

INTEGRITI Operator Authentication Modules

INNERRANGE.COM

CONTENTS

CONTENTS 2
PURPOSE 3
INTEGRITI AUTHENTICATION MODULE REQUIREMENTS 4
Licensing Requirements 4
Pre-requisites/System Requirements 4
AUTHENTICATION SYSTEM CONFIGURATION 5
OAuth Authentication Configuration 5
INTEGRITI CONFIGURATION 6
Authentication Module Configuration 6
Built-In Authentication 6
Windows Active Directory Authentication 6
External Authentication Provider Configuration 7
OAuth Authentication 7
External Authentication Provider Configuration 7
Operator Configuration 9
Operator Type Authentication Configuration 10
OPERATOR LOGIN 11
TROUBLESHOOTING 12
Unable to log on: Authentication scheme not licensed 12
Unable to log on using Active Directory: The server is not operational 12
Unable to log on using Active Directory: Current security context is not associated with an Active Directory domain or forest 12
Unable to log on using OAuth: Unknown operator or incorrect password 12

Copyright © Inner Range PTY LTD January 2025

PURPOSE

Integriti's Operator Authentication Modules allow the system used to authenticate Operators logging into Integriti against. This allows Operator authentication to be managed entirely by Integriti or handled by an external authentication service to centralise Operator credential across multiple systems. The following Authentication Modules are supported for Integriti's Operator authentication.

- **Built-In Authentication:** Integriti's built-in authentication module allows for all Operator authentication to be managed entirely by Integriti. Operator credentials are stored and updated directly in the Integriti database.
- **Windows Active Directory Authentication:** The Active Directory authentication module allows Operators to be authenticated against a Windows Active Directory domain, allowing Windows credentials to be used to log into an Integriti system. Operator credentials can be authenticated against either the current, or a manually specified alternative Active Directory domain, depending on the system's requirements.
- **OAuth Authentication:** The OAuth authentication module allows Operators to be authenticated against a compatible OAuth authentication server. This is compatible with systems that support OpenID Connect 1.0 and OpenID Connect Discovery 1.0, such as Okta and Microsoft Entra ID.

Copyright © Inner Range PTY LTD January 2025

INTEGRITI AUTHENTICATION MODULE REQUIREMENTS

Licensing Requirements

Integriti's built-in authentication module is included with all versions of Integriti.

All authentication modules that authenticate against an external authentication system require Integriti Business Edition or higher. Systems using Integriti Business Edition or higher can authenticate an unlimited number of users against supported external authentication systems.

Pre-requisites/System Requirements

The only system requirement for Integriti's authentication modules is for all Integriti Application Servers to be able to communicate with the authentication system that Operators are to be authenticated against. For Integriti systems authenticating against external authentication systems, this will require the necessary network access and ports to be opened between the two systems.

Copyright © Inner Range PTY LTD January 2025

AUTHENTICATION SYSTEM CONFIGURATION

OAuth Authentication systems typically require some additional configuration to enable Integriti Operator authentication. See below for further details. Built-in and Windows Active Directory authentication modules typically require no additional configuration in the authentication system.

OAuth Authentication Configuration

Configuration of OAuth systems varies from system to system, however the typical options requiring enabling are below:

- **Create an Application:** In order for Integriti to authenticate Operators against an OAuth authentication system, an 'Application' must be created in the OAuth system representing the integration with Integriti's OAuth authentication module.
- **Retrieve Issuer:** The Issuer URL for the authentication system should be retrieved for the Integriti configuration. This is typically found either in the OAuth System's configuration, or in the created Application's configuration, and takes the form of a URL to the authentication system.
- **Retrieve Client ID:** Once an Application has been created, take note of the 'Client ID' or 'Audience' assigned to the Application – this will be used in the Integriti configuration.
- **Client Secret:** Enable 'Client Secret Authentication' in the OAuth system and take note of the generated Client Secret to use in the Integriti configuration.
  NOTE: Some OAuth systems only make the Client Secret visible when it is first created. Make sure to take note of the Client Secret as soon as it is generated to ensure it isn't lost prior to configuring the OAuth Authentication module in Integriti.
- **Password Flow:** If using the Legacy OAuth Authentication module as configured in previous versions of Integriti, ensure the OAuth Resource Owner Password flow is enabled for the OAuth system. This allows Integriti to securely authenticate against the OAuth system.
  NOTE: In Integriti 24.1 and above, this is not necessary when configuring a new system.
- **Assign Users:** Assign Users in the OAuth system to be used to authenticate Integriti Operators against to the Application that was created. Users who haven't been assigned to the correct Application in the OAuth system cannot be used to authenticate Integriti Operators against.
- **Configure the Application to provide the groups claim:** With some providers, in order to automatically assign Operator Types or create new Operator accounts in Integriti, it may be necessary to configure the Application to allow Integriti to receive the groups claim. For more details, see the provider's documentation.

