Microsoft Intune Data Warehouse API

Article • 03/03/2025

The Intune Data Warehouse API lets you access your Intune data in a machine-readable format for use in your favorite analytics tool. You can use the API to build reports that provide insight into your enterprise mobile environment. The API uses the OData protocol, which follows standard patterns for:

- Request and response headers
- Status codes
- HTTP methods
- URL conventions
- Media types
- Payload formats
- Query options

The OData (Open Data Protocol) is an Organization for the Advancement of Structured Information Standards (OASIS) standard that defines the best practice for building and consuming RESTful APIs. The Intune Data Warehouse uses OData version 4.0.

This reference section provides an overview of endpoints, supported HTTP methods, return payload formats, and documentation of the Intune Data Warehouse data model.

> ⓘ **Important**
>
> You can try out the latest functionality of the Data Warehouse by using the beta version. To use the beta version, your URL must contain the query parameter `api-version=beta`. The beta version offers features before they are made generally available as a supported service. As Intune adds new features, the beta version may change behavior and data contracts. Any custom code or reporting tools dependent on the beta version may break with ongoing updates.

OData custom client

You can access the Intune Data Warehouse data model through RESTful endpoints. To gain access to your data, your client must authorize with Microsoft Entra ID using OAuth 2.0. You first set up a web app and a client app in Azure, grant permissions to the client. Your local client gets authorization and can then communicate with the Data Warehouse endpoints.

For more information, see Get data from the Data Warehouse API with a REST client.

> ⓘ Note
>
> You can access the GitHub Intune Data Warehouse repo on Github for code samples.

Interacting with the API

The API requires authorization with Microsoft Entra ID. Microsoft Entra ID uses OAuth 2.0. Once authorized, you can get data from the API using an HTTP GET verb and contacting the exposed entity collections. For details see:

- Authorization
- API URL Structure

Intune Data Warehouse data model

OData defines an abstract data model and a protocol that let any client access information exposed by any data source. The data model documentation topic contains an explanation of the namespaces, entities, and return objects in the Intune Data Warehouse data model. For more information, see Data Warehouse Data Model.

Next steps

Learn more about working with Microsoft Entra ID by reading the Authentication Scenarios for Microsoft Entra ID.

Find OData resources at odata.org.

Review the OData Version 4.0 standard at OData Version 4.0.

Feedback

Was this page helpful? Yes No

Get data from the Intune Data Warehouse API with a REST client

Article • 03/03/2025

You can access the Intune Data Warehouse data model through RESTful endpoints. To gain access to your data, your client must authorize with Microsoft Entra ID using OAuth 2.0. To enable access, first set up a native app in Azure and grant permissions to the Microsoft Intune API. Your local client gets authorization, and then the client can communicate with the Data Warehouse endpoints through the native app.

The steps to set up a client to get data from the Data Warehouse API require you to:

1. Create a client app as a native app in Azure
2. Grant the client app access to the Microsoft Intune API
3. Create a local REST client to get the data

Use the following steps to learn how to authorize and access the API with a REST client. First, you will look at using a generic REST client using Postman. Postman is a commonly used tool troubleshooting and developing REST clients to work with APIs. For more information about Postman, see the Postman site. Then you can look at a C# code sample. The sample provides an example for authorizing a client and getting data from the API.

Create a client app as a native app in Azure

Create a native app in Azure. This native app is the client app. The client running on your local machine references the Intune Data Warehouse API when the local client requests credentials.

1. Sign in to the Microsoft Entra admin center.
2. Choose **Microsoft Entra ID** > **App Registrations** to open the **App registrations** pane.
3. Select **New app registration**.
4. Type the app details.
   a. Type a friendly name, such as 'Intune Data Warehouse Client' for the **Name**.
   b. Select **Accounts in this organizational directory only (Microsoft only - Single tenant)** for the **Supported account types**.
   c. Type a URL for the **Redirect URI**. The Redirect URI will depend on the specific scenario, however if you plan on using Postman, type

`https://www.getpostman.com/oauth2/callback`. You will use the callback for client authentication step when authenticating to Microsoft Entra ID.

5. Select **Register**.
6. Note the **Application (client) ID** of this app. You will use the ID in the next section.

Grant the client app access to the Microsoft Intune API

You now have an app defined in Azure. Grant access from the native app to the Microsoft Intune API.

1. Sign in to the Microsoft Entra admin center.
2. Choose **Microsoft Entra ID** > **App Registrations** to open the **App registrations** pane.
3. Select the app that you need to grant access. You named the app something such as **Intune Data Warehouse Client**.
4. Select **API permissions** > **Add a permission**.
5. Find and select the Intune API. It is named **Microsoft Intune API**.
6. Select **Delegated Permissions** box and click the **Get data warehouse information from Microsoft Intune** box.
7. Click **Add permissions**.
8. Optionally, Select **Grant admin consent for Microsoft** in the Configured permissions pane, then select **Yes**. This will grant access to all accounts in the current directory. This will prevent the consent dialog box from appearing for every user in the tenant. For more information, see Integrating applications with Microsoft Entra ID.
9. Select **Certificates & secrets** > **+ New client secret** and generate a new secret. Make sure to copy it some place safe because you won't be able to access it again.

Get data from the Microsoft Intune API with Postman

You can work with the Intune Data Warehouse API with a generic REST client such as Postman. Postman can provide insight into the features of the API, the underlying OData data model, and troubleshoot your connection to the API resources. In this section, you can find information about generating an Auth2.0 token for your local client. The client will need the token to authenticate with Microsoft Entra ID and access the API resources.

Information you will need to make the call

You need the following information to make a REST call using Postman:

Expand table

Attribute	Description	Example
Callback URL	Set this as the callback URL in your app settings page.	`https://www.getpostman.com/oauth2/callback`
Token Name	A string used to pass the credentials to the Azure app. The process generates your token so you can make a call to the Data Warehouse API.	Bearer
Auth URL	This is the URL used to authenticate.	https://login.microsoftonline.com/common/oauth2/authorize?resource=https://api.manage.microsoft.com/
Access Token URL	This is the URL used to grant the token.	https://login.microsoftonline.com/common/oauth2/token
Client ID	You created, and noted this when creating the native app in Azure.	4184c61a-e324-4f51-83d7-022b6a81b991
Client Secret	You created, and noted this when creating the native app in Azure.	Ksml3dhDJs+jfK1f8Mwc8
Scope (Optional)	You can leave the field blank. **NOTE**: Some SDKs, such as the Microsoft Authentication Library (MSAL) for Python, may need the scope defined with double slashes (//).	SCOPE = ['https://api.manage.microsoft.com//.default']

Attribute	Description	Example
Grant Type	The token is an authorization code.	Authorization code

OData endpoint

You also need the endpoint. To get your Data Warehouse endpoint, you will need the custom feed URL. You can get the OData endpoint from the Data Warehouse pane.

1. Sign in to the Microsoft Intune admin center.
2. Open the **Data Warehouse** pane by selecting **Reports** > **Data warehouse**.
3. Copy the custom feed url under **OData feed for reporting service**. It should look something like: `https://fef.tenant.manage.microsoft.com/ReportingService/DataWarehouseFEService?api-version=v1.0`

The endpoint follows the following format: `https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/{entity}?api-version={verson-number}`

For example, the **dates** entity looks like: `https://fef.tenant.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api-version=v1.0`

For more information, see Intune Data Warehouse API endpoint.

Make the REST call

To get a new access token for Postman, you must add the Microsoft Entra authorization URL, add your Client ID, and Client Secret. Postman will load the authorization page where you will type your credentials.

Before you make the call, verify that you have already added the Callback URL to your app in Azure. The Callback URL is `https://www.getpostman.com/oauth2/callback`.

Add the information used to request the token

1. Download Postman if you do not already have it installed. To download Postman, see www.getpostman.com.

2. Open Postman. Choose the HTTP operation **GET**.

3. Paste the endpoint URL into the address. It should look something like:

   `https://fef.tenant.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api-version=v1.0`

4. Choose the **Authorization** tab, and select **OAuth 2.0** from the **Type** list.

5. Scroll down to the **Configure New Token** section.

6. Type Bearer for the **Token Name**.

7. Select **Authorization Code** as the Grant Type.

8. Add the **Callback URL**. The callback URL is `https://www.getpostman.com/oauth2/callback`.

9. Add the **Auth URL**. It should look something like:

   `https://login.microsoftonline.com/common/oauth2/authorize?resource=https://api.manage.microsoft.com/`

