

Dangerous Windows Groups

The **Dangerous Windows Groups** report shows all SQL Server instances that grant access to any OS-controlled Windows Group.



Warning

This report does not apply to **Azure SQL Database** and **Amazon RDS** for SQL Server instances.



Recommendation

OS-controlled Windows Groups allow access to almost any Windows Account access to a SQL Server Instance, causing a high-security risk. To guarantee a secure environment, consider removing all SQL Logins for these groups or their parent groups from all SQL Server instances.

Getting Started

Follow these steps to generate this report:

1. Select the Date, Policy, and Baseline options from the Report Settings box.
2. Select a target instance.
3. Click the **View Report** button to generate your report.


SQL Secure™
Assess and audit security risks and access rights

Dangerous Windows Groups

Most current audit data as of Tuesday, September 13, 2022

Server: All servers in policy


There are no audited servers with OS Controlled Windows Groups.

About: This report shows all SQL Server instances that grant access to any OS controlled Windows Group.

Recommendation: OS controlled Windows Groups allow almost any Windows Account access to a SQL Server instance and pose a high security risk. Consider removing all SQL Logins for these groups or their parent groups from all SQL Server instances.

APPENDIX: Audit Data

The following snapshots were used to generate this report. For complete information on what audit data was captured, check the filter settings and status of each snapshot.

SQL Server	Version	Audited On
	SQL Server 2016 v13.0.1601.5	6/15/2022 6:13:57 PM

IDERA
Copyright © 2005-2022 Idera, Inc.

Generated by on 9/13/2022 7:57:07 AM
 Execution Time: 0 hours, 0 minutes, 0 seconds

Page 1 of 1