Copyright © Inner Range PTY LTD January 2025

INTEGRITI CONFIGURATION

Authentication Module Configuration

NOTE: For systems using Active Directory or OAuth authentication, it is recommended to leave Built-In Authentication enabled at least until AD/OAuth Operators have been tested, if not permanently. If Built-In authentication is disabled prior to correctly configuring AD/OAuth Operators, or if connection to the external authentication system is lost, this can result in a permanent lock-out of the Integriti Software.

Authentication modules can be configured from Integriti's System Settings. Open Integriti's System Settings and configure as below.



Built-In Authentication

Integriti's built-in authentication module is enabled by default for all Integriti installations. Built-in authentication can be optionally disabled, and re-enabled, through the 'Allow Built-In Authentication' option in the System Settings.

Windows Active Directory Authentication

Windows Active Directory Authentication can be enabled and disabled with the 'Allow Active Directory Authentication' option above. Enabling this option will show additional general options for configuring the Active Directory Authentication module.



Allow Login With Current Windows User: Enabling this option allows an Operator to log directly into Integriti using the credentials of the Windows User they are currently logged in with. This allows Operators to log in without the need to manually type in any credentials. See Operator Login for more details on using this option.

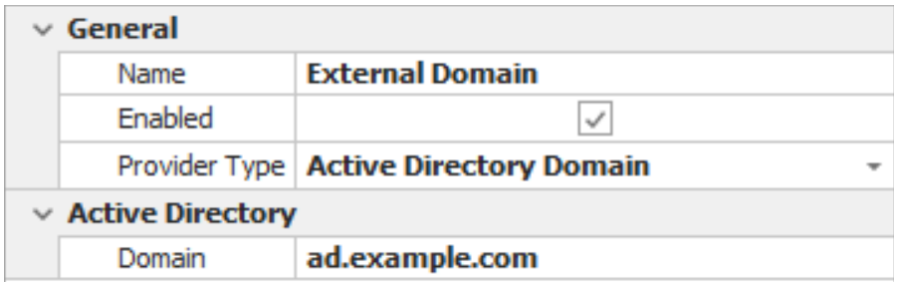
Use User Credentials to Connect to Extra Domains: If enabled, the connection to additional Active Directory domains to authenticate against will be established using the credentials of the Windows User currently attempting to log into Integriti. This requires the Windows User to have permission to connect to the AD domain in question and read User data.
If disabled, the connection to all Active Directory domains to authenticate against will be established using the User the Integriti Application server is running as. This requires an appropriate trust relationship between this User and the Active Directory domain being authenticated against. Authentication against the current domain will always be done using the User the Integriti Application server is running as.

Copyright © Inner Range PTY LTD January 2025

Additional AD Domains: To specify alternative Active Directory domains to attempt to authenticate Operators against, use the External Authentication Providers list in the Authentication section.

When using Active Directory authentication. Integriti will always attempt to authenticate Operators against the current AD domain that the Integriti server PC is connected to. Domains specified there will be authenticated against in addition to the current AD domain.

