# Login Security Checks

Login Security Checks ensure credentials from users and permissions, meet the organization's policy, and alert if there are changes.

The Login Security Checks available on the Configure the Policy section are the following:

| Name | Description |
|---|---|
| Active Directory Helper Login Account Not Acceptable | Determine whether the Active Directory Helper account is acceptable |
| Analysis Services Login Account Not Acceptable | Determine whether the Analysis Services account is acceptable |
| Blank Passwords | Determine whether any SQL Logins have blank passwords |
| DISTRIBUTOR_ADMIN Login | Determine whether DISTRIBUTOR_ADMIN account should be deleted. |
| Ensure Windows BUILTIN Groups are not SQL Logins | Determine whether the Windows BUILTIN groups and accounts are not SQL logins. Windows BUILTIN groups have broad memberships and should not be used to get access to the SQL Server Database Engine instance. |
| Ensure Windows Local Groups are not SQL Logins | Determine whether Windows Local groups are used as logins. Allowing local Windows groups to be used as SQL Logins creates a loophole where an OS administrator could add users and give access to SQL Server instances. |
| Full-Text Search Login Account Not Acceptable | Determine whether the Full-Text Search Service account is acceptable |
| Integration Services Login Account Not Acceptable | Determine whether the Integration Services account is acceptable |
| Notification Services Login Account Not Acceptable | Determine whether the Notification Services account is acceptable |
| Orphaned users | Determine whether any orphaned users exist in databases. |
| Reporting Services Login Account Not Acceptable | Determine whether the Reporting Services account is acceptable |
| sa Account Has Blank Password | Determine whether the SQL Server sa account has a blank password |
| sa Account Not Using Password Policy | Determine whether password policy is enforced on the sa account |
| SQL Authentication Enabled | Determine whether SQL Authentication is allowed on the SQL Server |
| SQL Logins not using Must Change | Ensure that all SQL Authentication Logins have the 'must_change' option set to ON. |
| SQL Logins Not Using Password Expiration | Determine whether password expiration is enabled for all SQL Logins |
| SQL Logins Not Using Password Policy | Determine whether password policy is enforced on all SQL Logins |
| SQL Server Agent Login Account Not Acceptable | Determine whether the SQL Server Agent Service account is acceptable |
| SQL Server Browser Login Account Not Acceptable | Determine whether the SQL Server Browser Service account is acceptable |
| SQL Server Service Login Account Not Acceptable | Determine whether the SQL Server Service account is acceptable |

| | |
|---|---|
| SQL Server SYSADMIN accounts | Determine whether SQL SYSADMIN accounts that are in the local Administrator role for the physical server. |
| Suspect Logins | Determine whether suspect logins exist on the SQL Server |
| Unauthorized SQL Logins Exist | Determine whether unauthorized SQL Logins have been created on the SQL Server |
| VSS Writer Login Account Not Acceptable | Determine whether the VSS Writer account is acceptable |
| Weak Passwords | Determine whether any SQL login passwords match the login name or a list of common and restricted passwords. |