10. Add the **Access Token URL**. It should look something like:

    `https://login.microsoftonline.com/common/oauth2/token`

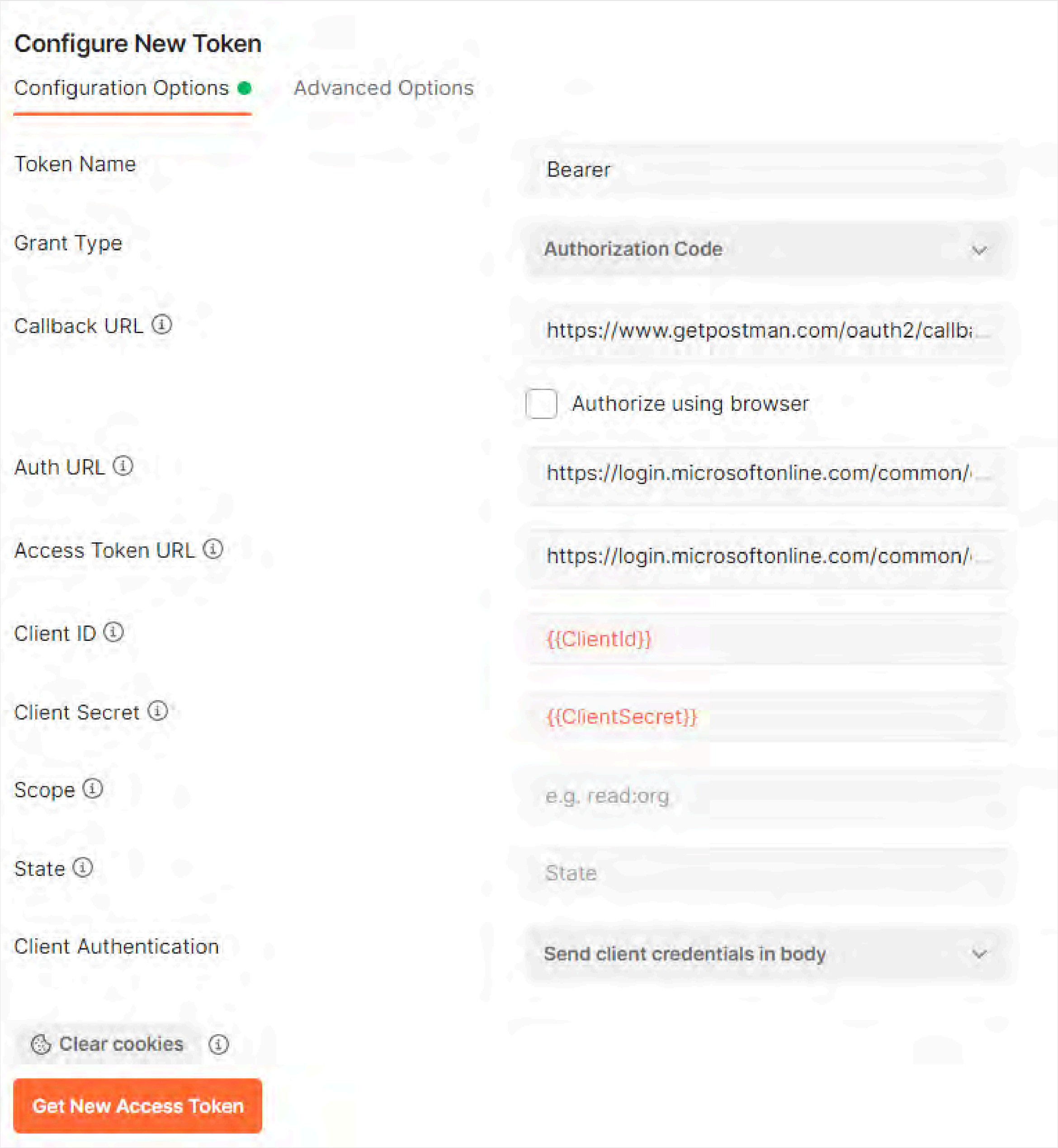
11. Add the **Client ID** from the native app that you created in Azure and named `Intune Data Warehouse Client`. It should look something like:

    `88C8527B-59CB-4679-A9C8-324941748BB4`

12. Add the **Client Secret** you generated from within the native app that you created in Azure. It should look something like:

    `Ksml3dhDJs+jfK1f8Mwc8`

13. Select **Get New Access Token**.



Configure New Token

Token Name: Bearer

Grant Type: Authorization Code

Callback URL ⓘ: https://www.getpostman.com/oauth2/callb

□ Authorize using browser

Auth URL ⓘ: https://login.microsoftonline.com/common/

Access Token URL ⓘ: https://login.microsoftonline.com/common/

Client ID ⓘ: {{ClientId}}

Client Secret ⓘ: {{ClientSecret}}

Scope ⓘ: e.g. read:org

State ⓘ: State

Client Authentication: Send client credentials in body

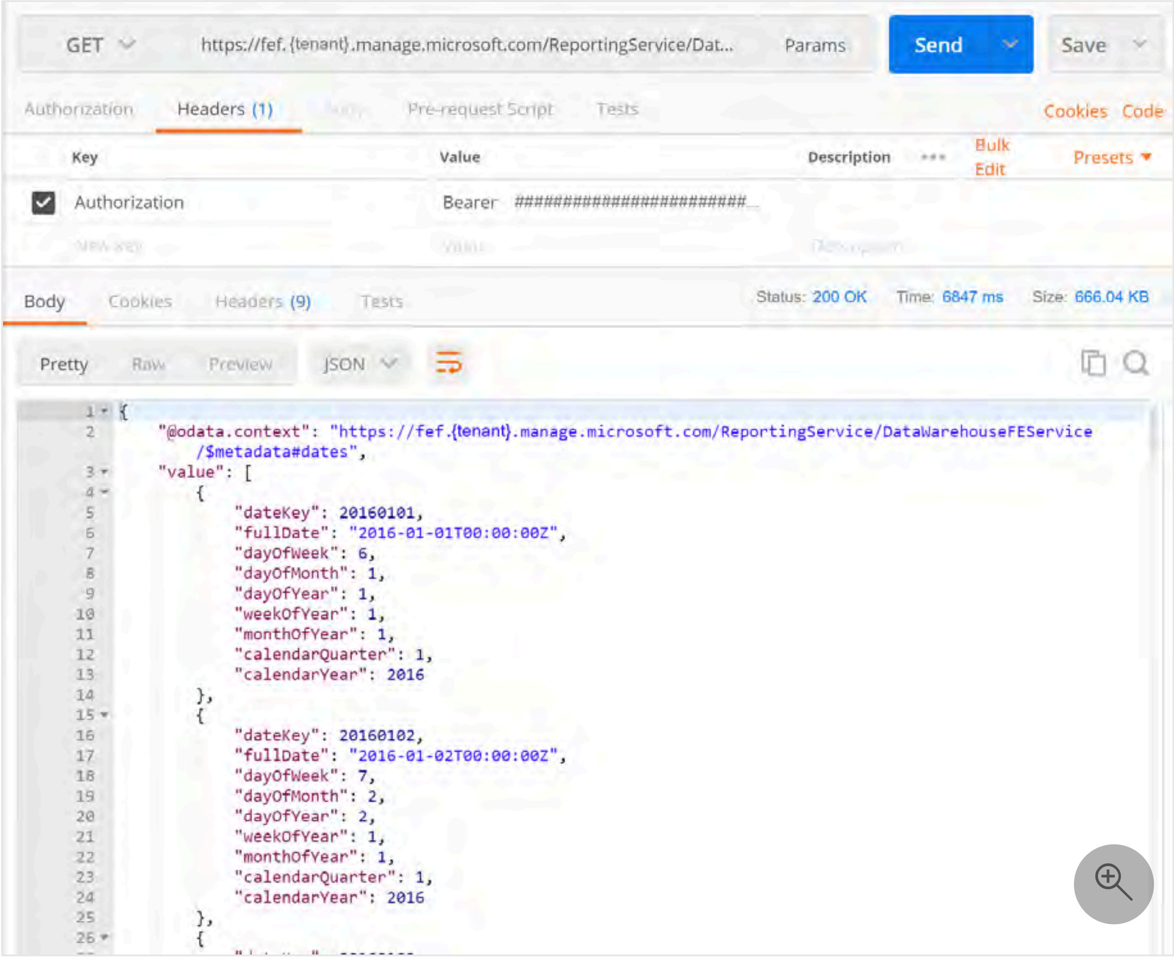
14. Type your credentials in the Active AD authorization page. The list of tokens in Postman now contains the token named `Bearer`.

15. Select **Use Token**. The list of headers contains the new key value of Authorization and the value `Bearer <your-authorization-token>`.

Send the call to the endpoint using Postman

1. Select **Send**.

2. The return data appears in the Postman response body.



GET https://fef.{tenant}.manage.microsoft.com/ReportingService/Dat...

☑ Authorization Bearer ########################...

Status: 200 OK Time: 6847 ms Size: 666.04 KB

```
{
    "@odata.context": "https://fef.{tenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService
        /$metadata#dates",
    "value": [
        {
            "dateKey": 20160101,
            "fullDate": "2016-01-01T00:00:00Z",
            "dayOfWeek": 6,
            "dayOfMonth": 1,
            "dayOfYear": 1,
            "weekOfYear": 1,
            "monthOfYear": 1,
            "calendarQuarter": 1,
            "calendarYear": 2016
        },
        {
            "dateKey": 20160102,
            "fullDate": "2016-01-02T00:00:00Z",
            "dayOfWeek": 7,
            "dayOfMonth": 2,
            "dayOfYear": 2,
            "weekOfYear": 1,
            "monthOfYear": 1,
            "calendarQuarter": 1,
            "calendarYear": 2016
        },
        {
```

Create a REST client (C#) to get data from the Intune Data Warehouse

The following sample contains a simple REST client. The code uses the **httpClient** class from the .NET library. Once the client gains credentials to Microsoft Entra ID, the client constructs a GET REST call to retrieve the dates entity from the Data Warehouse API.

> ⓘ **Note**
>
> You can access the following code sample on GitHub. Refer to the GitHub repo for the latest changes and updates to the sample.

1. Open **Microsoft Visual Studio**.
2. Choose **File** > **New Project**. Expand **Visual C#**, and choose **Console App (.NET Framework)**.
3. Name the project `IntuneDataWarehouseSamples`, browse to where you would like to save the project, and then select **OK**.

