Omada

Omada APIs:

The Key to Effortless IGA Integration and Automation

Streamlining Identity Governance and Administration (IGA) is a critical but often complex task for security professionals because of the highly diverse tapestry of tools and systems in use by many enterprises. To address this complexity Omada offers an extensive solution through our GraphQL and OData APIs. These APIs act as efficient data access tools, enabling the identity fabric by supporting the development of integrations and providing granular control over access management. This brief will give an overview of these APIs, including what they can do, how you can use them, and their key differences. By understanding these APIs, you'll extend the full potential of Omada across your identity infrastructure and bring your IGA processes to the next level.

Understanding GraphQL vs OData

Before diving into Omada's APIs, let's explore the key differences between GraphQL and OData. GraphQL is designed for client-side applications that need to interact with Omada at a business functions level. Imagine building a custom report - you specify exactly what information you need in a single request, minimizing data transfer and simplifying development. In contrast, OData follows a more structured data access model. Imagine it like browsing a traditional online store - you need to visit separate pages for product details, reviews, and similar items. OData might require multiple API calls to retrieve related data points. This approach provides fine-grained control for manipulating data within the underlying system but can involve more steps for client-side applications.

Precise Control with Omada's OData REST API

Omada's OData REST API provides a versatile toolkit for optimizing identity and access management within your organization.

This API equips you with the following capabilities :

- **Core Entity Management:** Perform CRUD (Create, Read, Update, Delete) operations on various built-in object entities within Omada Identity. This allows you to add, modify, retrieve, and delete user accounts, groups, roles, and other essential identity data.

- **Actionable Functions:** Utilize a set of pre-built functions to automate specific tasks. These functions can directly interact with the Omada data store, enabling actions like:
    - Changing a user's password.
    - Verifying password strength against defined policies.
    - Resetting forgotten passwords.
    - Converting between an object's unique identifier (GUID) and its integer ID.
    - Granting or verifying access to the CIAM portal for specific identities.
- **Granular Search and Filtering:** Construct precise queries using OData's robust filtering and sorting capabilities.
    - Leverage filter operators to narrow down results based on specific criteria like user names, group memberships, or creation time.
    - Employ sorting options to organize search results by properties like ID, creation date, or display name.
- **Efficient Data Retrieval:** Optimize data retrieval through functionalities including:
    - `select:` Specify the exact properties you require, minimizing data transfer and improving performance.
    - `top:` Limit the number of returned results, ideal for retrieving the most recent or relevant data.
    - `skip:` Bypass a specific number of initial results, useful for paginating through large datasets.
- **Batch Processing:** Expedite bulk operations by utilizing OData's batch processing capabilities. Submit a group of changes as a single transaction, ensuring all modifications succeed or fail together, maintaining data integrity.

By leveraging the OData API's versatility, you can simplify identity and access management tasks within Omada. From core data manipulation to automated functions and efficient querying, the OData API empowers you to take full control over your identity landscape.

Omada's OData REST API lets you to swiftly retrieve and manage identity data with fine-grained control through its intuitive query capabilities.

Agility and Flexibility with the Omada Identity Graph API

Leveraging, GraphQL, the Omada Identity Graph API enables Omada Identity Cloud customers to seamlessly integrate access request workflows directly within their existing applications.

