Wing Public API Documentation

Overview

The Wing Public API provides endpoints for managing your organization's security posture through programmatic access to users, applications, security issues, and OAuth connections. All endpoints require authentication and are designed for external integrations and automated workflows.

Key Capabilities:

- **User & Application Inventory**: Retrieve detailed information about users and applications in your organization
- **Security Issues Management**: List and update the status of security issues detected by Wing
- **Connection Management**: View and revoke OAuth connections between users and third-party applications

Base URL: `https://public-api.wing.security`

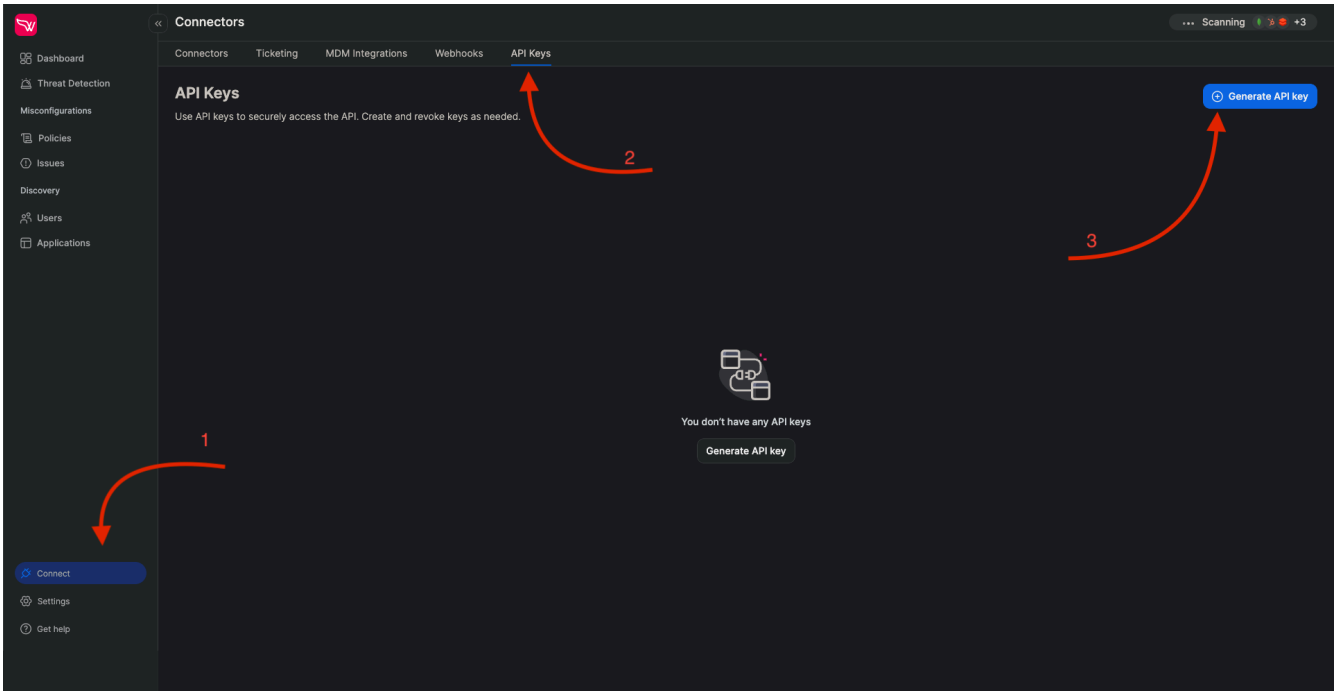
Authentication

To access the Wing Public API, you must first create an API key through the Wing portal. All API requests require authentication using an API key in the x-api-key header.