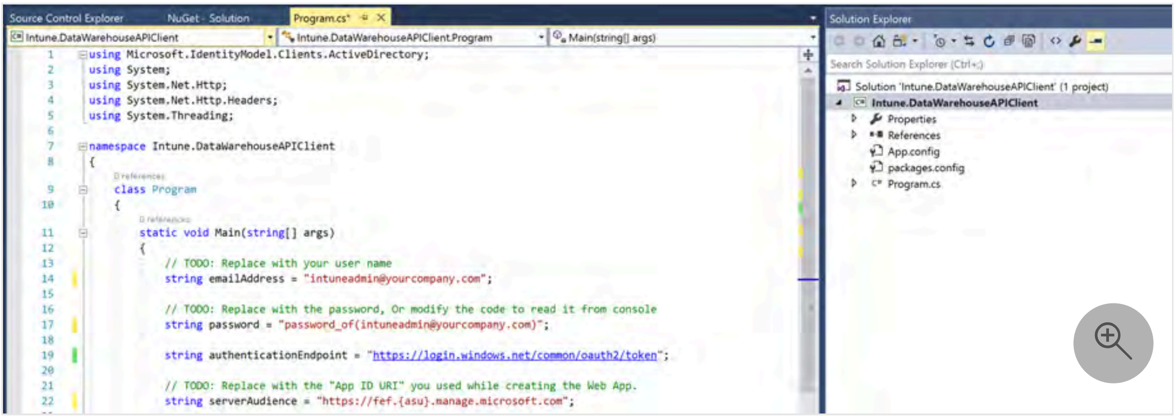
4. Right-click the name of the solution in the Solution Explorer, and then select **Manage NuGet Packages for Solution**. Select **Browse**, and then type `Microsoft.Identity.Client` in the search box.

> ⓘ **Note**
>
> You must use the Microsoft Authentication Library (MSAL). For more information, see [Update your applications to use Microsoft Authentication Library (MSAL) and Microsoft Graph API](#) .

5. Choose the package, select the **IntuneDataWarehouseSamples** project under Manage Packages for Your Solution, and then select **Install**.

6. Select **I Accept** to accept the NuGet package license.

7. Open `Program.cs` from the Solution Explorer.


Source Control Explorer
NuGet - Solution
Program.cs*
Intune.DataWarehouseAPIClient
Intune.DataWarehouseAPIClient.Program
Main(string[] args)
0 references
0 references
Solution Explorer
Search Solution Explorer (Ctrl+;)
Solution 'Intune.DataWarehouseAPIClient' (1 project)
Intune.DataWarehouseAPIClient
Properties
References
App.config
packages.config
Program.cs

```
using Microsoft.IdentityModel.Clients.ActiveDirectory;
using System;
using System.Net.Http;
using System.Net.Http.Headers;
using System.Threading;

namespace Intune.DataWarehouseAPIClient
{
    class Program
    {
        static void Main(string[] args)
        {
            // TODO: Replace with your user name
            string emailAddress = "intuneadmin@yourcompany.com";

            // TODO: Replace with the password, Or modify the code to read it from console
            string password = "password_of(intuneadmin@yourcompany.com)";

            string authenticationEndpoint = "https://login.windows.net/common/oauth2/token";

            // TODO: Replace with the "App ID URI" you used while creating the Web App.
            string serverAudience = "https://fef.{asu}.manage.microsoft.com";
```

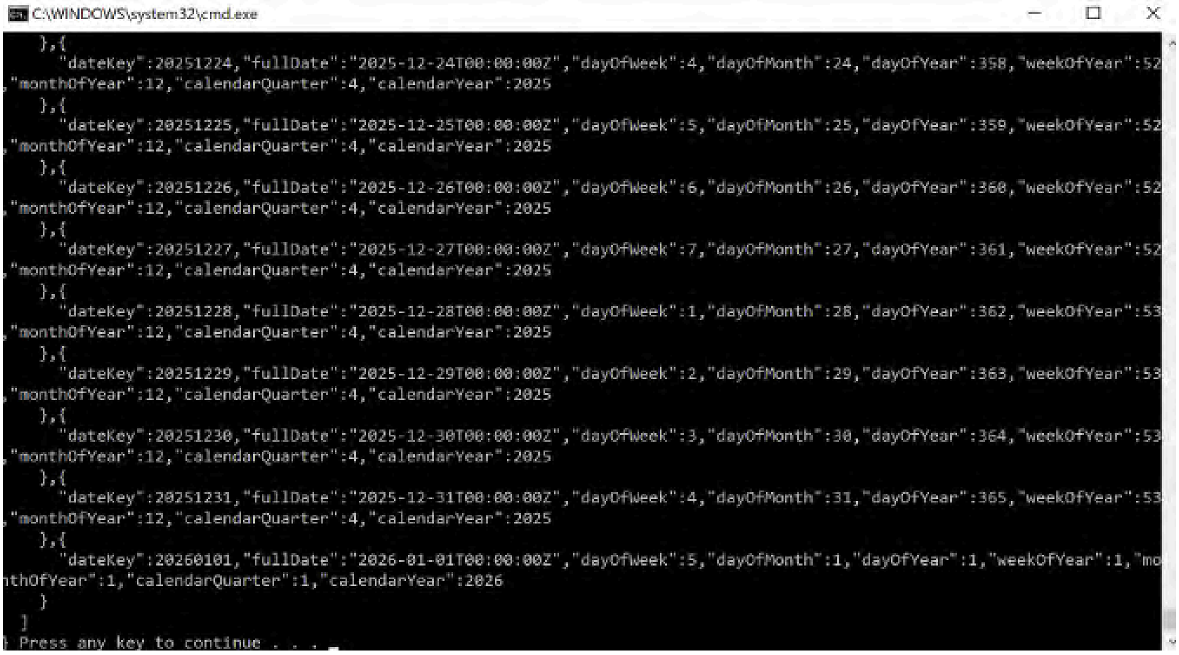
8. Replace the code in *Program.cs* with the following code:

C#

```csharp
namespace IntuneDataWarehouseSamples
{
using System;
using System.Net.Http;
using System.Net.Http.Headers;
using Microsoft.Identity.Client;

class Program
{
 static void Main(string[] args)
{
/**
* TODO: Replace the below values with your own.
* emailAddress - The email address of the user that you will
authenticate as.
*
* password  - The password for the above email address.
*    This is inline only for simplicity in this sample. We do not
*    recommend storing passwords in plaintext.
*
* applicationId - The application ID of the native app that was created
in AAD.
*
* warehouseUrl   - The data warehouse URL for your tenant. This can be
found in
*      the Microsoft Intune admin center.
*
* collectionName - The name of the warehouse entity collection you
would like to
*      access.
*/
var emailAddress = "intuneadmin@yourcompany.com";
var password = "password_of(intuneadmin@yourcompany.com)";
var applicationId = "<Application ID>";
var warehouseUrl = "https://fef.
{yourinfo}.manage.microsoft.com/ReportingService/DataWarehouseFEService
?api-version=v1.0";
var collectionName = "dates";

var msalContext = new
AuthenticationContext("https://login.windows.net/common/oauth2/token");
AuthenticationResult authResult = msalContext.AcquireTokenAsync(
resource: "https://api.manage.microsoft.com/",
clientId: applicationId,
userCredential: new UserPasswordCredential(emailAddress,
password)).Result;

var httpClient = new HttpClient();
httpClient.DefaultRequestHeaders.Authorization = new
AuthenticationHeaderValue("Bearer", authResult.AccessToken);

var uriBuilder = new UriBuilder(warehouseUrl);
uriBuilder.Path += "/" + collectionName;

HttpResponseMessage response =
httpClient.GetAsync(uriBuilder.Uri).Result;

Console.Write(response.Content.ReadAsStringAsync().Result);
Console.ReadKey();
}
}
}
```

9. Update the `TODO`s in the code sample.

10. Press **Ctrl** + **F5** to build and execute the Intune.DataWarehouseAPIClient client in Debug mode.



```
    },{
      "dateKey":20251224,"fullDate":"2025-12-24T00:00:00Z","dayOfWeek":4,"dayOfMonth":24,"dayOfYear":358,"weekOfYear":52
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20251225,"fullDate":"2025-12-25T00:00:00Z","dayOfWeek":5,"dayOfMonth":25,"dayOfYear":359,"weekOfYear":52
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20251226,"fullDate":"2025-12-26T00:00:00Z","dayOfWeek":6,"dayOfMonth":26,"dayOfYear":360,"weekOfYear":52
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20251227,"fullDate":"2025-12-27T00:00:00Z","dayOfWeek":7,"dayOfMonth":27,"dayOfYear":361,"weekOfYear":52
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20251228,"fullDate":"2025-12-28T00:00:00Z","dayOfWeek":1,"dayOfMonth":28,"dayOfYear":362,"weekOfYear":53
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20251229,"fullDate":"2025-12-29T00:00:00Z","dayOfWeek":2,"dayOfMonth":29,"dayOfYear":363,"weekOfYear":53
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20251230,"fullDate":"2025-12-30T00:00:00Z","dayOfWeek":3,"dayOfMonth":30,"dayOfYear":364,"weekOfYear":53
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20251231,"fullDate":"2025-12-31T00:00:00Z","dayOfWeek":4,"dayOfMonth":31,"dayOfYear":365,"weekOfYear":53
,"monthOfYear":12,"calendarQuarter":4,"calendarYear":2025
    },{
      "dateKey":20260101,"fullDate":"2026-01-01T00:00:00Z","dayOfWeek":5,"dayOfMonth":1,"dayOfYear":1,"weekOfYear":1,"mo
nthOfYear":1,"calendarQuarter":1,"calendarYear":2026
    }
  ]
} Press any key to continue . . .
```

11. Review the console output. The output contains data in a JSON format pulled from the **dates** entity in your Intune tenant.