External Authentication Provider Configuration



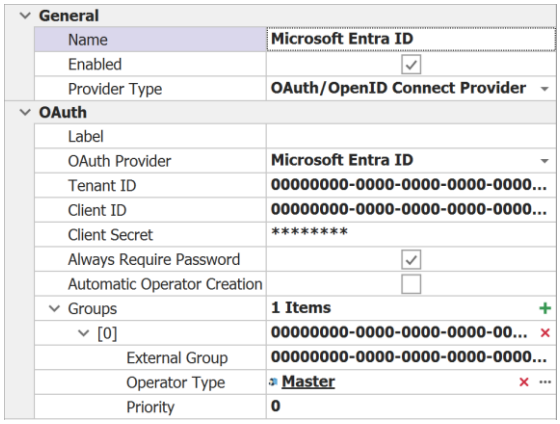
Domain: Specify the domain name to be used for Active Directory authentication.

OAuth Authentication

OAuth Authentication can be enabled and disabled with the 'Allow OAuth Authentication' option above.

To specify the OAuth provider configuration or access the legacy OAuth module configuration, use the External Authentication Providers list in the Authentication section.

External Authentication Provider Configuration



Label: Specify the label that will be shown for this provider in the 'Log in with' list in the login dialog in System Designer and GateKeeper, and the Integriti web interface login page.

OAuth Provider: Select the OAuth provider to use if it is one of the supported providers listed below, or select Custom to use a different provider.

- Microsoft Entra ID

Copyright © Inner Range PTY LTD January 2025

- Google
- Okta
- Custom (specified issuer URL)

Tenant ID: If using Microsoft Entra ID, specify the tenant ID of your Entra ID app.

Okta Domain: If using Okta, specify the full Okta domain name to authenticate against.

Issuer URL: If using a Custom OAuth provider, specify the Issuer URL from the OAuth system to authenticate against. This can be found in the OAuth system configuration, typically either in the configuration for the authentication system itself, or in the configuration for the Application (as created in 'Authentication System Configuration – OAuth Authentication Configuration').

Client ID: Specify the Client ID (sometimes called the Audience) for the Application created in the OAuth system. This can typically be found in the configuration for the Application.

Client Secret: Specify the Client Secret created in the OAuth system's Application when configuring Client Secret authentication for the Application. It is worth noting that on some systems, the Client Secret is only visible when first created, so ensure to take note of it as soon as Client Secret authentication is configured.
NOTE: Some systems require that Client Secrets expire or are changed at a regular frequency. Ensure that this property is updated whenever the client secret is updated in the OAuth system. If Built-In authentication is disabled and the OAuth client secret becomes invalid, this can result in a permanent lock-out of the Integriti Software.

Always Require Password: Select this to request that the OAuth provider force the user to verify their password on each authorisation attempt. If this is not selected, and the user already has a logged-in session with the external provider, the provider may skip the login page and immediately return to Integriti using the existing session.

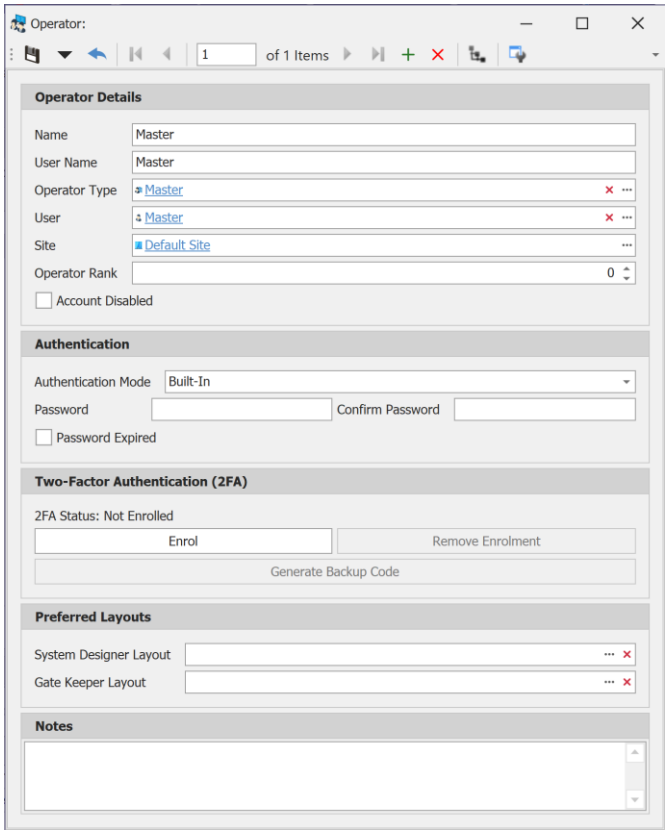
Automatic Operator Creation: Select this to allow a new Operator account to be automatically created for an unknown user logging in using OAuth, if they are a member of an external group associated with an Operator Type below.