Creating an API Key

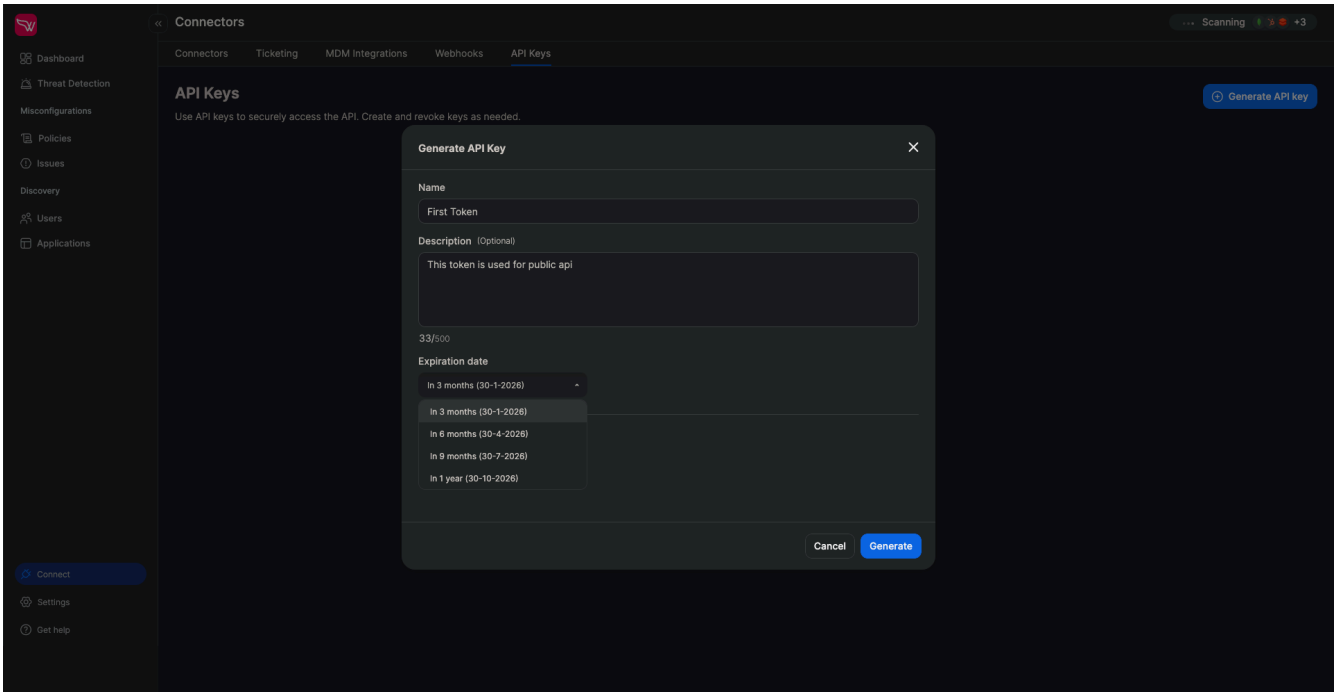
Step 1: Navigate to API Keys

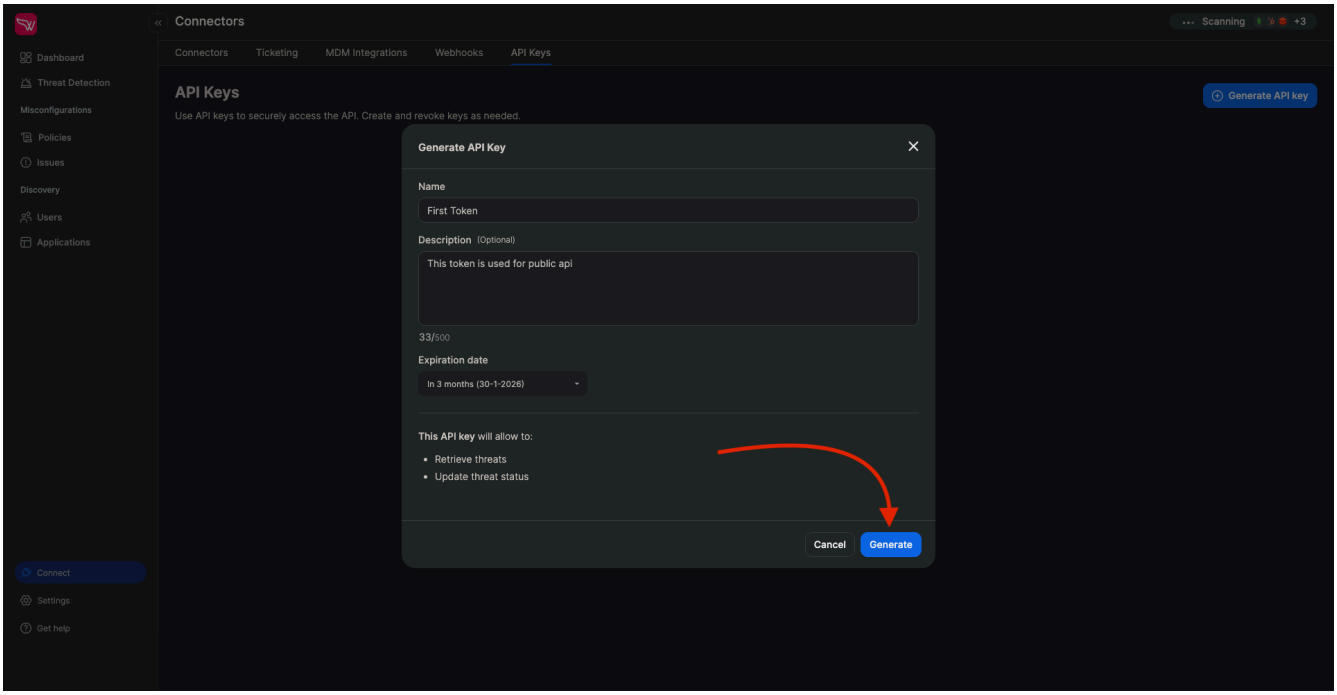
- Log in to the Wing portal
- Navigate to the **Connect** section
- Locate and click on **API Keys**



Step 2: Generate a New API Key

1. Click **Generate API Key** to create a new key
2. Enter a descriptive name for your API key
3. Optionally add a meaningful description to help identify the key's purpose
4. Select an appropriate expiration date from the available options
5. Click **Generate** to create the key



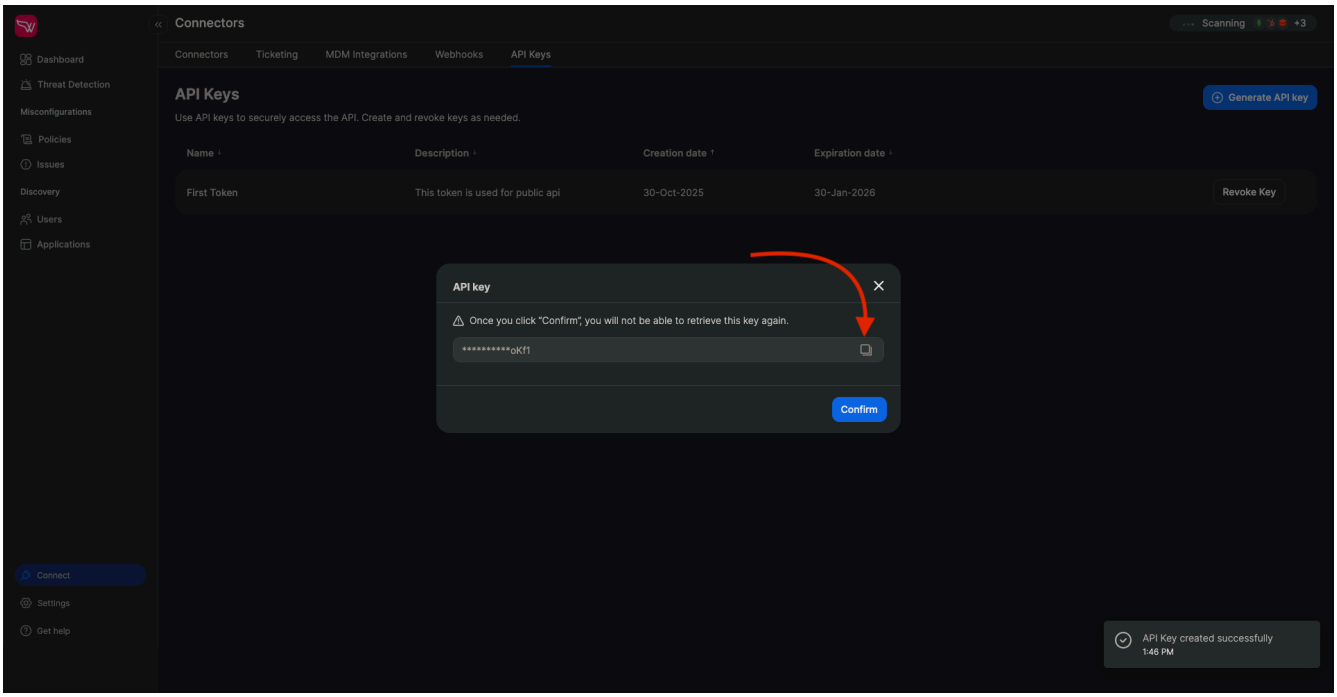


Step 3: Copy Your API Key

After generation, you'll see a popup window displaying your API key. For security reasons:

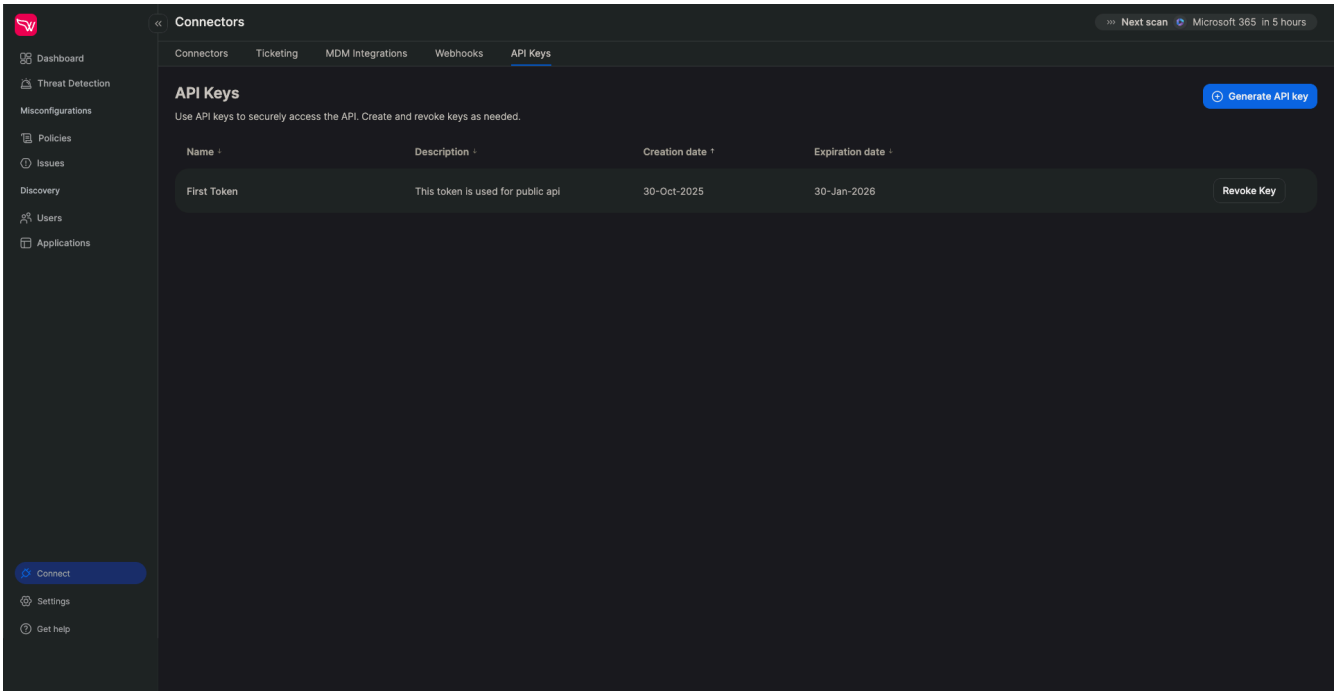
- The complete key is only shown once
- The key is not stored in our system after confirmation
- You cannot retrieve the key again after closing this window

Important: Copy your API key immediately using the **Copy** button before clicking **Confirm**.