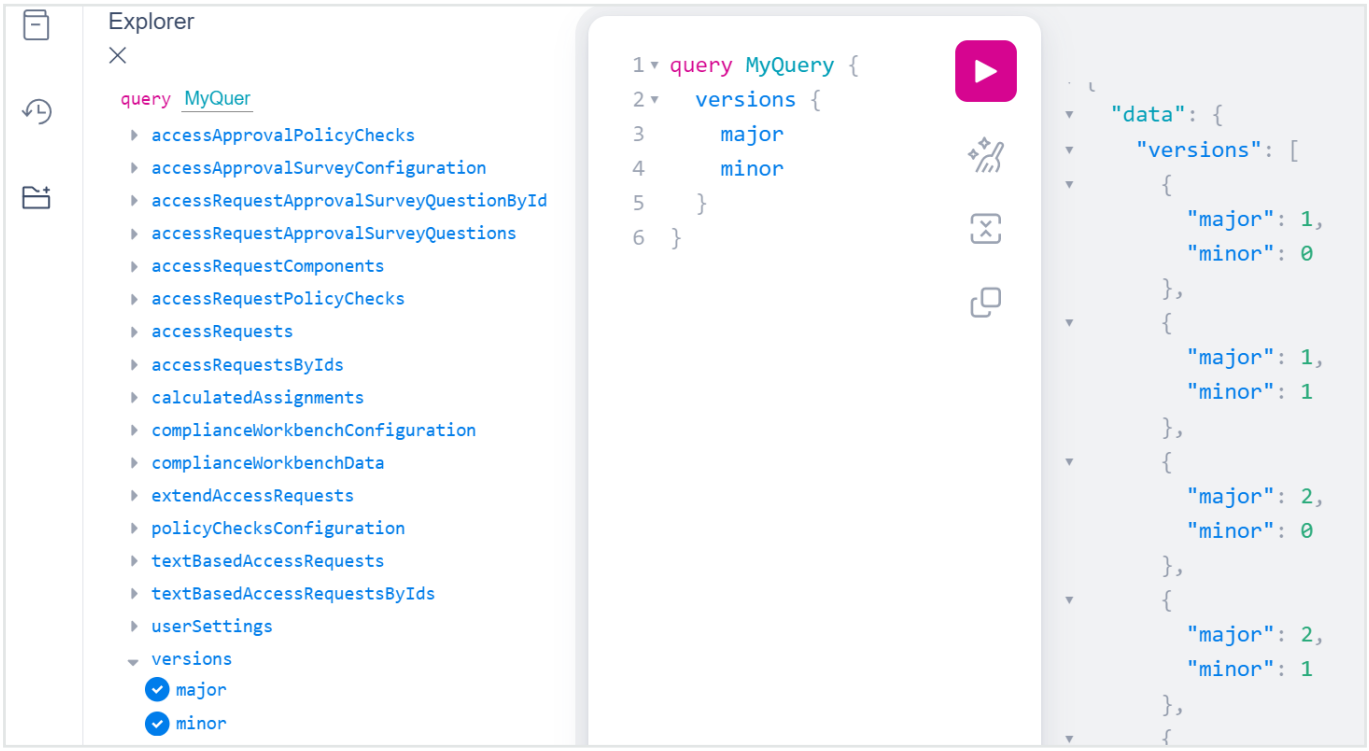
The Omada Identity Graph API provides a range of versatile capabilities for access request management:

- **Streamlined Request Creation:** Submit access requests directly from your custom clients, specifying identities and desired resources.
- **Enhanced Visibility:** Gain a comprehensive overview of submitted access requests, including their current status.
- **Granular Control:** Request access for individual identities or multiple identities at once. Similarly, target specific resources or request access to multiple resources.
- **Contextual Awareness:** Leverage server-side hidden and "Requires Value" settings for Business Context and Reason fields, ensuring a clear and well-defined access request.
- **Resource Transparency:** Access detailed information about resources, including their visible attributes.
- **Multi-Account Support:** Manage access requests across multiple Omada accounts within your client application.
- **Validity Management:** Set a specific validity period for access requests, ensuring temporary access when needed.
- **Request Tracking:** Maintain a comprehensive list of submitted access requests and resource assignments .
- **Status Reporting:** Gain real-time insights into the status of your access requests.
- **Advanced Filtering:** Filter access requests based on specific resources and their attributes for efficient management.

The Omada Identity Graph API transcends access requests, offering two key features that significantly enhance IGA workflows. Firstly, it eliminates the time-consuming task of identifying and filtering out resources already assigned to users. This "pre-allocation filtering" ensures that administrators only see relevant options when granting access, saving valuable time and minimizing the risk of human error. This API also prioritizes data by sorting resources based on popularity. This intuitive approach simplifies navigation and decision-making for administrators, especially when managing large numbers of resources within the organization. These features collectively contribute to a more optimal and improved IGA experience.