Next steps

You can find details on authorization, the API URL structure, and OData endpoints in Use the Intune Data Warehouse API.

You can also refer to the Intune Data Warehouse Data Model to find the data entities contained in the API. For more information, see Intune Data Warehouse API Data Model.

Feedback

Was this page helpful? Yes No

Intune Data Warehouse API endpoint

Article • 03/03/2025

You can use the Intune Data Warehouse API with an account with specific role-based access controls and Microsoft Entra credentials. You will then authorize your REST client with Microsoft Entra ID using OAuth 2.0. And finally, you will form a meaningful URL to call a data warehouse resource.

Microsoft Entra ID and Intune credential requirements

Authentication and authorization are based on Microsoft Entra credentials and Intune role-based access control (RBAC). All global administrators and Intune service administrators for your tenant have access to the Data warehouse by default. Use Intune roles to provide access for more users by giving them access to the **Intune data warehouse** resource.

Requirements for accessing the Intune Data Warehouse (including the API) are:

- User must have a minimum of one of the following roles:
  - An Intune service administrator
  - User with role-based access to **Intune data warehouse** resource
  - User-less authentication using application-only authentication

ⓘ Important

To be assigned an Intune role and access the Intune Data Warehouse, the user must have an Intune license. For more information, see Role-based access control (RBAC) with Microsoft Intune and Microsoft Intune licensing.

Authorization

Microsoft Entra ID uses OAuth 2.0 to enable you to authorize access to web applications and web APIs in your Microsoft Entra tenant. This guide is language independent, and describes how to send and receive HTTP messages without using any open-source libraries. The OAuth 2.0 authorization code flow is described in section 4.1 of the OAuth 2.0 specification.

For more information, see Authorize access to web applications using OAuth 2.0 and Microsoft Entra ID.

API URL structure

The Data Warehouse API endpoints read the entities for each set. The API supports a **GET** HTTP verb, and a subset of query options.

The URL for Intune uses the following format:
`https://fef.{location}.manage.microsoft.com/ReportingService/DataWarehouseFEService/{entity-collection}?api-version={api-version}`

> ⓘ **Note**
>
> In the above URL, replace `{location}`, `{entity-collection}`, and `{api-version}` based on the details provided in the table below.

The URL contains the following elements:

⛶ Expand table

Element	Example	Description
location	msua06	The base URL can be found by viewing the Data Warehouse API blade in the Microsoft Intune admin center.
entity-collection	devicePropertyHistories	The name of the OData entity collection. For more information on collections and entities in the data model, see Data Model.
api-version	beta	Version is the version of the API to access. For more information, see Version.
maxhistorydays	7	(Optional) The maximum number of days of history to retrieve. This parameter can be supplied to any collection, but will only take effect for collections that include `dateKey` as a part of their key property. See DateKey Range Filters for more information.

API version information

You can now use the v1.0 version of the Intune Data Warehouse by setting the query parameter `api-version=v1.0`. Updates to collections in the Data Warehouse are additive in nature and do not break existing scenarios.

You can try out the latest functionality of the Data Warehouse by using the beta version. To use the beta version, your URL must contain the query parameter `api-version=beta`. The beta version offers features before they are made generally available as a supported service. As Intune adds new features, the beta version may change behavior and data contracts. Any custom code or reporting tools dependent on the beta version may break with ongoing updates.

OData query options

The current version supports the following OData query parameters: `$filter`, `$select`, `$skip,` and `$top`. In `$filter`, only `DateKey` or `RowLastModifiedDateTimeUTC` may be supported when the columns are applicable, and other properties would trigger a bad request.

DateKey Range Filters

`DateKey` range filters may be used to limit the amount of data to download for some of the collections with `dateKey` as a key property. The `DateKey` filter can be used to optimize service performance by providing the following `$filter` query parameter:

1. `DateKey` alone in the `$filter`, supporting the `lt/le/eq/ge/gt` operators and joining with the logic operator `and`, where they can be mapped to a begin date and/or end date.
2. `maxhistorydays` is supplied as custom query option.

Filter examples

> ⓘ Note
>
> The filter examples assume today is 2/21/2018.

Expand table

Filter	Performance Optimization	Description
`maxhistorydays=7`	Full	Return data with `DateKey` between 20180214 and 20180221.
`$filter=DateKey eq 20180214`	Full	Return data with `DateKey` equal to 20180214.
`$filter=DateKey ge 20180214 and DateKey lt 20180221`	Full	Return data with `DateKey` between 20180214 and 20180220.
`maxhistorydays=7&$filter=DateKey eq 20180214`	Full	Return data with `DateKey` equal to 20180214. `maxhistorydays` is ignored.
`$filter=RowLastModifiedDateTimeUTC ge 2018-02-21T23:18:51.3277273Z`	Full	Return data with `RowLastModifiedDateTimeUTC` is greater than or equal to `2018-02-21T23:18:51.3277273Z`

Feedback

Was this page helpful? Yes No

Intune Data Warehouse application-only authentication

Article • 03/03/2025

You can set up an application using Microsoft Entra ID and authenticate to the Intune Data Warehouse. This process is useful for websites, apps, and background processes where the application should not have access to user credentials. Using the following steps, you authorize your application with Microsoft Entra ID using OAuth 2.0.

Authorization

Microsoft Entra ID uses OAuth 2.0 to enable you to authorize access to web applications and web APIs in your Microsoft Entra tenant. This guide shows you how to authenticate your application using C#. The OAuth 2.0 authorization code flow is described in section 4.1 of the OAuth 2.0 specification. For more information, see Authorize access to web applications using OAuth 2.0 and Microsoft Entra ID.

Azure KeyVault

The following process uses a private method to process and convert an app key. This private method has been named SecureString. As an alternative, you could use Azure KeyVault to store the app key. For more information, see Key Vault.

Create a Web App

In this section, you provide details about the Web app you would like to point to at Intune. A web app is a client-server application. The server provides the web app, which includes the UI, content, and functionality. This type of app is separately maintained on the Web. You use Intune to grant a web app access to Intune. The data flow is initiated by the web app.

1. Sign in to the Microsoft Intune admin center.

2. Select **All services** > **M365 Microsoft Entra ID** > **Microsoft Entra ID** > **App registrations**.

3. Click **New registration** to display the **Register an application** pane.

4. In the **Register an application** pane, add your app details:

- An app name, such as *Intune App-Only Auth*.
- The **Supported account type**.
- The **Redirect URI** of the application. This is the location users automatically navigate to during the authentication process. They are required to prove that they are who they say they are. For more information, see What is application access and single sign-on with Microsoft Entra ID?

5. Click **Register**.

> ⓘ Note
>
> Copy the **Application (client) ID** from the app pane to use later.

Create a key (password)

In this section, Microsoft Entra ID generates a key value for your app.

1. On the **App registrations** pane, select your newly created app to display the app pane.

2. Select **Certificates & secrets** near the top of the pane to display the **Certificates & secrets** pane.

3. Select **Client secrets** on the **Certificates & secrets** pane.

4. Add the key **Description** and an **Expires** duration for the key.

5. Click **Add** to save and update the application's keys.

6. You must copy the generated key value (base64 encoded).

> ⓘ Note
>
> The key value disappears after you leave the **Certificates & secrets** pane. You cannot retrieve the key from this pane later. Copy it to use later.

Grant application permissions

In this section, you grant permissions to the applications.

1. Select **API permissions** > **Add a permission** > **Intune** > **Application permissions**.

2. Choose the **get_data_warehouse** option (*Get data warehouse information from Microsoft Intune*).
3. Click **Add permissions**.
4. Click **Done** from the **Add API access** pane.
5. Click **Grant admin consent** from the **API permissions** pane and click **Yes** when promoted to update any existing permissions this application already has.

Generate token

Using Visual Studio, create a Console App (.NET Framework) project that supports the .NET Framework and uses C# as the coding language.

1. Select **File** > **New** > **Project** to display the **New Project** dialog box.

2. On the left, select **Visual C#** to display all .NET Framework projects.

3. Select **Console App (.NET Framework)**, add an app name, and then click **OK** to create the app.

4. In **Solution Explorer**, select **Program.cs** to display the code.

5. In Solution Explorer, add a reference to the assembly `System.Configuration`.

6. In the pop-up menu, select **Add** > **New item**. The **Add New Item** dialog box is displayed.

7. On the left, under **Visual C#**, select **Code**.

8. Select **Class**, change the name of the class to *IntuneDataWarehouseClass.cs*, and click **Add**.

9. Add the following code within the `Main` method:

   C#

   ```
        var applicationId =
   ConfigurationManager.AppSettings["appId"].ToString();
        SecureString applicationSecret =
   ConvertToSecureStr(ConfigurationManager.AppSettings["appKey"].ToString(
   )); // Load as SecureString from configuration file or secret store
   (i.e. Azure KeyVault)
        var tenantDomain =
   ConfigurationManager.AppSettings["tenantDomain"].ToString();
        var msalContext = new
   AuthenticationContext($"https://login.windows.net/" + tenantDomain +
   "/oauth2/token");
   ```

```
    AuthenticationResult authResult = msalContext.AcquireTokenAsync(
        resource: "https://api.manage.microsoft.com/",
        clientCredential: new ClientCredential(
            applicationId,
            new SecureClientSecret(applicationSecret))).Result;
```

10. Add additional namespaces by adding the following code at the top of the code file:

C#

```
using System.Security;
using Microsoft.Identity.Client;
using System.Configuration;
```

ⓘ Note

You must use the Microsoft Authentication Library (MSAL). For more information, see Update your applications to use Microsoft Authentication Library (MSAL) and Microsoft Graph API.