Step 4: Manage Your API Keys

Your newly created API key will appear in the list of available API keys. You can view all your active keys and their details from this interface.

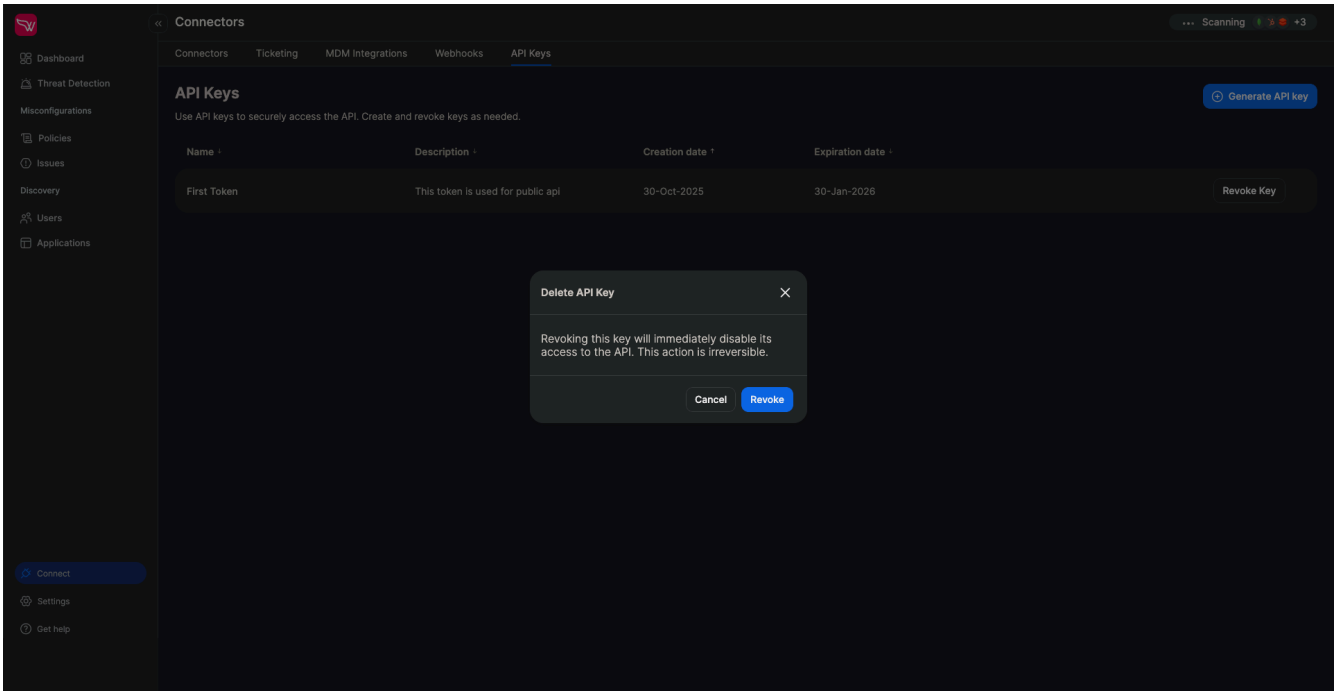


Step 5: Revoke API Keys

To revoke an API key:

1. Locate the key you want to revoke in the API keys list
2. Click the **Revoke** button
3. Confirm the revocation in the popup dialog

Warning: Once revoked, the API key will immediately become invalid and cannot be restored.



Using Your API Key

Include your API key in all requests using the Authorization header:

```
curl -X GET "https://public-api.wing.security/v1/users" \
```

```
  -H "x-api-key: YOUR_API_KEY_HERE"
```

Security Best Practices:

- Store your API key securely and never commit it to version control
- Use environment variables or secure credential management systems
- Regularly rotate your API keys
- Revoke unused or compromised keys immediately

API Endpoints

Method	Endpoint	Description
GET	`/v1/users`	Retrieve users with filters and pagination
GET	`/v1/users/{user_id}`	Retrieve a specific user by ID
POST	`/v1/users/{user_id}/connections/revoke`	Revoke all connections for a specific user
GET	`/v1/apps`	Retrieve applications with filters and pagination
GET	`/v1/apps/{app_id}`	Retrieve a specific application by ID
GET	`/v1/apps/{app_id}/connections`	Retrieve connections for a specific application
POST	`/v1/apps/{app_id}/connections/revoke`	Revoke all connections for a specific application
GET	`/v1/connections`	Retrieve app connections with filters and pagination
POST	`/v1/connections/{connectionId}/revoke`	Revoke a specific connection
POST	`/v1/connections/revoke`	Bulk revoke multiple connections
GET	`/v1/issues`	Retrieve issues with filters, sorting, and pagination
GET	`/v1/issues/{issue_id}`	Retrieve a specific issue by ID
PATCH	`/v1/issues/{issue_id}`	Update a specific issue (e.g., change status)

Endpoints Reference

Get Users

```
GET /v1/users
```

Retrieve a filtered and paginated list of users with their organizational details and security status.

Request Parameters

Parameter	Type	Required	Description
org_unit	string	No	Filter by organizational unit
tags	array[string]	No	Filter by user tags
status	string	No	Filter by user status (active, inactive, deleted, etc.)
mfa_enabled_in	array[string]	No	Filter users with MFA enabled in specific connectors
mfa_disabled_in	array[string]	No	Filter users with MFA disabled in specific connectors
page	integer	No	Page number (default: 0)
page_size	integer	No	Items per page (default: 50, max: 1000)
search_term	string	No	Filter users by name or email (partial match)

Response Schema

```
{
  "type": "object",
  "properties": {
    "users": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "id": {
            "type": "string",
            "description": "Unique user identifier"
          },
          "name": {
            "type": "string",
            "description": "User's name (may be full name or email addr
          },
          "status": {
            "type": "string",
            "enum": ["active", "inactive", "deleted", "deleted from api
            "description": "Current user account status"
          },
          "hrStatus": {
            "type": "string",
            "description": "Employment status from HR system"
          },
          "jobTitle": {
            "type": "string",
            "description": "User's job title"
          },
          "reportsTo": {
            "type": "string",
            "description": "User ID of direct manager"
          },
          "organizationalUnit": {
            "type": "string",
```

```
        "description": "Organizational unit or department"
      },
      "idpMfaStatus": {
        "type": "array",
        "items": {
          "type": "object",
          "properties": {
            "connectorName": {
              "type": "string",
              "description": "Name of the identity provider connect
            },
            "status": {
              "type": "string",
              "enum": ["Enabled", "Disabled", "Unknown"],
              "description": "MFA status for this connector"
            }
          },
          "required": ["connectorName", "status"]
        },
        "description": "MFA status per identity provider"
      },
      "adminIn": {
        "type": "array",
        "items": {
          "type": "string"
        },
        "description": "List of connectors where user has admin pri
      },
      "tags": {
        "type": "array",
        "items": {
          "type": "string"
        },
        "description": "User tags"
      },
      "applicationsCount": {
        "type": "integer",
        "description": "Total number of applications user has acces
      }
    },
    "required": ["id"]
  }
},
"pagination": {
  "type": "object",
  "properties": {
    "page": {
      "type": "integer",
      "description": "Current page number (zero-indexed)"
    },
    "pageSize": {
      "type": "integer",
      "description": "Number of items per page"
```

```
        },
        "total": {
          "type": "integer",
          "description": "Total number of items across all pages"
        }
      },
      "required": ["page", "pageSize", "total"]
    }
  },
  "required": ["users", "pagination"]
}
```

