNow processes tickets per the organization's predefined ServiceNow workflow definitions.
- A provisioning claim is created in Omada after tickets are completed in ServiceNow.
- Provisioning claim created once tickets are completed in ServiceNow.

Additional Integrations

Organizations that use the development and configurability options in ServiceNow to build applications that mimic company-specific processes can also use the rich set of APIs exposed by Omada to build any workflow, including the possibility to retrieve relevant identity, account, and entitlement data. Customers often build contractor onboarding processes to onboard new contractors and manage access for them

Use Case

Onboarding a contractor in ServiceNow
- Leveraging the rich API functionality provided, the organization can use Omada to create access policies and assign birth rights directly from ServiceNow.
- Omada is solely for policy validation and provisioning.
- Omada functionality remains available to ensure continuous compliance within the organization.

Functionality
- ServiceNow is utilized as the end-user interface for contractor onboarding.

- The Omada OData API generates the identity and assignment records.
- Organizations leverage the Omada provisioning framework for target system provisioning.

Implementation
- Use the Omada OData API to retrieve contexts and entitlement catalogs.
- Integration using impersonation through a service account can be achieved for a seamless experience for the end user.
- Submit the entitlement for policy validation (e.g. Separation of Duties), provisioning, and reconciliation.

Use Case
Using ServiceNow to verify that status of an access request

- An end-user has submitted an access request but has not received confirmation that their request has been fulfilled. The user opens ServiceNow to verify the status of their request.
- Data is returned from Omada Identity Cloud, showing the access request, approval, and fulfillment status for this request. This request is awaiting approval from their manager. The end user reaches out to their manager for approval.
- This functionality also exists for managers, who are provided with an overview of all organizational requests.

Functionality
- Utilize ServiceNow as an end-user interface to display data from Omada.

- ServiceNow calls Omada OData API to display access requests, approvals, and fulfillment status for a particular identity.

Implementation
- Utilize the Omada Data API for access request overview information for a particular user/identity.
- Integration using impersonation through a service account can be achieved for a seamless experience for the end user.
- Provide user credentials when requesting information from the Omada Data API. The API supports basic authentication and integrated security to enforce access controls.
- To see the status of a request, search for the specific user who started the request.
- Configure or develop dashboard widgets within ServiceNow to display data from Omada.

Use Case
An end user calls the Help Desk to determine if they have access to an application

- An end-user is unsure if they have access to an application. Before submitting an access request, they call the Help Desk to verify if they have access.
- The Help Desk administrator navigates to the implemented assignments dashboard within ServiceNow and searches for the user.
- Data is returned from Omada Identity Cloud showing the current assignments/access rights for the identity. The end-user does not have access to this application but can submit a new access request to gain access.

Functionality
- Utilize ServiceNow as an end-user interface to display data from Omada.

- ServiceNow calls Omada OData API to display an assignment overview for a particular identity.

Implementation
- Utilize the Omada Data API for access request overview information for a particular user/identity.
- Integration using impersonation through a service account can be achieved for a seamless experience for the end user.
- Provide user credentials when requesting information from the Omada Data API. The API supports basic authentication and integrated security to enforce access controls.
- To see the status of a request, search for the specific user who started the request.
- Configure or develop dashboard widgets within ServiceNow to display data from Omada.

Improving Security, Compliance, and Efficiency

The benefits of integrating ServiceNow with Omada include streamlining business services, empowering end users, and improving 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 ".

The integration of Omada Identity Cloud and ServiceNow presents a strategic approach that enhances organizational processes, security, and user experiences. This integration not only streamlines access requests and provisioning, but also ensures that the right individuals have access to the appropriate resources within complex hybrid, cloud, and multi-cloud environments. The unified interface simplifies user interactions, reducing the need for proficiency in multiple tools. Whether it's through governance, indirect provisioning, out-of-the-box integration, or tailored additional integrations, this partnership empowers organizations to efficiently manage identity access rights, enhance compliance, and elevate security measures.

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