Groups: Assign Operator Types to groups on the external system for use when automatically creating or updating an Operator account.

Copyright © Inner Range PTY LTD January 2025

Operator Configuration

Prior to logging in to Integriti using any of the Authentication modules, Operators must first be configured for each person who needs to log into the system (except for Active Directory and OAuth Operator Type authentication, see below). Operators can be created from the Add New button in the Operators list in System Designer.



Name: The name of the Operator.

User Name: The username used to log in to this Operator account. When using Active Directory or OAuth authentication, this must match the username on the external system. It must be unique among all Operators using a particular OAuth provider, or all Operators not using the OAuth authentication module.

Operator Type: Select the Operator Type that should define permissions for the Operator.

User: Select the Integriti User that represents this Operator, if applicable.

Authentication Mode: Choose the authentication module or OAuth provider that this Operator should use to log in.

Password: If using the built-in authentication module, enter and confirm a password for the new Operator.

Password Expired: Select to require the Operator to change their password when logging in.

Copyright © Inner Range PTY LTD January 2025

OAuth Status: Shows whether a stored OpenID user identifier exists for this operator. This happens when the operator has successfully signed in, and allows the username to be changed while still allowing the user to sign in subsequently.

Once saved, this Operator will be able to log into Integriti with the given username.

Operator Type Authentication Configuration

When using the Active Directory authentication module, it is possible to allow validation of AD users against an Operator Type based on their AD group membership. This allows Operators to be automatically created in Integriti under a given Operator Type for all AD Users in a specified AD group, saving the need to manually create an Operator for all AD Users who need to log into Integriti.

Enabling this option is as simple as setting the 'Active Directory Group' property of an Operator Type to the name of the AD Group to be associated with that Operator Type. AD Users attempting to log into Integriti without an Operator already created in the system will have an Operator automatically created in the corresponding Operator Type, if they are a member of the AD Group specified.

When using the OAuth authentication module in Integriti 24.1 or higher, it is possible to allow validation of external users against groups defined by the external system similarly.

To use this option, ensure that the external Application is configured to provide the groups claim in ID tokens. This configuration varies depending on the provider. The label identifying a group on the external system, along with the associated Operator Type, should be listed under the OAuth Provider in System Settings; what this group label is depends on the provider, but will be logged to Integriti Review in the event of an unsuccessful OAuth login.

See the following pages for more information on configuring OpenID Connect applications to provide a groups claim:

- Microsoft Entra ID: Configure optional claims
- Okta: Customize tokens returned from Okta with a groups claim