Response Status Codes

Status Code	Description
200	Success
400	Bad Request - Invalid parameters
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

User Status Values

- `active` - User is currently active
- `inactive` - User account is inactive
- `deleted from api` - User was deleted from the source system
- `deleted` - User account has been deleted
- `inconsistent` - User data is in an inconsistent state

MFA Status Values

- `Enabled` - Multi-factor authentication is enabled
- `Disabled` - Multi-factor authentication is disabled
- `Unknown` - MFA status cannot be determined

Example Request

```
curl -X GET "https://public-api.wing.security/v1/users?search_term=john
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response

```
{
  "users": [
    {
      "id": "usr_abc123",
      "name": "John Doe",
      "status": "active",
      "hrStatus": "employed",
```

```
      "jobTitle": "Senior Engineer",
      "reportsTo": "usr_mgr456",
      "organizationalUnit": "Engineering",
      "idpMfaStatus": [
        {
          "connectorName": "okta",
          "status": "Enabled"
        },
        {
          "connectorName": "google",
          "status": "Disabled"
        }
      ],
      "adminIn": ["slack", "github"],
      "tags": ["engineering", "full-time"],
      "applicationsCount": 42
    },
    {
      "id": "usr_def789",
      "name": "Jane Smith",
      "status": "active",
      "hrStatus": "employed",
      "jobTitle": "Product Manager",
      "reportsTo": "usr_dir321",
      "organizationalUnit": "Product",
      "idpMfaStatus": [
        {
          "connectorName": "okta",
          "status": "Enabled"
        }
      ],
      "adminIn": [],
      "tags": ["product", "full-time"],
      "applicationsCount": 28
    }
  ],
  "pagination": {
    "page": 0,
    "pageSize": 50,
    "total": 156
  }
}
```

Get User by ID

`GET /v1/users/{user_id}`

Retrieve detailed information for a specific user by their ID, including accounts and applications.

Path Parameters

Parameter	Type	Required	Description
`user_id`	string	Yes	The ID of the user to retrieve

Response Schema

```
{
  "type": "object",
  "properties": {
    "user": {
      "type": "object",
      "properties": {
        "id": {
          "type": "string",
          "description": "Unique user identifier"
        },
        "name": {
          "type": "string",
          "description": "User's name (may be full name or email addres
        },
        "status": {
          "type": "string",
          "enum": ["active", "inactive", "deleted", "deleted from api",
          "description": "Current user account status"
        },
        "hrStatus": {
          "type": "string",
          "description": "Employment status from HR system"
        },
        "jobTitle": {
          "type": "string",
          "description": "User's job title"
        },
        "reportsTo": {
          "type": "string",
          "description": "User ID of direct manager"
        },
        "organizationalUnit": {
          "type": "string",
          "description": "Organizational unit or department"
        },
        "idpMfaStatus": {
          "type": "array",
          "items": {
            "type": "object",
            "properties": {
              "connectorName": {
                "type": "string",
                "description": "Name of the identity provider connector
              },
              "status": {
                "type": "string",
                "enum": ["Enabled", "Disabled", "Unknown"],
```

```
        "description": "MFA status for this connector"
      }
    }
  },
  "description": "MFA status per identity provider"
},
"adminIn": {
  "type": "array",
  "items": {
    "type": "string"
  },
  "description": "List of connectors where user has admin privi
},
"tags": {
  "type": "array",
  "items": {
    "type": "string"
  },
  "description": "User tags"
},
"applicationsCount": {
  "type": "integer",
  "description": "Total number of applications user has access
},
"accounts": {
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "accountId": {
        "type": "string",
        "description": "Account identifier"
      },
      "connectorName": {
        "type": "string",
        "description": "Name of the connector"
      },
      "primaryEmail": {
        "type": "string",
        "description": "Primary email for this account"
      },
      "isAdmin": {
        "type": "boolean",
        "description": "Whether user is admin in this account"
      },
      "isMfaEnabled": {
        "type": "boolean",
        "description": "Whether MFA is enabled for this account
      }
    }
  },
  "description": "User accounts across connectors"
},
```

```
        "applications": {
          "type": "array",
          "items": {
            "type": "object",
            "properties": {
              "name": {
                "type": "string",
                "description": "Application name"
              }
            }
          },
          "description": "Applications the user has access to"
        }
      },
      "required": ["id"]
    }
  },
  "required": ["user"]
}
```

Response Status Codes

Status Code	Description
200	Success
404	User not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X GET "https://public-api.wing.security/v1/users/usr_abc123" \
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response

```
{
  "user": {
    "id": "usr_abc123",
    "name": "John Doe",
    "status": "active",
    "hrStatus": "employed",
    "jobTitle": "Senior Engineer",
    "reportsTo": "usr_mgr456",
    "organizationalUnit": "Engineering",
    "idpMfaStatus": [
      {
        "connectorName": "okta",
        "status": "Enabled"
```

```
      },
      {
        "connectorName": "google",
        "status": "Disabled"
      }
    ],
    "adminIn": ["slack", "github"],
    "tags": ["engineering", "full-time"],
    "applicationsCount": 42,
    "accounts": [
      {
        "accountId": "acc_123",
        "connectorName": "google",
        "primaryEmail": "john.doe@company.com",
        "isAdmin": false,
        "isMfaEnabled": false
      },
      {
        "accountId": "acc_456",
        "connectorName": "slack",
        "primaryEmail": "john.doe@company.com",
        "isAdmin": true,
        "isMfaEnabled": true
      }
    ],
    "applications": [
      {
        "name": "Slack"
      },
      {
        "name": "GitHub"
      },
      {
        "name": "Google Workspace"
      }
    ]
  }
}
```

Get Apps

`GET /v1/apps`

Retrieve a filtered and paginated list of applications discovered in your organization.

Request Parameters

Parameter	Type	Required	Description
`classification`	string	No	Filter by app classification (Unclassified, Authorized, Internal, Forbidden)
`tags`	array[string]	No	Filter by application tags

`first_seen`	string (date-time)	No	Filter apps discovered after this date (ISO 8601 format)
`last_seen`	string (date-time)	No	Filter apps last seen before this date (ISO 8601 format)
`connectors`	array[string]	No	Filter by connector names where app was discovered
`page`	integer	No	Page number (default: 0)
`page_size`	integer	No	Items per page (default: 50, max: 1000)

Response Schema