11. After the `Main` method, add the following private method to process and convert the app key:

C#

```
private static SecureString ConvertToSecureStr(string appkey)
{
    if (appkey == null)
        throw new ArgumentNullException("AppKey must not be null.");

    var secureAppKey = new SecureString();

    foreach (char c in appkey)
        secureAppKey.AppendChar(c);

    secureAppKey.MakeReadOnly();
    return secureAppKey;
}
```

12. In the **Solution Explorer**, right-click on **References**, then select **Manage NuGet Packages**.

13. Search for *Microsoft.Identity.Client* and install the related Microsoft NuGet package.

14. In **Solution Explorer** select and open the *App.config* file.

15. Add the `appSettings` section so that the xml appears as follows:

XML

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <startup>
        <supportedRuntime version="v4.0"
sku=".NETFramework,Version=v4.6.1" />
    </startup>
    <appSettings>
      <add key="appId" value="App ID created from 'Create a Web App'
procedure"/>
      <add key="appKey" value="Key created from 'Create a key'
procedure" />
      <add key="tenantDomain" value="contoso.onmicrosoft.com"/>
    </appSettings>
</configuration>
```

16. Update the `appId`, `appKey`, and `tenantDomain` values to match your unique app-related values.

17. Build your app.

> Note
>
> To see additional implementation code, see Intune-Data-Warehouse code example.

Next Steps

Learn more about Azure Key Vault by reviewing What is Azure Key Vault?

Feedback

Was this page helpful? Yes No

Microsoft Intune Data Warehouse data model

Article • 03/03/2025

The Intune Data Warehouse samples data daily to provide a historical view of your continually changing environment of mobile devices. The view is composed of related entities in time.

Entities: Entity sets

The warehouse exposes data in the following high-level areas:

- App protection enabled apps and usage
- Enrolled devices, properties, and inventory
- Apps and software inventory
- Device configuration and compliance policies

These areas contain the entities that are meaningful to your Intune environment. You find details about the entity sets in the following topics:

- Application
- Date
- Devices
- Intune Management Extension
- Policy
- Mobile App Management (MAM)
- User
- User Device Associations

Relationships: Star-schema model

The warehouse organizes the entities in relationships that are meaningful to the type of questions you want to ask. For example, you can review the number of installations of an in-house developed Android application. The structure of the data warehouse enables you to gain insight into your mobile environment. In turn, analytics tools, such as Microsoft Power BI, can use the Data Warehouse data model to create visualizations and dynamic dashboards.

The entities and relationships use a star-schema model. A star-schema correlates facts over the dimension of time. A *fact* in the context of the model is a quantitative measurement such as the number of devices, number of apps, or time of enrollment. Fact tables store a lot of data. They can get very large, and so they typically limit information to 30 days. A *dimension* provides context to the facts. Where the fact measures what happened, the dimensions indicate to whom it happened. Dimension tables, such as the **User** table, are smaller and can retrain data for longer periods of time than fact tables.

A star-schema model is optimized for flexibility and data analysis so that you can create the reports needed to understand your evolving mobile environment.

Time: Daily snapshots

The warehouse is downstream from your Intune data. Intune takes a daily snapshot at Midnight UTC and stores the snapshot in the warehouse. The duration of held snapshots vary from fact table to fact table. Some may hold seven days, others 30 days, and some even longer durations.

> ⓘ Note
>
> The Data Warehouse does not sync Jamf devices. For more information about Jamf, see Troubleshooting Jamf Pro integration with Microsoft Intune and Data Jamf Pro sends to Intune.

Next steps

- To learn more about how the data warehouse tracks a user's lifetime in Intune, see User lifetime representation in the Intune Data Warehouse.
- To learn more about working with data warehouses in the Create First Data WareHouse ☑ .
- To learn more about working with Power BI and a data warehouse in Create a new Power BI report by importing a dataset ☑ .

Feedback

Was this page helpful? Yes No

Intune Data Warehouse Collections

Article • 03/03/2025

The following Intune Data Warehouse collections provides the properties, descriptions, and examples for v1.0 collections of the Data Warehouse API entities.

appRevisions

The **appRevision** entity lists all the versions of apps.

⛶ Expand table

Property	Description	Example
appKey	Unique identifier of the App.	123
applicationId	Unique identifier of the App - similar to AppKey, but this key is a natural.	b66bc706-ffff-7437-0340-032819502773
revision	The version as mentioned by admin during uploading of the binary.	2
title	Title of the app.	Excel
publisher	Publisher of the app.	Microsoft
uploadState	Upload state of the app.	1
appTypeKey	Reference to AppType described in the following section.	1
vppProgramTypeKey	Reference to VppProgramType described below.	30876
creationTime	The time when this revision was created.	11/23/2016 0:00
modifiedTime	Last time anything related to this revision was changed.	11/23/2016 0:00
size	Size of the binary in bytes.	120,392,000
startDateInclusiveUTC	Date and time in UTC when this App revision was created in the data warehouse.	11/23/2016 0:00
endDateExclusiveUTC	Date and time in UTC when this app revision became obsolete.	11/23/2016 0:00

Property	Description	Example
isCurrent	Indicates whether this App version is current or not in the data warehouse.	True/False
rowLastModifiedDateTimeUTC	Date and time in UTC when this app version was last modified in the data warehouse.	11/23/2016 0:00

appTypes

The **appType** entity lists the installation source of an app.

> ⓘ **Note**
>
> Win32 apps are not included in the Intune Data Warehouse.

Expand table

Property	Description
appTypeID	ID for the type
appTypeKey	Surrogate key for the key
appTypeName	App type

Example

Expand table

AppTypeID	Name	Description
0	Android store app	An Android store app.
1	Android LOB app	An Android line-of-business app.
2	Managed Android store app (MAM)	An Android store app that has management enabled.
3	iOS store app	An iOS store app.
4	iOS LOB app	An iOS line-of-business app.
5	Managed iOS store app (MAM)	An iOSstore app that is management enabled.

AppTypeID	Name	Description
6	Microsoft 365 Apps for enterprise	The Microsoft 365 Apps for Windows 10.
7	Web app	A web app.
8	Windows Phone 8.1 store app	A Windows phone 8.1 store app.
9	Windows store app	A Windows store app.
10	Windows LOB apps	A Windows AppX line-of-business app.
11	Windows Mobile MSI	An MSI line-of-business app.
12	Windows Phone LOB app	A Windows phone line-of-business app.

compliancePolicyStatusDeviceActivities

The following table summarizes the assignment status of compliance policies to devices. It lists the count of devices found in each compliance state.

⛶ Expand table

Property	Description	Example
dateKey	Date key when the summary was created for the compliance policy.	20161204
unknown	Number of devices that are offline or failed to communicate with Intune or Microsoft Entra ID for other reasons.	5
notApplicable	Number of devices where device compliance policies targeted by the admin are not applicable.	201
compliant	Number of devices that successfully applied one or more device compliance policies targeted by the admin.	4083
inGracePeriod	Number of devices that are not compliant but that are in the grace-period defined by the admin.	57
nonCompliant	Number of devices that failed to apply one or more device compliance policies targeted by the admin or where the user hasn't complied with the policies targeted by the admin.	43
error	Number of devices that failed to communicate with Intune or Microsoft Entra ID, and returned an error message.	3

compliancePolicyStatusDevicePerPolicyActivities

The following table summarizes the assignment status of compliance policies to devices on a per policy and a per policy type basis. It lists the count of devices found in each compliance state for each assigned compliance policy.

Expand table

Property	Description	Example
dateKey	Date key when the summary was created for the compliance policy.	20161219
policyKey	Key for the compliance policy for which the summary was created.	10178
policyPlatformKey	Key for the platform type of the compliance policy for which the summary was created.	5
unknown	Number of devices that are offline or failed to communicate with Intune or Microsoft Entra ID for other reasons.	13
notApplicable	Number of devices where device compliance policies targeted by the admin are not applicable.	3
compliant	Number of devices that successfully applied one or more device compliance policies targeted by the admin.	45
inGracePeriod	Number of devices that are not compliant but that are in the grace-period defined by the admin.	3
nonCompliant	Number of devices that failed to apply one or more device compliance policies targeted by the admin or where the user hasn't complied with the policies targeted by the admin.	7
error	Number of devices that failed to communicate with Intune or Microsoft Entra ID, and returned an error message.	3

complianceStates

Expand table

Property	Description
complianceStatus	Compliance status of devices with mdmStatusKey
complianceStateKey	Compliance key to match device and compliance status
complianceStateID	The ID to match this compliance state

Example

⛶ Expand table

complianceStatus	Description
Unknown	Unknown.
Compliant	Compliant.
Noncompliant	Device is non-compliant and is blocked from corporate resources.
Conflict	Conflict with other rules.
Error	Error.
ConfigManager	Managed by Config Manager.
InGracePeriod	Device is non-compliant but still has access to corporate resources

dates

The **date** entity represents dates that are referenced across multiple data warehouse entities.

⛶ Expand table

Property	Description	Example
dateKey	Unique identifier for this date in the data warehouse.	20160703
fullDate	This date represented in full Date/Time format.	7/3/2016 0:00
dayOfWeek	Day of week	1
dayOfMonth	Day of month	3
dayOfYear	Day of year	185
weekOfYear	Week of year	28
monthOfYear	Month of the year	7