Copyright © Inner Range PTY LTD January 2025

OPERATOR LOGIN

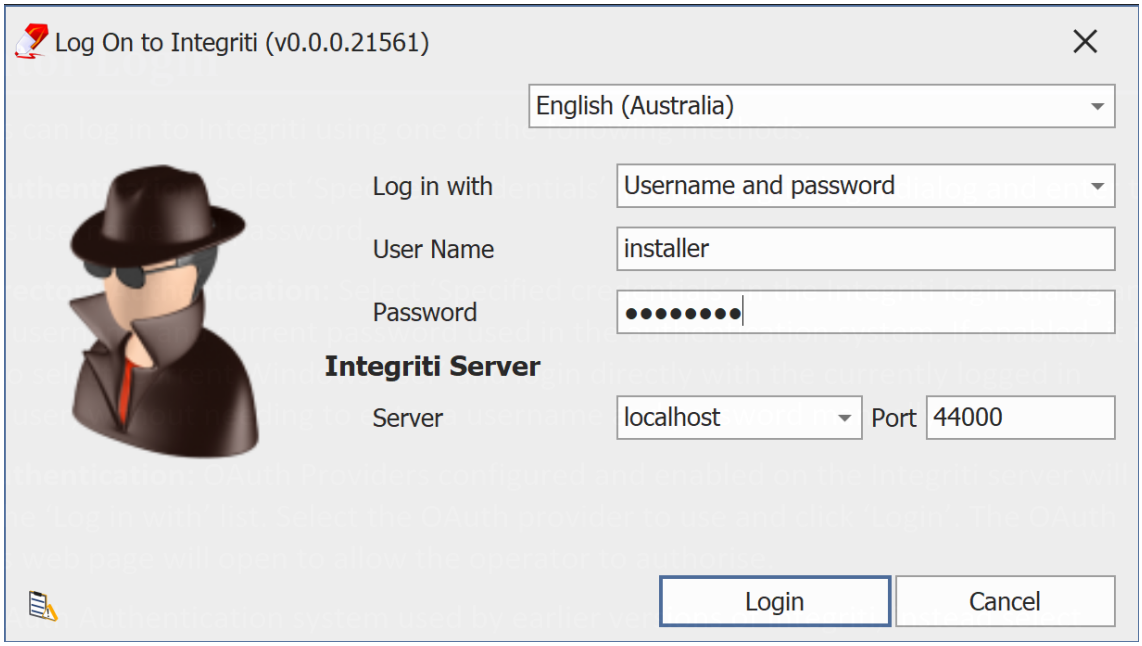
Operators can log in to Integriti using one of the following methods.

Built-In Authentication: Select 'Username and password' in the Integriti login dialog and enter the operator's username and password.

Active Directory Authentication: Select 'Username and password' in the Integriti login dialog and enter the username and current password used in the authentication system. If enabled, it is possible to select 'Current Windows user' and login directly with the currently logged in Windows user, without needing to enter a username and password manually.

OAuth Authentication: OAuth Providers configured and enabled on the Integriti server will be listed in the 'Log in with' list. Select the OAuth provider to use and click 'Login'. The OAuth provider's web page will open to allow the operator to authorise.

For the OAuth Authentication system used by earlier versions of Integriti, instead select 'Specified credentials' and enter the operator's username and password for the configured provider.



Copyright © Inner Range PTY LTD January 2025

TROUBLESHOOTING

Unable to log on: Authentication scheme not licensed

Attempted to log in to Integriti using Active Directory without an 'Active Directory Operators' license or using OAuth without the 'OAuth Authentication' feature license.

Unable to log on using Active Directory: The server is not operational

There is a network outage, or the domain controller is not accessible.

Unable to log on using Active Directory: Current security context is not associated with an Active Directory domain or forest

The domain user does not exist or does not belong to an Active Directory Group that has been assigned to an Operator Type.

Unable to log on using OAuth: Unknown operator or incorrect password

- System administrators will see the username, subject ID and group information (if available) from the OAuth provider in Integriti Review for troubleshooting.
- If the Integriti Operator was already added, ensure the username matches the external username exactly.
- If the Integriti Operator should be automatically created, the OAuth provider does not have Automatic Operator Creation enabled, or no group information is available, or the user does not belong to any group that is assigned to an Operator Type.
- The external group membership may have changed so that the user is no longer assigned to an Operator Type

Copyright © Inner Range PTY LTD January 2025



Global Headquarters

Inner Range Australia
+61 3 9780 4300
sales.au@innerrange.com

Inner Range United States
+1 (844) 588-0874
sales.usa@innerrange.com

Inner Range United Kingdom
+44 (0) 845 470 5000
sales.uk@innerrange.com

Inner Range Canada
+1 (844) 588-0874
sales.canada@innerrange.com

Inner Range Middle East
+971 4 8067100
sales.me@innerrange.com

Inner Range India
+91 80 4070 3333
sales.india@innerrange.com

INNERRANGE.COM