```
{
  "type": "object",
  "properties": {
    "apps": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "id": {
            "type": "string",
            "description": "Unique application identifier"
          },
          "name": {
            "type": "string",
            "description": "Application name"
          },
          "categories": {
            "type": "string",
            "description": "Comma-separated list of application categor
          },
          "compliances": {
            "type": "array",
            "items": {
              "type": "string"
            },
            "description": "List of compliance standards (e.g., SOC2, G
          },
          "usersCount": {
            "type": "integer",
            "description": "Number of users with access to this applica
          },
          "firstSeen": {
            "type": "string",
            "format": "date-time",
            "description": "Timestamp when application was first discov
          },
          "lastSeen": {
            "type": "string",
            "format": "date-time",
            "description": "Timestamp when application was last seen"
```

```
      },
      "intelEventsCount": {
        "type": "integer",
        "description": "Number of intelligence/security events asso
      },
      "aiStatus": {
        "type": "string",
        "description": "AI capability status (e.g., AI, AI Integrat
      },
      "classification": {
        "type": "string",
        "enum": ["Unclassified", "Authorized", "Internal", "Forbidd
        "description": "Application classification status"
      },
      "foundInConnectors": {
        "type": "array",
        "items": {
          "type": "object",
          "properties": {
            "connector": {
              "type": "string",
              "description": "Connector name where app was discover
            },
            "permissions": {
              "type": "array",
              "items": {
                "type": "string"
              },
              "description": "List of permissions/scopes granted"
            }
          },
          "required": ["connector", "permissions"]
        },
        "description": "Connectors where this application was disco
      },
      "tags": {
        "type": "array",
        "items": {
          "type": "string"
        },
        "description": "Application tags"
      }
    },
    "required": ["id"]
  }
},
"pagination": {
  "type": "object",
  "properties": {
    "page": {
      "type": "integer",
      "description": "Current page number (zero-indexed)"
    },
```

```
        "pageSize": {
          "type": "integer",
          "description": "Number of items per page"
        },
        "total": {
          "type": "integer",
          "description": "Total number of items across all pages"
        }
      },
      "required": ["page", "pageSize", "total"]
    }
  },
  "required": ["apps", "pagination"]
}
```

Response Status Codes

Status Code	Description
200	Success
400	Bad Request - Invalid parameters
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Classification Values

- `Unclassified` - Application has not been classified
- `Authorized` - Application is authorized for use
- `Internal` - Internal/proprietary application
- `Forbidden` - Application was classified as forbidden for use

Example Request

```
curl -X GET "https://public-api.wing.security/v1/apps?classification=Au
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response

```
{
  "apps": [
    {
      "id": "app_slack_001",
      "name": "Slack",
      "categories": "Communication, Collaboration",
      "compliances": ["SOC2", "GDPR", "ISO27001"],
      "usersCount": 156,
      "firstSeen": "2023-06-15T08:00:00Z",
      "lastSeen": "2024-01-20T16:30:00Z",
      "intelEventsCount": 0,
```

```
    "aiStatus": "AI Integrated",
    "classification": "Authorized",
    "foundInConnectors": [
      {
        "connector": "slack",
        "permissions": ["channels:read", "users:read", "chat:write"]
      }
    ],
    "tags": ["productivity", "approved"]
  },
  {
    "id": "app_github_001",
    "name": "GitHub",
    "categories": "Development, Version Control",
    "compliances": ["SOC2", "ISO27001"],
    "usersCount": 89,
    "firstSeen": "2023-03-10T12:00:00Z",
    "lastSeen": "2024-01-20T17:15:00Z",
    "intelEventsCount": 2,
    "aiStatus": "None",
    "classification": "Authorized",
    "foundInConnectors": [
      {
        "connector": "github",
        "permissions": ["repo", "admin:org", "read:user"]
      }
    ],
    "tags": ["development", "critical"]
  },
  {
    "id": "app_notion_001",
    "name": "Notion",
    "categories": "Productivity, Documentation",
    "compliances": ["SOC2"],
    "usersCount": 234,
    "firstSeen": "2023-08-22T14:20:00Z",
    "lastSeen": "2024-01-21T09:15:00Z",
    "intelEventsCount": 0,
    "aiStatus": "AI",
    "classification": "Authorized",
    "foundInConnectors": [
      {
        "connector": "google",
        "permissions": ["openid", "profile", "email"]
      },
      {
        "connector": "slack",
        "permissions": ["links:read", "links:write"]
      }
    ],
    "tags": ["documentation", "approved"]
  }
],
```

```
  "pagination": {
    "page": 0,
    "pageSize": 20,
    "total": 45
  }
}
```

Get App by ID

```
GET /v1/apps/{app_id}
```

Retrieve detailed information for a specific application by its ID, including comprehensive metadata, security information, and connector details.

Path Parameters

Parameter	Type	Required	Description
`app_id`	string	Yes	The ID of the application to retrieve

Response Schema

```
{
  "type": "object",
  "properties": {
    "app": {
      "type": "object",
      "properties": {
        "id": {
          "type": "string",
          "description": "Unique application identifier"
        },
        "name": {
          "type": "string",
          "description": "Application name"
        },
        "domain": {
          "type": "string",
          "description": "Application domain"
        },
        "status": {
          "type": "string",
          "enum": ["active", "inactive", "deleted from api"],
          "description": "Application status"
        },
        "categories": {
          "type": "string",
          "description": "Comma-separated list of application categorie
        },
        "compliances": {
          "type": "array",
          "items": {
```

```
    "type": "string"
  },
  "description": "List of compliance standards (e.g., SOC2, GDP
},
"usersCount": {
  "type": "integer",
  "description": "Number of users with access to this applicati
},
"firstSeen": {
  "type": "string",
  "format": "date-time",
  "description": "Timestamp when application was first discover
},
"lastSeen": {
  "type": "string",
  "format": "date-time",
  "description": "Timestamp when application was last seen"
},
"discoveredAt": {
  "type": "string",
  "format": "date-time",
  "description": "Timestamp when application was discovered"
},
"intelEventsCount": {
  "type": "integer",
  "description": "Number of intelligence/security events associ
},
"aiStatus": {
  "type": "string",
  "description": "AI capability status (e.g., AI, AI Integrated
},
"aiInfo": {
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "tierName": {
        "type": "string",
        "description": "AI policy tier name"
      },
      "info": {
        "type": "object",
        "properties": {
          "model": {
            "type": "string",
            "description": "AI model information"
          },
          "updatedAt": {
            "type": "string",
            "format": "date-time",
            "description": "When AI policy was last updated"
          },
          "dataRetentionPeriod": {
```

```
            "type": "string",
            "description": "Data retention period"
          },
          "userDataTrainsModel": {
            "type": "string",
            "description": "Whether user data trains the model"
          },
          "humansReviewCustomerData": {
            "type": "string",
            "description": "Whether humans review customer data
          },
          "optionToConfigureTraining": {
            "type": "string",
            "description": "Options to configure training"
          },
          "optionToConfigureRetention": {
            "type": "string",
            "description": "Options to configure data retention
          },
          "userDataTrainsModelCategory": {
            "type": "string",
            "description": "Category of user data training"
          },
          "userDataTrainsModelRawText": {
            "type": "string",
            "description": "Raw text about user data training"
          },
          "humansReviewCustomerDataCategory": {
            "type": "string",
            "description": "Category of human review of custome
          }
        }
      }
    }
  },
  "description": "Detailed AI policy information"
},
"classification": {
  "type": "string",
  "enum": ["Unclassified", "Authorized", "Internal", "Forbidden
  "description": "Application classification status"
},
"foundInConnectors": {
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "connector": {
        "type": "string",
        "description": "Connector name where app was discovered
      },
      "permissions": {
        "type": "array",
```

```
        "items": {
          "type": "string"
        },
        "description": "List of permissions/scopes granted"
      }
    },
    "required": ["connector", "permissions"]
  },
  "description": "Connectors where this application was discove
},
"tags": {
  "type": "array",
  "items": {
    "type": "string"
  },
  "description": "Application tags"
},
"isConnected": {
  "type": "boolean",
  "description": "Whether the application is connected"
},
"externalUsersCount": {
  "type": "integer",
  "description": "Number of external users with access"
},
"internalUsersCount": {
  "type": "integer",
  "description": "Number of internal users with access"
},
"foundInConnectorsCount": {
  "type": "integer",
  "description": "Number of connectors where this app was found
},
"connectorAppsIds": {
  "type": "array",
  "items": {
    "type": "string"
  },
  "description": "List of connector application IDs"
},
"connectors": {
  "type": "array",
  "items": {
    "type": "string"
  },
  "description": "List of connector names"
},
"thirdPartyAppsCount": {
  "type": "integer",
  "description": "Number of third-party apps connected"
},
"reputationScore": {
  "type": "number",
```

```
          "format": "float",
          "description": "Application reputation score"
        },
        "apiKeysCount": {
          "type": "integer",
          "description": "Number of API keys for this application"
        },
        "isUnknown": {
          "type": "boolean",
          "description": "Whether the application is unknown"
        },
        "isInactive": {
          "type": "boolean",
          "description": "Whether the application is inactive"
        },
        "isWorkspaceConnected": {
          "type": "boolean",
          "description": "Whether the application is workspace connecte
        },
        "hasHighScopes": {
          "type": "boolean",
          "description": "Whether the application has high-risk scopes/
        },
        "compliancesCount": {
          "type": "integer",
          "description": "Number of compliance standards met"
        },
        "country": {
          "type": "string",
          "description": "Country where the application is based"
        },
        "description": {
          "type": "string",
          "description": "Application description"
        },
        "companySize": {
          "type": "string",
          "description": "Size of the company that makes the applicatio
        },
        "riskRank": {
          "type": "integer",
          "nullable": true,
          "description": "Risk rank (0 being highest risk, null means n
        }
      },
      "required": ["id"]
    }
  },
  "required": ["app"]
}
```


