Credential Locker Overview

Archived: 2026-04-06 01:10:46 UTC

Applies To: Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2

This topic for the IT professional provides basic conceptual overview information for Credential Locker, and it serves as a portal to other information. Credential Locker is managed by Credential Manager.

Did you mean…

- Windows Vault
- Credential Manager
- Stored User Names and Passwords
- Credentials Protection and Management

Credential Locker is a service that creates and maintains a secure storage area on the local computer that stores user names and passwords the user saved from websites and Windows 8 apps. Credential Locker is accessed through **Credential Manager** in Control Panel as part of the local User Account management feature.

Credential management by using Credential Manager is controlled by the user on the local computer. Users can save and store credentials from supported browsers and Windows applications to make it convenient when they need to sign in to these resources. Credentials are saved in special encrypted folders on the computer under the user's profile. Applications that support this feature (through the use of the Credential Manager APIs), such as web browsers and Windows 8 apps, can present the correct credentials to other computers and websites during the sign-in process.

When a website, an application, or another computer requests authentication through NTLM or Kerberos, an **Update Default Credentials** or **Save Password** check box is presented to the user. This dialog to request credentials saving is generated by an application that supports the Credential Manager APIs. If the user selects the check box, Credential Manager keeps track of the user's name, password, and related information for the authentication service that is in use.

The next time the service is used, Credential Manager automatically supplies the credential that is stored in Credential Locker. If it is not accepted, the user is prompted for the correct access information. If access is granted with the new credentials, Credential Manager overwrites the previous credential with the new one and then stores the new credential in Credential Locker.

For example, if the user adds a Windows credential through Credential Manager, Remote Desktop Connection will detect it and populate the dialog box with that credential. If that credential is rejected and the user supplies the correct one on the next attempt, Credential Locker stores the successful credential. Similarly, Internet Explorer 10 searches Credential Locker for any credentials that are associated with a website where sign in is required. If no

credentials are found, the user is prompted to sign in and can optionally save the credentials that are entered to Credential Locker to be used the next time the website is accessed.

Isolating credentials is part of the feature's architecture. Credential Locker only releases credentials under the following conditions:

- To Windows Store apps that support the Credential Manager APIs
- To the website that the user elected to store that credential when the browser supports the Credential Manager APIs

Note

There is no change in how Credential Locker handles credentials for legacy Windows applications.

Windows Server 2012 and Windows 8 introduce the ability to sign in to a computer by using a Microsoft account, or to connect a domain account on a computer with a Microsoft account. A Microsoft account was formerly known as a Windows Live ID account, which uses the form, for example, someone@contoso.com. Using a Microsoft account provides user personalization through roaming credentials, which includes website and Windows Store app sign in information that is stored in Credential Locker.

Credential roaming is enabled by default on non-domain joined computers, making it possible for users to access their Credential Locker through all their trusted Windows devices. The files that compose Credential Locker cannot be password protected and access to Credential Locker cannot be locked. The Credential Locker roams with the user's Microsoft account, and Windows synchronizes the credentials as sign in occurs.

Following are some important behaviors to consider if you use Credential Locker in your enterprise.

- Credential management by using Credential Manager is controlled by the user on the local computer.
- Windows prevents credentials that are stored in Credential Locker on domain-joined computers from leaving the enterprise as part of the user profile in the Microsoft account.
- Credentials in the Microsoft account will not roam within your enterprise if you are using Credential Roaming (formerly known as Digital ID Management Service or DIMS).The Roaming User Profiles feature incorporates Credential Locker, which might result in credential usage conflicts with Credential Manager. Therefore, we recommend that you choose either Credential Manager which uses Credential Locker or the Roaming User Profiles in your enterprise design.
- Credentials only roam into your enterprise by using a user profile of a Microsoft account if a credential with the same username, target, and Windows Store app package ID does not currently exist in your enterprise.

Users can take advantage of the ability to save and store the credentials they use when they sign in to different systems, including websites and Windows applications. In the supported Windows versions as designated in the **Applies To** list at the beginning of this topic, Windows Store apps can also be programmed so that users have the option to save credentials to Credential Locker. Internet Explorer 10 also provides this functionality.

Users can access their Credential Locker through all their trusted Windows devices as part of their identity user profile, but this feature is turned off for domain-joined computers.

Windows Store apps can be programmed to leverage Credential Locker.

Credential roaming is accomplished by synchronizing the user's profile using the Microsoft account (formerly known as the Windows Live ID).

Credential roaming is enabled by default on non-domain-joined computers, and it is disabled on domain-joined computers.

Important

Credential Manager is controlled by the user on the local computer. The user has the option to locally enable credentials storage at any time, even on a domain-joined computer.

Credential Locker supports seamless sign in by using Windows Store apps that use Web Authentication Broker. It remembers passwords for services like Facebook and Twitter, so the user does not have to enter credentials multiple times. This seamless sign-in experience has been extended across the user's devices that are running Windows 8.1.

Formerly, when multiple credentials were stored for the same resource, there was no way to specify a "default" credential. In Windows 8.1, the user can designate a default credential for a particular resource. And to assist with the user's choice, credentials stored in Credential Locker display the date when they were last used.

The following list describes functionality that is present in Windows Server 2008 R2 and Windows 7, but has been removed in Windows Server 2012 and Windows 8.

1. Automatically loading Credential Locker information to and from USB devices is not supported.
2. There is no UI support for displaying multiple lockers, creating lockers, removing lockers, deleting lockers, copying lockers, or viewing the advanced properties for Credential Locker.
3. There is no UI support for adding or editing web passwords in Credential Manager. Passwords can be changed through the application that requires them.
4. There is no support for locking or unlocking Credential Locker. To facilitate roaming, access to Credential Locker cannot be locked.
5. There is no support for password protecting Credential Locker.
6. The Credential Locker feature manages the release of a user's credentials to the correct application or website. Users cannot be prompted to consent the release of a specific credential to any other.

For a list of deprecated features in the Windows Server 2012, see Features Removed or Deprecated in Windows Server 2012.

You can use the Security Policy setting **Network access: Do not allow storage of passwords and credentials for network authentication** to control Credential Manager. If you enable this setting, Credential Manager does not store passwords or credentials for domain authentication on the computer.

Because Windows Store apps can be programmed to support Credential Locker, there is no way for the IT administrator to control the storage of credentials from these apps on the local computer. You can, however, control what apps can run in your enterprise by using application control features such as AppLocker.

Credential Manager is a Control Panel app that is available in all editions of the supported Windows versions as designated in the **Applies To** list at the beginning of this topic. There are no additional software requirements to use this feature.

The following table provides additional resources for Credential Manager, Credential Locker, and related technologies.

Content type	References
Product evaluation	Not available
Planning	Not available
Deployment	Not available
Operations	Not available
Troubleshooting	Not available
Security	Not available
Tools and settings	Credential Manager Credential Manager Reference
Community resources	Protecting your digital identity Signing in to Windows 8 with a Windows Live ID

Content type	References
Related technologies	AppLocker Overview Implementing Roaming User Profiles

---