Omada provides an intuitive, built-in API explorer that empowers you to prototype GraphQL queries directly within your Omada instance. This interactive tool eliminates the need for external documentation or guesswork, allowing you to quickly understand and experiment with Omada's API capabilities. With real-time feedback and error handling, you can iterate on your queries efficiently, ensuring seamless integration with your security infrastructure. This explorer is a valuable resource for streamlining the process of discovering and utilizing Omada's API functionalities.

By leveraging the Omada Identity Graph API, you can optimize access request workflows, enhance visibility, and gain granular control over access management within your organization. This enables you to seamlessly integrate IGA functionalities into your existing applications, fostering a more effective and secure environment.



With Omada's intuitive API explorer, you can effortlessly visualize, build, and test GraphQL queries, accelerating your integration process and maximizing the potential of Omada Identity Cloud.

Authentication

Omada offers two methods of authentication to secure access to its APIs, providing flexibility and adaptability to suit different integration scenarios:

- **OAuth:** Omada employs OAuth, a widely adopted authorization protocol, to enhance security and flexibility. OAuth involves a three-way handshake between the client application, Omada Identity server, and the authorization server. This process ensures that only authorized users can access protected resources.
- **Basic Authentication:** For simpler use cases, Omada also supports basic authentication. This method requires providing the username and password directly in the request headers. While it's easier to implement, basic authentication is generally less secure than OAuth due to the transmission of credentials in plain text.

The choice between OAuth and basic authentication depends on your specific security requirements and which API you're using. Omada's OData REST API supports both OAuth and basic authentication, providing you with options to choose the method that best aligns with your integration needs. On the other hand, the Omada Identity Graph API strictly requires OAuth authentication for enhanced security and to support advanced features.

Choosing the Right API

While each API provide access to Omada's identity data, they cater to different use cases:

Use Case	Best API	Why
Retrieving user details and associated group memberships in a single request	Omada Identity Graph API	Swiftly retrieves all necessary data in one call. Reduces development time and network traffic.
Performing complex data filtering and sorting on specific user attributes	Omada Identity Graph API	Offers flexibility to specify exact data needs in the query, reducing unnecessary data transfer and improving performance.
Integrating with custom applications requiring specific data points	Omada Identity Graph API	Enables developers to tailor data requests to the application's needs, simplifying integration and reducing development overhead.
Fetching data for client-side applications (user interfaces, dashboards)	Omada Identity Graph API	Designed for rapid retrieval of specific data sets, minimizing data transfer and improving responsiveness for client-side applications.
Frequent data updates and real-time synchronization	Omada Identity Graph API	Offers potential for subscriptions, allowing for real-time data updates within applications, enhancing user experience.
Bulk data updates or complex data manipulation on the server-side	OData REST API	More streamlined for performing large-scale updates or manipulating data within your Omada environment. Provides finer-grained control for server-side operations.
Integrating with existing systems that utilize OData protocols	OData REST API	Ensures compatibility and simplifies integration with legacy systems or platforms already utilizing OData for data access.
Need for granular control over specific data elements within Omada	OData REST API	Offers a more structured approach, allowing for precise control over individual data elements retrieved or manipulated within Omada.
Direct manipulation of raw data within the Omada data model	OData REST API	Offers deeper control over the data model
Limited development resources or need for a simpler API for basic data retrieval	OData REST API	Easier to learn and implement for basic use cases, requiring less development effort compared to GraphQL's flexibility.

When deciding between these APIs, understanding their strengths is key. The Omada Identity Graph API shines for client-side applications, offering prompt data retrieval for specific needs and enabling real-time data updates. Its flexibility allows developers to tailor data requests for custom integrations. However, OData and REST remain solid choices for bulk data updates, server-side operations, and integration with existing OData-based systems. They also provide a more structured approach with granular control over data elements. Ultimately, the ideal API hinges on your specific use case, data complexity, and your development team's experience.

By leveraging any of our API, you gain granular control over Omada's identity data, empowering you to implement robust and swift IGA practices today. This future-proof approach ensures your organization can adapt to evolving identity management needs while maintaining the highest levels of security and efficiency.

Omada

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.

09172024