Response Status Codes

Status Code	Description
200	Success
404	Application not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Application Status Values

- `active` - Application is currently active
- `inactive` - Application is inactive
- `deleted from api` - Application was deleted from the source system

Example Request

```
curl -X GET "https://public-api.wing.security/v1/apps/app_slack_001" \
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response


```
{
  "app": {
    "id": "app_slack_001",
    "name": "Slack",
    "domain": "slack.com",
    "status": "active",
    "categories": "Communication, Collaboration",
    "compliances": ["SOC2", "GDPR", "ISO27001"],
    "usersCount": 156,
    "firstSeen": "2023-06-15T08:00:00Z",
    "lastSeen": "2024-01-20T16:30:00Z",
    "discoveredAt": "2023-06-15T08:00:00Z",
    "intelEventsCount": 0,
    "aiStatus": "AI Integrated",
    "aiInfo": [
      {
        "tierName": "Enterprise",
        "info": {
          "model": "Claude, GPT-4",
          "updatedAt": "2024-01-15T00:00:00Z",
          "dataRetentionPeriod": "90 days",
          "userDataTrainsModel": "No",
          "humansReviewCustomerData": "No",
          "optionToConfigureTraining": "Yes",
          "optionToConfigureRetention": "Yes",
          "userDataTrainsModelCategory": "Not Used",
          "userDataTrainsModelRawText": "User data is not used for trai
          "humansReviewCustomerDataCategory": "Not Reviewed"
        }
```

```
      }
    ],
    "classification": "Authorized",
    "foundInConnectors": [
      {
        "connector": "slack",
        "permissions": ["channels:read", "users:read", "chat:write", "f
      }
    ],
    "tags": ["productivity", "approved", "communication"],
    "isConnected": true,
    "externalUsersCount": 12,
    "internalUsersCount": 144,
    "foundInConnectorsCount": 1,
    "connectorAppsIds": ["slack_workspace_001"],
    "connectors": ["slack"],
    "thirdPartyAppsCount": 5,
    "reputationScore": 8.5,
    "apiKeysCount": 3,
    "isUnknown": false,
    "isInactive": false,
    "isWorkspaceConnected": true,
    "hasHighScopes": true,
    "compliancesCount": 3,
    "country": "United States",
    "description": "Slack is a cloud-based collaboration platform that
    "companySize": "1000+",
    "riskRank": null
  }
}
```

Get Issues

`GET /v1/issues`

Retrieve a filtered, sorted, and paginated list of security issues detected in your organization.

Request Parameters

Parameter	Type	Required	Description
`severity`	string	No	Filter by issue severity (low, medium, high, critical)
`issue_type`	string	No	Filter by issue type/rule
`user_id`	string	No	Filter by specific user ID
`status`	array[string]	No	Filter by issue status (open, in_progress, dismissed, resolved)
`sortBy`	string	No	Field to sort by (status, severity, issueType, detectedAt, userId)
`sortDir`	string	No	Sort direction (asc, desc) - default: desc
`page`	integer	No	Page number (default: 0)

`page_size`	integer	No	Items per page (default: 50, max: 1000)

Response Schema

```
{
  "type": "object",
  "properties": {
    "issues": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "id": {
            "type": "string",
            "description": "Unique issue identifier"
          },
          "title": {
            "type": "string",
            "description": "Issue title"
          },
          "description": {
            "type": "string",
            "description": "Detailed description of the issue"
          },
          "severity": {
            "type": "string",
            "enum": ["low", "medium", "high", "critical"],
            "description": "Issue severity level"
          },
          "status": {
            "type": "string",
            "enum": ["open", "in_progress", "dismissed", "resolved"],
            "description": "Current issue status"
          },
          "userId": {
            "type": "string",
            "description": "ID of the user associated with this issue"
          },
          "mitreAttackTactic": {
            "type": "string",
            "description": "MITRE ATT&CK tactic (e.g., credential_acces
          },
          "detectedAt": {
            "type": "string",
            "format": "date-time",
            "description": "When the issue was first detected"
          },
          "updatedAt": {
            "type": "string",
            "format": "date-time",
            "description": "When the issue was last updated"
          }
```

```
        },
        "required": ["id"]
      }
    },
    "pagination": {
      "type": "object",
      "properties": {
        "page": {
          "type": "integer",
          "description": "Current page number (zero-indexed)"
        },
        "pageSize": {
          "type": "integer",
          "description": "Number of items per page"
        },
        "total": {
          "type": "integer",
          "description": "Total number of items across all pages"
        }
      },
      "required": ["page", "pageSize", "total"]
    }
  },
  "required": ["issues", "pagination"]
}
```

Response Status Codes

Status Code	Description
200	Success
400	Bad Request - Invalid parameters
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Severity Values

- `low` - Low severity issue
- `medium` - Medium severity issue
- `high` - High severity issue
- `critical` - Critical severity issue requiring immediate attention

Status Values

- `open` - Issue is newly detected and needs attention
- `in_progress` - Issue is being investigated or remediated
- `dismissed` - Issue has been dismissed as acceptable risk
- `resolved` - Issue has been resolved

MITRE ATT&CK Tactics

Issues are mapped to MITRE ATT&CK tactics including:

- `reconnaissance`, `resource_development`, `initial_access`
- `execution`, `persistence`, `privilege_escalation`
- `defense_evasion`, `credential_access`, `discovery`
- `lateral_movement`, `collection`, `command_and_control`
- `exfiltration`, `impact`

Example Request

```
curl -X GET "https://public-api.wing.security/v1/issues?severity=high&s
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response


```
{
  "issues": [
    {
      "id": "issue_abc123",
      "title": "User with admin privileges has MFA disabled",
      "description": "Admin user john.doe@company.com does not have mul
      "severity": "high",
      "status": "open",
      "userId": "usr_abc123",
      "mitreAttackTactic": "credential_access",
      "detectedAt": "2024-01-20T15:30:00Z",
      "updatedAt": "2024-01-20T15:30:00Z"
    },
    {
      "id": "issue_def456",
      "title": "Suspicious OAuth application with excessive permissions
      "description": "Third-party application 'DataExporter' has been g
      "severity": "high",
      "status": "in_progress",
      "userId": "usr_def789",
      "mitreAttackTactic": "initial_access",
      "detectedAt": "2024-01-19T10:15:00Z",
      "updatedAt": "2024-01-20T09:00:00Z"
    }
  ],
  "pagination": {
    "page": 0,
    "pageSize": 20,
    "total": 47
  }
}
```

Get Issue by ID

```
GET /v1/issues/{issue_id}
```

Retrieve detailed information for a specific issue by its ID.

