



BitLocker Recovery Keys

Last Modified on 08.12.24

ConfigMgr BitLocker Recovery Keys

The **ConfigMgr BitLocker Recovery Keys** tool lets you retrieve current recovery passwords stored in Configuration Manager.

To run the tool:

1. In your Configuration Manager console, right-click on a device.
2. Click **Right Click Tools > Security Tools > ConfigMgr BitLocker Recovery Keys**.

The **ConfigMgr BitLocker Keys** window that opens displays the following information:

- Machine Name
- Recovery Key
- Recovery Key ID
- Error

3. Right-click on a Recovery Key ID and click **Copy Key to Clipboard**.
-

AD BitLocker Recovery Keys

The **AD BitLocker Recovery Keys** tool lets you view current recovery passwords and their detailed history.

To run the tool:

1. In your Configuration Manager console, right-click on a device.
2. Click **Right Click Tools > Security Tools > AD BitLocker Recovery Keys**.

The **AD BitLocker Keys** window that opens displays the history of the recovery password including the dates when it was created and last changed.

See also [Delegate Access to BitLocker Recovery Keys in Active Directory](#)

MBAM BitLocker Recovery Keys

The **MBAM BitLocker Recovery Keys** tool allows you to request new MBAM recovery keys.

To run the tool:

1. In your Configuration Manager console, right-click on a device.
2. Click **Right Click Tools > Security Tools > MBAM BitLocker Recovery Keys**.
3. In the **MBAM Recovery Key Request** window, select the reason for requesting MBAM recovery keys.

Reasons include:

- Operating System Boot Order changed
- BIOS changed
- Operating System files modified
- Lost Startup Key
- Lost PIN
- TPM Reset
- Lost Passphrase
- Lost Smartcard
- Other

4. Click **Request Key(s)**.

TIP: You can copy a recovery key by right-clicking on an entry and choosing **Copy Key to Clipboard**.

Entra ID BitLocker Recovery Keys

The **Entra ID BitLocker Recovery Keys** tool lets you retrieve current recovery passwords stored in Microsoft Entra ID (formerly Azure Active Directory). This tool requires a connection to your Recast Management Server.

NOTE: You must be running [Recast Software Version 5.6.2407.1103](#) or later to use this tool.

Prerequisites

- [Recast Management Server installed with Recast Proxy](#)
- [Users or user groups delegated access to view BitLocker Keys in Entra ID](#)

Before you can [run the tool](#) and receive a token to retrieve Entra ID BitLocker keys, you'll also need to do the

following:

- [Register the Right Click Tools Console Extension as an application with the Microsoft identity platform](#)
- [Configure a new platform](#)
- [Grant the application API permissions](#)
- [Add a service connection from your Recast Management Server to Entra ID \(Azure Active Directory\)](#)

Register the Right Click Tools Console Extension with Microsoft

To register the application:

1. Log into <https://portal.azure.com> using your Azure credentials with full admin rights.
2. Search for **App registrations**.
3. On the **App registrations** page, click **New registration**.
4. Give the application a meaningful display **Name**.
5. As the **Supported account type**, select **Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)**.
6. Click **Register**.
7. In the **Overview** pane that opens, copy the **Application (client) ID** and **Directory (tenant) ID** as you will need to enter these later in your Recast Management Server.

Add a Platform

To add a platform:

1. On the **App registrations** page, under **Manage**, click **Authentication**.
2. Under **Platform Configurations**, select **Add a platform**.
3. Under **Configure platforms**, select **Mobile and desktop applications**.
4. Under **Redirect URIs**, add a custom URI with your App ID in the name: `ms-appx-web://microsoft.aad.brokerplugin/<Your-App-ID>`
5. Click **Configure** to add the platform.
6. Under **Advanced Settings**, toggle **Enable the following mobile and desktop flows:** to **Yes** and click to **Save** this configuration.

Add API Permissions for the Application

To add API permissions:

1. On the **App registrations** page, under **Manage**, click **API Permissions**.
2. Select **Add a permission**.
3. Add the following permissions from the Microsoft Graph API for the application:

Delegated permissions

- BitlockerKey.Read.All
- BitlockerKey.ReadBasic.All
- DeviceManagementConfiguration.Read.All
- DeviceManagementManagedDevices.Read.All

Application permissions

- Device.Read.All

4. Once the required permissions are added, click **Grant admin consent for [Tenant Name]**.

Add an Entra ID Service Connection for the Application

The Entra ID BitLocker Recovery Key tool requires a service connection from your Recast Management Server to Entra ID for your registered application.

To add an Entra ID service connection:

1. On the **Service Connections** page in your Recast Management Server interface, click **Add Service Connection**.
2. Select **AzureActiveDirectory** (Entra ID) as the connection **Type**.
3. Name the new connection and add the **Application (client) ID** and **Directory (tenant) ID** that you copied from the **Overview** pane in the Azure portal.
4. Select a **Proxy Computer Name** and **Proxy User Name** from the drop-down lists.
5. Click the **Confirmed** check box to ensure that the service connection is available for use.
6. Click **Submit**.

Run the Entra ID BitLocker Recovery Keys Tool

To run the tool:

1. In your Configuration Manager console, right-click on a device.
2. Click **Right Click Tools > Security Tools > EntraID BitLocker Recovery Keys**.

The **EntraID BitLocker Keys** window that opens displays the following information:

- Machine Name
- Recovery Key
- Recovery Key ID
- Date Created
- Error

3. Right-click on a Recovery Key ID and click **Copy Key to Clipboard**.
-