calendarQuarter	Calendar quarter	3
calendarYear	Calendar year	2016
dateKey	Unique identifier for this date in the data warehouse.	20160703

Property	Description	Example
fullDate	This date represented in full Date/Time format.	7/3/2016 0:00
dayOfWeek	Day of week	1
dayOfMonth	Day of month	3
dayOfYear	Day of year	185
weekOfYear	Week of year	28
monthOfYear	Month of the year	7
calendarQuarter	Calendar quarter	3
calendarYear	Calendar year	2016

deviceCategories

Expand table

Property	Description	Example
deviceCategoryID	Unique identifier for the device category.	fb415ba2-7c08-41f6-a5e5-685b50da2c4c
deviceCategoryKey	Unique identifier of the device category in the data warehouse - surrogate key	1
deviceCategoryName	Display name for the device category.	Smartphones

deviceConfigurationProfileDeviceActivities

The **DeviceConfigurationProfileDeviceActivity** entity lists the number of devices in the succeeded, pending, failed, or error state per day. The number reflects the Device configuration profiles assigned to the entity. For example, if a device is in the succeeded state for all its assigned policies, it increments the succeeded counter up one for that day. If a device has two profiles assigned to it, one in the succeeded state and another in an error state, the entity increments the Succeeded counter and place the device in the error state. The entity lists how many devices are in which state on a given day over the last 30 days.

Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703
pending	Number of unique Devices in pending state.	123
succeeded	Number of unique Devices in success state.	12
error	Number of unique Devices in error state.	10
failed	Number of unique Devices in failed state.	2

deviceConfigurationProfileUserActivities

The **DeviceConfigurationProfileUserActivity** entity lists the number of users in the succeeded, pending, failed, or error state per day. The number reflects the Device configuration profiles assigned to the entity. For example, if a user is in the succeeded state for all their assigned policies, it moves up the succeeded counter by one for that day. If a user has two profiles assigned to them, one in the succeeded state and the other is in an error state, the user in the error state is counted. The **DeviceConfigurationProfileUserActivity** entity lists how many users are in which state on a given day over the last 30 days.

⛶ Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703
pending	Number of unique Users in pending state.	123
succeeded	Number of unique Users in success state.	12
error	Number of unique Users in error state.	10
failed	Number of unique Users in failed state.	2

devicePropertyHistories

⛶ Expand table

Property	Description
dateKey	Reference to date table indicating the day.
deviceKey	Unique identifier of the device in the data warehouse - surrogate key. This is a reference to the Device table that contains the Intune device ID.
deviceName	Name of the device on platforms that allow naming a device. On other platforms, Intune creates a name from other properties. This attribute cannot be available for all devices.
deviceRegistrationStateKey	Key of the device registration state attribute for this device.
ownerTypeKey	Key of the owner type attribute for this device: corporate, personal, or unknown.
managementStateKey	Key of the management state associated with this device, indicating latest state of a remote action or if it was jailbroken/rooted.
azureADRegistered	Whether the device is Microsoft Entra registered.
complianceStateKey	A key to ComplianceState.
oSVersion	OS version.
jailBroken	Whether the device is jail broken or rooted.
deviceCategoryKey	Key of device category attribute for this device.
physicalMemoryInBytes	The physical memory in bytes.
totalStorageSpaceInBytes	Total storage capacity in bytes.

deviceRegistrationStates

The **DeviceRegistrationState** entity represents the registration type referenced by other data warehouse collections.

Expand table

Property	Description
deviceRegistrationStateID	Unique identifier for registration state
deviceRegistrationStateKey	Unique identifier of the registration state in the data warehouse - surrogate key
deviceRegistrationStateName	Registration state

Property	Description
notRegistered	Not registered
registered	Registered
revoked	State means the IT administrator has blocked the client, and the client can be unblocked. A device can also be in the Revoked state after it is wiped or retired.
keyConflict	Key conflict
approvalPending	Approval pending
certificateReset	Reset certificate
notRegisteredPendingEnrollment	Not registered pending enrollment
unknown	Unknown state

devices

The **device** entity lists all enrolled devices under management and their corresponding properties.

Expand table

Property	Description
deviceKey	Unique identifier of the device in the data warehouse - surrogate key.
deviceId	Unique identifier of the device.
deviceName	Name of the device on platforms that allow naming a device. On other platforms, Intune creates a name from other properties. This attribute cannot be available for all devices.
deviceTypeKey	Key of the device type attribute for this device.
deviceRegistrationState	Key of the client registration state attribute for this device.
ownerTypeKey	Key of the owner type attribute for this device: corporate, personal, or unknown.
enrolledDateTime	Date and time that this device was enrolled.
ethernetMacAddress	The unique network identifier of this device.
lastSyncDateTime	Last known device check-in with Intune.

Property	Description
managementAgentKey	Key of the management agent associated with this device.
managementStateKey	Key of the management state associated with this device, indicating latest state of a remote action or if it was jailbroken/rooted.
azureADDeviceId	The Azure deviceID for this device.
azureADRegistered	Whether the device is Microsoft Entra registered.
deviceCategoryKey	Key of the category associated with this device.
deviceEnrollmentType	Key of the enrollment type associated with this device, indicating method of enrollment.
complianceStateKey	Key of the Compliance state associated with this device.
office365Version	The version of Microsoft 365 that is installed on the device.
oSVersion	Operating system version of the device.
easDeviceId	Exchange ActiveSync ID of the device.
serialNumber	SerialNumber
userId	Unique Identifier for the user associated with the device.
rowLastModifiedDateTimeUTC	Date and time in UTC when this device was last modified in the data warehouse.
manufacturer	Manufacturer of the device
model	Model of the device
operatingSystem	Operating system of the device. Windows, iOS/iPadOS, etc.
isDeleted	Binary to show whether the device is deleted or not.
androidSecurityPatchLevel	Android security patch level
mEID	MEID
isSupervised	Device supervised status
freeStorageSpaceInBytes	Free Storage in bytes.
encryptionState	Encryption state on the device.
subscriberCarrier	Subscriber carrier of the device
phoneNumber	Phone number of the device

Property	Description
iMEI	IMEI
cellularTechnology	Cellular technology of the device.
wiFiMacAddress	Wi-Fi MAC.
windowsOsEdition	Windows Operating System edition.

ⓘ Note

For more information about Windows SKU enum values, see Device properties.

deviceTypes

The **deviceType** entity represents the device type referenced by other data warehouse entities. The device type typically describes either the device model, manufacturer, or a combination of both.

⛶ Expand table

Property	Description
deviceTypeID	Unique identifier of the device type
deviceTypeKey	Unique identifier of the device type in the data warehouse - surrogate key
deviceTypeName	Device type

Example

⛶ Expand table

deviceTypeID	Name	Description
-1	Not Available	The device type is unavailable.
0	Desktop	Windows Desktop device
1	Windows	Windows device
2	WinMO6	Windows Mobile 6.0 device
3	Nokia	Nokia device

deviceTypeID	Name	Description
4	WindowsPhone	Windows Phone device
5	Mac	Mac device
6	WinCE	Windows CE device
7	WinEmbedded	Windows Embedded device
8	IPhone	iPhone device
9	IPad	iPad device
10	IPod	iPod device
11	Android	Android device-managed using Device Administrator
12	ISocConsumer	iSoc Consumer device
13	Unix	Unix Device
14	MacMDM	OS X device managed with the built-in MDM agent
15	HoloLens	HoloLens device
16	SurfaceHub	Surface Hub device
17	AndroidForWork	Android device-managed using Android Profile Owner
18	AndroidEnterprise	Android enterprise device.
100	Blackberry	Blackberry Device
101	Palm	Palm device
255	Unknown	Unknown device type

deviceEnrollmentTypes

The **deviceEnrollmentType** entity indicates how a device was enrolled. The enrollment type captures the method of enrollment. Examples list the different enrollment types and what they mean.

Expand table

Property	Description
deviceEnrollmentTypeID	Unique identifier of the enrollment type.

Property	Description
deviceEnrollmentTypeKey	Unique identifier of the enrollment type in the data warehouse - surrogate key.
deviceEnrollmentTypeName	Enrollment type name.

Example

⛶ Expand table

enrollmentTypeID	Name	Description
0	Unknown	Enrollment type was not collected
1	UserEnrollment	User driven enrollment through BYOD channel.
2	DeviceEnrollmentManager	User enrollment with a device enrollment manager account.
3	AppleBulkWithUser	Apple bulk enrollment with user challenge. (DEP, Apple Configurator)
4	AppleBulkWithoutUser	Apple bulk enrollment without user challenge. (DEP, Apple Configurator, Mobile Config)
5	WindowsAzureADJoin	Windows 10 Microsoft Entra join.
6	WindowsBulkUserless	Windows 10 Bulk enrollment through ICD with certificate.
7	WindowsAutoEnrollment	Windows 10 automatic enrollment. (Add work account)
8	WindowsBulkAzureDomainJoin	Windows 10 bulk Microsoft Entra join.
9	WindowsCoManagement	Windows 10 co-management triggered by Autopilot or Group Policy.
10	WindowsAzureADJoinsUsingDeviceAuth	Windows 10 Microsoft Entra join using Device Auth.

enrollmentActivities

The **EnrollmentActivity** entity indicates the activity of a device enrollment.

Expand table

Property	Description
dateKey	Key of the date when this enrollment activity was recorded.
deviceEnrollmentTypeKey	Key of the type of the enrollment.
deviceTypeKey	Key of the type of device.
enrollmentEventStatusKey	Key of the status indicating the success or failure of the enrollment.
enrollmentFailureCategoryKey	Key of the enrollment failure category (if the enrollment failed).
enrollmentFailureReasonKey	Key of the enrollment failure reason (if the enrollment failed).