Path Parameters

Parameter	Type	Required	Description
`issue_id`	string	Yes	The ID of the issue to retrieve

Response Schema

```
{
  "type": "object",
  "properties": {
    "issue": {
      "type": "object",
      "properties": {
        "id": {
          "type": "string",
          "description": "Unique issue identifier"
        },
        "title": {
          "type": "string",
          "description": "Issue title"
        },
        "description": {
          "type": "string",
          "description": "Detailed description of the issue"
        },
        "severity": {
          "type": "string",
          "enum": ["low", "medium", "high", "critical"],
          "description": "Issue severity level"
        },
        "status": {
          "type": "string",
          "enum": ["open", "in_progress", "dismissed", "resolved"],
          "description": "Current issue status"
        },
        "userId": {
          "type": "string",
          "description": "ID of the user associated with this issue"
        },
        "mitreAttackTactic": {
          "type": "string",
          "description": "MITRE ATT&CK tactic"
        },
        "detectedAt": {
          "type": "string",
          "format": "date-time",
          "description": "When the issue was first detected"
        },
        "updatedAt": {
          "type": "string",
```

```
          "format": "date-time",
          "description": "When the issue was last updated"
        }
      },
      "required": ["id"]
    }
  },
  "required": ["issue"]
}
```

Response Status Codes

Status Code	Description
200	Success
404	Issue not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X GET "https://public-api.wing.security/v1/issues/issue_abc123" \
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response

```
{
  "issue": {
    "id": "issue_abc123",
    "title": "User with admin privileges has MFA disabled",
    "description": "Admin user john.doe@company.com does not have multi
    "severity": "high",
    "status": "open",
    "userId": "usr_abc123",
    "mitreAttackTactic": "credential_access",
    "detectedAt": "2024-01-20T15:30:00Z",
    "updatedAt": "2024-01-20T15:30:00Z"
  }
}
```

Update Issue

`PATCH /v1/issues/{issue_id}`

Update an issue's status (e.g., mark as in progress, resolved, or dismissed).

Path Parameters

Parameter	Type	Required	Description
`issue_id`	string	Yes	The ID of the issue to update

Request Body

```
{
  "type": "object",
  "properties": {
    "status": {
      "type": "string",
      "enum": ["open", "in_progress", "dismissed", "resolved"],
      "description": "New status for the issue"
    }
  },
  "required": ["status"]
}
```

Response Status Codes

Status Code	Description
200	Issue updated successfully
400	Bad Request - Invalid status value
404	Issue not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X PATCH "https://public-api.wing.security/v1/issues/issue_abc123"
  -H "x-api-key: YOUR_API_TOKEN" \
  -H "Content-Type: application/json" \
  -d '{
    "status": "in_progress"
  }'
```

Example Response

```
{
  "message": "Issue updated successfully"
}
```

Get Connections

`GET /v1/connections`

Retrieve a filtered and paginated list of OAuth/API connections between users and third-

party applications.

Request Parameters

Parameter	Type	Required	Description
source_app_id	string	No	Filter by source application ID
target_app_id	string	No	Filter by target application ID
scopes	array[string]	No	Filter by OAuth scopes/permissions granted
connector_name	string	No	Filter by connector name (e.g., google, office365)
token_type	string	No	Filter by token type
classification	string	No	Filter by app classification (Unclassified, Authorized, Internal, Forbidden)
is_external_user	boolean	No	Filter by external user status
reputation_score_min	number	No	Minimum reputation score filter
reputation_score_max	number	No	Maximum reputation score filter
revoked	boolean	No	Filter by revocation status
page	integer	No	Page number (default: 0)
page_size	integer	No	Items per page (default: 50, max: 1000)

Response Schema

```
{
  "type": "object",
  "properties": {
    "connections": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "userId": {
            "type": "string",
            "description": "User ID who authorized the connection"
          },
          "connectionId": {
            "type": "string",
            "description": "Unique connection identifier"
          },
          "connectorName": {
            "type": "string",
            "description": "Name of the connector (e.g., google, office
          },
          "sourceAppId": {
            "type": "string",
            "description": "Source application ID"
          },
          "targetAppId": {
            "type": "string",
```

```
            "description": "Target application ID"
          },
          "scopes": {
            "type": "array",
            "items": {
              "type": "object",
              "properties": {
                "name": {
                  "type": "string",
                  "description": "OAuth scope name"
                },
                "description": {
                  "type": "string",
                  "description": "Human-readable scope description"
                }
              }
            },
            "description": "OAuth scopes/permissions granted to the app
          },
          "revoked": {
            "type": "boolean",
            "description": "Whether the connection has been revoked"
          }
        }
      }
    },
    "pagination": {
      "type": "object",
      "properties": {
        "page": {
          "type": "integer",
          "description": "Current page number (zero-indexed)"
        },
        "pageSize": {
          "type": "integer",
          "description": "Number of items per page"
        },
        "total": {
          "type": "integer",
          "description": "Total number of items across all pages"
        }
      },
      "required": ["page", "pageSize", "total"]
    }
  },
  "required": ["connections", "pagination"]
}
```

Response Status Codes

Status Code	Description
200	Success

400	Bad Request - Invalid parameters
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X GET "https://public-api.wing.security/v1/connections?revoked=fa
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response


```
{
  "connections": [
    {
      "userId": "usr_abc123",
      "connectionId": "conn_xyz789",
      "connectorName": "google",
      "sourceAppId": "app_workspace_001",
      "targetAppId": "app_slack_001",
      "scopes": [
        {
          "name": "https://www.googleapis.com/auth/userinfo.email",
          "description": "View your email address"
        },
        {
          "name": "https://www.googleapis.com/auth/userinfo.profile",
          "description": "View your basic profile info"
        }
      ],
      "revoked": false
    }
  ],
  "pagination": {
    "page": 0,
    "pageSize": 20,
    "total": 156
  }
}
```

Get App Connections

```
GET /v1/apps/{app_id}/connections
```

Retrieve all connections associated with a specific application, where the app is either the source or target of the connection.

Path Parameters

Parameter	Type	Required	Description
`app_id`	string	Yes	The ID of the application

Request Parameters

Parameter	Type	Required	Description
`direction`	string	No	Filter by connection direction (source, target, or both)
`page`	integer	No	Page number (default: 0)
`page_size`	integer	No	Items per page (default: 50, max: 1000)

Response Schema

Same as **Get Connections** endpoint.

Response Status Codes

Status Code	Description
200	Success
404	Application not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X GET "https://public-api.wing.security/v1/apps/app_slack_001/con
  -H "x-api-key: YOUR_API_TOKEN"
```

Revoke Connection

`POST /v1/connections/{connectionId}/revoke`

Revoke a specific OAuth connection's access token. This immediately invalidates the connection and removes the application's access to user data.

