

IDOL

OmniGroupServer

Software Version 12.10.0

Release Notes



Document Release Date: October 2021
Software Release Date: October 2021

Legal notices

Copyright notice

© Copyright 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit <https://www.microfocus.com/support-and-services/documentation/>.

Support

Visit the [MySupport portal](#) to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- Search for knowledge documents of interest
- Access product documentation
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts
- Submit and track service requests
- Contact customer support
- View information about all services that Support offers

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the [Access Levels descriptions](#).

Contents

New in this Release	4
Resolved Issues	5
Supported Operating System Platforms	6
Notes	7
Documentation	8

New in this Release

The following new features were released in OmniGroupServer version 12.10.0.

- The `ogs_azure` library, which retrieves security information from Azure Active Directory, has been improved:
 - OmniGroupServer uses the Microsoft Graph API to retrieve information from Azure Active Directory. Earlier versions of OmniGroupServer used the Azure Active Directory Graph API, which has been deprecated. To authenticate with the Microsoft Graph API you must create an OAuth service application. For information about how to do this refer to the *IDOL Document Security Administration Guide*.
 - When retrieving information from Azure Active Directory, OmniGroupServer can process contacts and directory roles. Contacts are processed only when `ImportExternalUsers=TRUE`. The default value of this parameter is now `TRUE`.
 - The configuration parameter `UseOnPremises` has been added, so that you can store users and groups by the value of their `OnPremisesSamAccountName` property (or `OnPremisesSecurityIdentifier` when you also set `UseIDs=TRUE`).
- The third-party libraries `libxml2` and `libxslt` have been updated, to versions 2.9.11 and 1.1.34 respectively.
- The third-party OpenSSL library has been updated to 1.1.1.j.
- ACI servers can now communicate with a License Server that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to `True`). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```
- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

The following issues were resolved in OmniGroupServer version 12.10.0.

- The QueueInfo action (with QueueAction=GetStatus) would return an error when the total number of actions exceeded 999.
- The server could terminate unexpectedly when an authorization role was configured and the list of Clients included a hostname with a wildcard, such as *.domain.example.com. The Clients parameter accepts wildcards only in IP addresses.
- Various GetRequestLog (GRL) HTML issues have been fixed:
 - Actions were not properly escaped in some places, which could allow malicious users to inject some alternative HTML in the GetRequestLog response.
 - The Open link in new window option did not work.
 - The auto refresh option would modify the selected open link option.
 - Links to the obsolete confighelp action have been removed.
 - The HTML page now uses a Content-Security-Policy to protect against malicious data injection by crafted actions sent to the server.

Supported Operating System Platforms

OmniGroupServer 12.10.0 is supported on the following platforms.

Windows (x86-64)

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012

Linux (x86-64)

The minimum supported versions of particular distributions are:

- Red Hat Enterprise Linux (RHEL) 6
- CentOS 6
- SuSE Linux Enterprise Server (SLES) 12
- Ubuntu 14.04
- Debian 8

Solaris (x86-64 and SPARC 64)

DEPRECATED: Support for Solaris x86-64 and SPARC 64 was deprecated in IDOL version 12.10, for all IDOL components except KeyView. IDOL components are currently still available for Solaris, but might not be available in future.

- Solaris 11
- Solaris 10

Notes

- The autpassword command-line tool has been updated to provide hardened AES encryption for passwords. Micro Focus strongly recommends that you reencrypt all passwords in configuration files by using the updated tool.

The older AES encryption format and basic encryption methods are now deprecated. Passwords that you have encrypted with older versions continue to work, but the server logs a warning. Support for these older encryption methods will be removed in future.

Documentation

The following documentation was updated for this release.

- *OmniGroupServer Reference*