osVersion	The operating system version of the device.
count	Total count of enrollment activities matching the classifications above.

enrollmentEventStatuses

The **EnrollmentEventStatus** entity indicates the result of a device enrollment.

Expand table

Property	Description
enrollmentEventStatusKey	Unique identifier of the enrollment status in the data warehouse (surrogate key)
enrollmentEventStatusName	The name of the enrollment status. See examples below.

Example

Expand table

enrollmentEventStatusName	Description
Success	A successful device enrollment

enrollmentEventStatusName	Description
Failed	A failed device enrollment
Not Available	The enrollment status is unavailable.

enrollmentFailureCategories

The **EnrollmentFailureCategory** entity indicates why a device enrollment failed.

⛶ Expand table

Property	Description
enrollmentFailureCategoryKey	Unique identifier of the enrollment failure category in the data warehouse (surrogate key)
enrollmentFailureCategoryName	The name of the enrollment failure category. See examples below.

Example

⛶ Expand table

enrollmentFailureCategoryName	Description
Not Applicable	The enrollment failure category is not applicable.
Not Available	The enrollment failure category is not available.
Unknown	Unknown error.
Authentication	Authentication failed.
Authorization	Call was authenticated, but not authorized to enroll.
AccountValidation	Failed to validate the account for enrollment. (Account blocked, enrollment not enabled)
UserValidation	User could not be validated. (User does not exist, missing license)
DeviceNotSupported	Device is not supported for mobile device management.
InMaintenance	Account is in maintenance.
BadRequest	Client sent a request that is not understood/supported by

enrollmentFailureCategoryName	Description
	the service.
FeatureNotSupported	Feature(s) used by this enrollment are not supported for this account.
EnrollmentRestrictionsEnforced	Enrollment restrictions configured by admin blocked this enrollment.
ClientDisconnected	Client timed out or enrollment was aborted by end user.
UserAbandonment	Enrollment was abandoned by end user. (End user started onboarding but failed to complete it in timely manner)

enrollmentFailureReasons

The **EnrollmentFailureReason** entity indicates a more detailed reason for a device enrollment failure within a given failure category.

Expand table

Property	Description
enrollmentFailureReasonKey	Unique identifier of the enrollment failure reason in the data warehouse (surrogate key)
enrollmentFailureReasonName	The name of the enrollment failure reason. See examples below.

Example

Expand table

enrollmentFailureReasonName	Description
Not Applicable	The enrollment failure reason is not applicable.
Not Available	The enrollment failure reason is not available.
Unknown	Unknown Error.
UserNotLicensed	The user was not found in Intune or does not have a valid license.
UserUnknown	User is not known to Intune.
BulkAlreadyEnrolledDevice	Only one user can enroll a device. This device was

enrollmentFailureReasonName	Description
	previously enrolled by another user.
EnrollmentOnboardingIssue	Intune mobile device management (MDM) authority is not configured yet.
AppleChallengeIssue	The iOS management profile installation was delayed or failed.
AppleOnboardingIssue	An Apple MDM push certificate is required to enroll into Intune.
DeviceCap	The user attempted to enroll more devices than maximum allowed.
AuthenticationRequirementNotMet	Intune enrollment service failed to authorize this request.
UnsupportedDeviceType	This device does not meet minimum requirements for Intune enrollment.
EnrollmentCriteriaNotMet	This device failed to enroll due to a configured enrollment restriction rule.
BulkDeviceNotPreregistered	This device's international mobile equipment identifier (IMEI) or serial number wasn't found. Without this identifier, devices are recognized as personal-owned devices which are currently blocked.
FeatureNotSupported	The user was attempting to access a feature that is not yet released for all customers or is not compatible with your Intune configuration.
UserAbandonment	Enrollment was abandoned by end user. (End user started onboarding but failed to complete it in timely manner)
APNSCertificateExpired	Apple devices cannot be managed with an expired Apple MDM push certificate.

intuneManagementExtensions

The **intuneManagementExtension** lists the **intuneManagementExtension** health on each Windows 10 device per day. The data is retained for the last 60 days.

Expand table

Property	Description	Example
dateKey	Unique identifier of the Date.	123

Property	Description	Example
tenantKey	Unique identifier of the Tenant.	456
deviceKey	Unique identifier of the Device.	789
extensionVersionKey	Unique identifier of the IntuneManagementExtension version.	1
extensionStateKey	Unique identifier of health state.	2

intuneManagementExtensionHealthStates

The **IntuneManagementExtensionHealthState** lists all possible health states of the **IntuneManagementExtension**.

⛶ Expand table

Property	Description	Example
extensionStateKey	Unique identifier of health state.	2
extensionState	Health state of a IntuneManagementExtension.	Healthy

intuneManagementExtensionVersions

The **IntuneManagementExtensionVersion** entity lists all the versions used by **IntuneManagementExtension**.

⛶ Expand table

Property	Description	Example
extensionVersionKey	Unique identifier of the IntuneManagementExtension version.	1
extensionVersion	The 4 digit version number.	1.0.2.0

MamApplications

The **MamApplication** entity lists Line-of-Business (LOB) apps that are managed through Mobile Application Management (MAM) without enrollment in your enterprise.

⛶ Expand table

Property	Description	Example
mamApplicationKey	Unique identifier of the MAM application.	432
mamApplicationName	Name of the MAM application.	MAM Application Example Name
mamApplicationId	Application ID of the MAM application.	123
isDeleted	Indicates whether this MAM app record has been updated. True- MAM app has a new record with updated fields in this table. False- the latest record for this MAM app.	True/False
startDateInclusiveUTC	Date and time in UTC when this MAM app was created in the data warehouse.	11/23/2016 12:00:00 AM
deletedDateUTC	Date and time in UTC when IsDeleted changed to True.	11/23/2016 12:00:00 AM
rowLastModifiedDateTimeUTC	Date and time in UTC when this MAM app was last modified in the data warehouse.	11/23/2016 12:00:00 AM

MamApplicationInstances

The **MamApplicationInstance** entity lists managed Mobile Application Management (MAM) apps as singular instances per user per device. All users and devices listed with in the entity are protected, as in, they have at least one MAM Policy assigned to them.

Expand table

Property	Description	Example
applicationInstanceKey	Unique identifier of the MAM app instance in the data warehouse - surrogate key.	123
userId	User ID of the user who has this MAM app installed.	b66bc706-ffff-7437-0340-032819502773
applicationInstanceId	Unique identifier of the MAM app instance - similar to ApplicationInstanceKey, but the identifier is a natural key.	b66bc706-ffff-7437-0340-032819502773
mamApplicationId	Application ID of the Mam Application for which this Mam Application Instance was	11/23/2016 12:00:00 AM

Property	Description	Example
	created.	
applicationVersion	Application version of this MAM app.	2
createdDate	Date when this record of the MAM app instance was created. Value can be null.	11/23/2016 12:00:00 AM
platform	Platform of the device on which this MAM app is installed.	2
platformVersion	Platform version of the device on which this MAM app is installed.	2.2
sdkVersion	The MAM SDK version that this MAM app was wrapped with.	3.2
mamDeviceId	Device ID of the device with which MAM Application Instance is associated with.	11/23/2016 12:00:00 AM
mamDeviceType	Device type of the device with which MAM Application Instance is associated with.	11/23/2016 12:00:00 AM
mamDeviceName	Device name of the device with which MAM Application Instance is associated with.	11/23/2016 12:00:00 AM
isDeleted	Indicates whether this MAM app instance record has been updated. True- this MAM app instance has a new record with updated fields in this table. False - the latest record for this MAM app instance.	True/False
startDateInclusiveUtc	Date and time in UTC when this MAM app instance was created in the data warehouse.	11/23/2016 12:00:00 AM
deletedDateUtc	Date and time in UTC when IsDeleted changed to True.	11/23/2016 12:00:00 AM
rowLastModifiedDateTimeUtc	Date and time in UTC when this MAM app instance was last modified in the data warehouse.	11/23/2016 12:00:00 AM

MamCheckins

The **MamCheckin** entity represents data gathered when a Mobile Application Management (MAM) app instance has checked in with the Intune Service.

ⓘ Note

When an app instance checks in multiple times a day, the data warehouse stores it as single check-in.

⛶ Expand table

Property	Description	Example
dateKey	Date Key when the MAM app check-in was recorded in the data warehouse.	20160703
applicationInstanceKey	Key of the app instance associated with this MAM app check-in.	123
userKey	Key of the user associated with this MAM app check-in.	4323
mamApplicationKey	Application Key of Application associated with MAM Application check in.	432
deviceHealthKey	Key of DeviceHealth associated with this MAM app check-in.	321
platformKey	Represents the platform of the device associated with this MAM app check-in.	123
lastCheckInDate	Date and time when this MAM app last checked in. Value can be null.	11/23/2016 12:00:00 AM

MamDeviceHealths

The **MamDeviceHealth** entity represents devices that have Mobile Application Management (MAM) policies deployed to them even if they are jailbroken.

⛶ Expand table

Property	Description	Example
deviceHealthKey	Unique identifier of the device and its associated health in the data warehouse - surrogate key.	123
deviceHealth	Unique identifier of the device and its associated health - similar to	b66bc706-ffff-7777-0340-032819502773

Property	Description	Example
	DeviceHealthKey, but the identifier is a natural key.	
deviceHealthName	Represents the status of the device. Not available - no information on this device. Healthy - device is not jailbroken. Unhealthy - device is jailbroken.	Not Available Healthy Unhealthy
rowLastModifiedDateTimeUtc	Date and time in UTC when this specific MAM Device Health was last modified in the data warehouse.	11/23/2016 12:00:00 AM