Path Parameters

Parameter	Type	Required	Description
`connectionId`	string	Yes	The ID of the connection to revoke

Request Body

```
{
  "type": "object",
  "properties": {
```

```
    "userId": {
      "type": "string",
      "description": "User ID associated with the connection"
    }
  },
  "required": ["userId"]
}
```

Response Schema

```
{
  "type": "object",
  "properties": {
    "connectionId": {
      "type": "string",
      "description": "The revoked connection ID"
    },
    "userId": {
      "type": "string",
      "description": "The user ID associated with the connection"
    }
  },
  "required": ["connectionId", "userId"]
}
```

Response Status Codes

Status Code	Description
200	Connection revoked successfully
404	Connection not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X POST "https://public-api.wing.security/v1/connections/conn_xyz7
  -H "x-api-key: YOUR_API_TOKEN" \
  -H "Content-Type: application/json" \
  -d '{
    "userId": "usr_abc123"
  }'
```

Example Response

```
{
  "connectionId": "conn_xyz789",
  "userId": "usr_abc123"
}
```

Bulk Revoke Connections

`POST /v1/connections/revoke`

Revoke multiple OAuth connections in a single request. Useful for bulk operations during security incidents or compliance requirements.

Request Body

```
{
  "type": "object",
  "properties": {
    "revokes": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "connectionId": {
            "type": "string",
            "description": "Connection ID to revoke"
          },
          "userId": {
            "type": "string",
            "description": "User ID associated with the connection"
          }
        },
        "required": ["connectionId", "userId"]
      }
    }
  },
  "required": ["revokes"]
}
```

Response Schema

```
{
  "type": "object",
  "properties": {
    "results": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "connectionId": {
            "type": "string",
            "description": "The connection ID"
          },
          "userId": {
            "type": "string",
            "description": "The user ID"
          },
```

```
          "revoked": {
            "type": "boolean",
            "description": "Whether revocation was successful"
          },
          "error": {
            "type": "string",
            "description": "Error message if revocation failed"
          }
        },
        "required": ["connectionId", "userId", "revoked"]
      }
    }
  },
  "required": ["results"]
}
```

Response Status Codes

Status Code	Description
200	Bulk revocation completed (check individual results for success/failure)
400	Bad Request - Invalid request body
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X POST "https://public-api.wing.security/v1/connections/revoke" \
  -H "x-api-key: YOUR_API_TOKEN" \
  -H "Content-Type: application/json" \
  -d '{
    "revokes": [
      {
        "connectionId": "conn_xyz789",
        "userId": "usr_abc123"
      },
      {
        "connectionId": "conn_abc456",
        "userId": "usr_def456"
      }
    ]
  }'
```

Example Response

```
{
  "results": [
    {
      "connectionId": "conn_xyz789",
```

```
      "userId": "usr_abc123",
      "revoked": true
    },
    {
      "connectionId": "conn_abc456",
      "userId": "usr_def456",
      "revoked": false,
      "error": "Token already revoked"
    }
  ]
}
```

Revoke App Connections

`POST /v1/apps/{app_id}/connections/revoke`

Revoke all OAuth connections for a specific application. This is useful for removing access when an application is identified as malicious or unauthorized.

Path Parameters

Parameter	Type	Required	Description
`app_id`	string	Yes	The ID of the application whose connections should be revoked

Request Body

No request body required.

Response Schema

```
{
  "type": "object",
  "properties": {
    "appId": {
      "type": "string",
      "description": "The application ID"
    },
    "totalProcessed": {
      "type": "integer",
      "description": "Total number of connections processed"
    },
    "revokedCount": {
      "type": "integer",
      "description": "Number of connections successfully revoked"
    },
    "alreadyRevokedCount": {
      "type": "integer",
      "description": "Number of connections that were already revoked"
    },
    "results": {
      "type": "array",
```

```
      "items": {
        "type": "object",
        "properties": {
          "connectionId": {
            "type": "string"
          },
          "userId": {
            "type": "string"
          },
          "revoked": {
            "type": "boolean"
          },
          "error": {
            "type": "string"
          }
        }
      },
      "description": "Detailed results for each connection"
    }
  },
  "required": ["appId", "totalProcessed", "revokedCount", "alreadyRevok
}
```

Response Status Codes

Status Code	Description
200	App connections revocation completed (check results for details)
404	Application not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X POST "https://public-api.wing.security/v1/apps/app_malicious_00
  -H "x-api-key: YOUR_API_TOKEN"
```

Example Response

```
{
  "appId": "app_malicious_001",
  "totalProcessed": 15,
  "revokedCount": 14,
  "alreadyRevokedCount": 1,
  "results": [
    {
      "connectionId": "conn_001",
      "userId": "usr_abc123",
      "revoked": true
```

```
    },
    {
      "connectionId": "conn_002",
      "userId": "usr_def456",
      "revoked": true
    }
  ]
}
```

Revoke User Connections

`POST /v1/users/{user_id}/connections/revoke`

Revoke all OAuth connections for a specific user. This is useful during offboarding or when a user's account may be compromised.

Path Parameters

Parameter	Type	Required	Description
`user_id`	string	Yes	The ID of the user whose connections should be revoked

Request Body

No request body required.

Response Schema

Same format as **Revoke App Connections** endpoint.

Response Status Codes

Status Code	Description
200	User connections revocation completed (check results for details)
404	User not found
401	Unauthorized - Missing or invalid authentication
403	Forbidden - Insufficient permissions
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error

Example Request

```
curl -X POST "https://public-api.wing.security/v1/users/usr_abc123/conn
  -H "x-api-key: YOUR_API_TOKEN"
```

Error Responses

Application Error Responses

Application-level errors returned by the Wing Public API follow this format:

```
{
  "status": "ERROR_TYPE",
  "detail": "Human-readable error description"
}
```

Common Application Error Types:

- `BAD_REQUEST_ERROR` - Invalid request parameters
- `NOT_FOUND_ERROR` - Resource not found

Example:

```
{
  "status": "BAD_REQUEST_ERROR",
  "detail": "Invalid page_size parameter: must be between 1 and 1000"
}
```

Gateway Error Responses

Infrastructure-level errors returned by AWS API Gateway follow a different format:

```
{
  "message": "Error description"
}
```

Common Gateway Error Types:

Status Code	Error Type	Description
401	Unauthorized	Missing or invalid authentication
403	Forbidden	Insufficient permissions or invalid API key
413	Request Too Large	Request payload exceeds size limit
415	Unsupported Media Type	Content-Type not supported
429	Too Many Requests	Rate limit exceeded
504	Gateway Timeout	Request timeout

Example:

```
{
  "message": "Missing Authentication Token"
}
```

Rate Limiting

The Wing Public API implements throttling limits to ensure optimal performance and fair usage across all clients.

Limits

- **Rate Limit**: 100 requests per second (RPS)
- **Burst Limit**: 200 concurrent requests

How Rate Limiting Works

The API uses a **token bucket algorithm** where each request consumes one token:

1. **Steady-State Rate**: Tokens replenish at 10,000 per second
2. **Burst Capacity**: Allows temporary traffic spikes up to 5,000 concurrent requests
3. **Throttling Response**: When limits are exceeded, the API returns HTTP `429 Too Many Requests`

Important Notes

- Limits apply to **all users collectively** by default
- Throttling is applied on a best-effort basis
- For higher limits or dedicated quotas, contact Wing Security Customer Success