MamPlatforms

The **MamPlatform** entity lists platform names and types on which a Mobile Application Management (MAM) app was installed.

Expand table

Property	Description	Example
platformKey	Unique identifier of the platform in the data warehouse - surrogate key.	123
platform	Unique identifier of the platform - similar to PlatformKey, but is a natural key.	123
platformName	Platform name	Not Available None Windows IOS Android.
rowLastModifiedDateTimeUtc	Date and time in UTC when this platform was last modified in the data warehouse.	11/23/2016 12:00:00 AM

managementAgentTypes

The **managementAgentType** entity represents the agents used to manage a device.

Expand table

Property	Description
managementAgentTypeID	Unique identifier of the management agent type.
managementAgentTypeKey	Unique identifier of the management agent type in the data warehouse - surrogate key.
managementAgentTypeName	Indicates what kind of agent is used to manage the device.

Example

Expand table

ManagementAgentTypeID	Name	Description
1	EAS	The device is managed through Exchange Active Sync
2	MDM	The device is managed using an MDM agent
3	EasMdm	The device is managed by both Exchange Active Sync and an MDM agent
4	IntuneClient	The device is managed by the Intune PC agent
5	EasIntuneClient	The device is managed by both Exchange Active Sync and the Intune PC agent
8	ConfigManagerClient	The device is managed by the Configuration Manager agent
10	ConfigurationManagerClientMdm	The device is managed by Configuration Manager and MDM.
11	ConfigurationManagerCLientMdmEas	The device is managed by Configuration Manager, MDM and Exchange Active Sync.
16	Unknown	Unknown management agent type

ManagementAgentTypeID	Name	Description
64	GoogleCloudDevicePolicyController	The device is managed by Google's CloudDPC.

managementStates

The **ManagementState** entity provides details on the state of the device. Detail can be useful in the cases where remote actions are applied, the device is jailbroken, or rooted.

⛶ Expand table

Property	Description
managementStateID	Unique identifier of the management state.
managementStateKey	Unique identifier of the management state in the data warehouse - surrogate key.
managementStateName	Indicates the state of the remote action applied to this device.

Example

⛶ Expand table

managementStateID	Name	Description
0	Managed	Managed with no pending remote actions.
1	RetirePending	There is a retire command pending for the device.
2	RetireFailed	The retire command failed on the device.
3	WipePending	There is a wipe command pending for the device.
4	WipeFailed	The wipe command failed on the device.
5	Unhealthy	Unhealthy state.
6	DeletePending	There is a delete command pending for the device.
7	RetireIssued	A retire command has been issued to the device.
8	WipeIssued	A wipe command has been issued.
9	WipeCanceled	Wipe command has been canceled.

managementStateID	Name	Description
10	RetireCanceled	Retire command has been canceled.
11	Discovered	The device is newly discovered by Intune, once it checks in for the first time it moves to -Managed- state.

mobileAppInstallStates

The MobileAppInstallState entity represents the install state for a mobile application after it has been assigned to a group containing devices, users or both.

Expand table

Property	Description
appInstallStateKey	The unique ID of the app install state for your account.
appInstallState	Enum value of the app install state.
appInstallStateName	Name of the app install state.

mobileAppInstallStatusCounts

Represents a mobile app install status for a given target device type using Mobile Application Management through Microsoft Intune.

Expand table

Property	Description
dateKey	Key of the date when the app install status was recorded.
appKey	Key of the mobile app used to identify an instance of AppRevision.
deviceTypeKey	Key of the Device Type associated with the Mobile Application.
appInstallStateKey	Key of the app install state used to identify an instance of MobileAppInstallState.
errorCode	The error code returned by the app installer, the mobile platform or the service pertaining to the installation of the app.
count	Total count.

ownerTypes

The **ownerType** entity indicates whether a device is corporate, personally owned, or unknown.

Expand table

Property	Description	Example
ownerTypeID	Unique identifier of the owner type.	
ownerTypeKey	Unique identifier of the owner type in the data warehouse - surrogate key.	
ownerTypeName	Represents the owner type of the devices: Corporate - Device is enterprise owned. Personal - Device is personally owned (BYOD). Unknown - No information on this device.	Corporate Personal Unknown

> Note
>
> For the `ownerTypeName` filter in AzureAD when creating Dynamic Groups for devices, you need to set the value `deviceOwnership` as `Company`. For more information, see Rules for devices.

policies

The **Policy** entity lists device configuration profiles, app configuration profiles, and compliance policies. You can assign the policies with Mobile Device Management (MDM) to a group in your enterprise.

Expand table

Property	Description	Example
policyKey	Unique Key to represent the policy in the data warehouse.	123
policyId	Unique identifier of the Policy in the data warehouse.	b66bc706-ffff-7437-0340-032819502773
policyName	Name of the Policy.	"Windows 10 Baseline"
policyVersion	Version of the Policy. When the policy is edited or changed, a newer version is	1, 2, 3

Property	Description	Example
	created.	
isDeleted	Indicates whether the Policy record has been updated. True - Policy has a new record with updated fields. False- The latest record for the policy.	True/False
startDateInclusiveUTC	Date and time in UTC when the policy was created in the data warehouse.	11/23/2016 0:00
deletedDateUTC	Date and time in UTC when IsDeleted changed to True.	11/23/2016 0:00
rowLastModifiedDateTimeUTC	Date and time in UTC when the policy was last modified in the data warehouse.	11/23/2016 0:00

policyDeviceActivities

The following table lists the number of devices in the succeeded, pending, failed, or error state per day. The number reflects the data per Policy Type profiles. For example, if a device is in the succeeded state for all its assigned policies, it increments the succeeded counter up one for that day. If a device has two profiles assigned to it, one in the succeeded state and another in an error state, the entity increments the Succeeded counter and place the device in the error state. The **policyDeviceActivity** entity lists how many devices are in which state on a given day over the last 30 days.

⛶ Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703
pending	Number of unique Devices in pending state.	123
succeeded	Number of unique Devices in success state.	12
policyKey	Policy Key, can be joined with Policy to get the policyName.	Windows 10 baseline
error	Number of unique Devices in error state.	10
failed	Number of unique Devices in failed state.	2

policyPlatformTypes

⛶ Expand table

Property	Description	Example
policyPlatformTypeKey	The unique key for the policy platform type.	20170519
policyPlatformTypeId	The unique identifier for the policy platform type.	1
policyPlatformTypeName	The name for the policy platform type.	AndroidForWork

policyTypeActivities

The **PolicyTypeActivity** entity lists the cumulative number of devices in the succeeded, pending, failed, or error state. It lists these states with respect to a device configuration profile, app configuration profile, or compliance policy per day.

⛶ Expand table

Property	Description	Example
dateKey	Date Key when the device Configuration profile check-in was recorded in the data warehouse.	20160703
policyKey	Policy Key, can be joined with Policy to get the policyName.	Windows 10 baseline
policyTypeKey	Type of Policy Key, can be joined with Policy Type to get the policy type name.	Windows10 Compliance Policy
pending	Number of unique devices in pending state.	123
succeeded	Number of unique devices in success state.	12
error	Number of unique devices in error state.	10
failed	Number of unique devices in failed state.	2

policyTypes

The **PolicyType** entity lists types of device configuration profiles, app configuration profiles, and Compliance policies. You can assign the policies with Mobile Device Management (MDM) to a group in your enterprise.

⛶ Expand table

Property	Description	Example
policyTypeId	Unique identifier of the policy in the source system.	123
policyTypeKey	Unique identifier of the policy in the data warehouse.	1
policyTypeName	Name of the policy type.	Windows 10 Compliance policy.

policyUserActivities

The following table lists the number of users in the succeeded, pending, failed, or error state per day. The number reflects the data per Policy Type profiles. For example, if a user is in the succeeded state for all their assigned policies, it moves up the succeeded counter by one for that day. If a user has two profiles assigned to them, one in the succeeded state and the other is in an error state, the user in the error state is counted. The **PolicyUserActivity** entity lists how many users are in which state on a given day over the last 30 days.

⛶ Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703
pending	Number of unique Devices in pending state.	123
succeeded	Number of unique Devices in success state.	12
policyKey	Policy Key, can be joined with Policy to get the policyName.	Windows 10 baseline
error	Number of unique Devices in error state.	10

termsAndConditions

A **termsAndConditions** entity represents the metadata and contents of a given Terms and Conditions (T&C) policy. The contents of T&C policies are presented to users upon their first attempt to enroll into Intune and subsequently upon edits where an administrator has required re-acceptance. They enable administrators to communicate the provisions to which a user must agree in order to have devices enrolled into Intune.

⛶ Expand table

Property	Description	Example
termsAndConditionsKey	A key corresponding to an entry in the 'userTermsAndConditionsAcceptances' collection	123
termsAndCondidionsId	The ID for this termsAndConditions entry	276edcb7-7440-4339-b6c5-8b6fc556fee6
termsAndConditionsVersion	The version of this terms and conditions entry	1
name	The name of this termsAndConditions entry.	Intune terms of use
description	The description for these terms and conditions.	
title	The title for these terms and conditions.	Device management corporate policy
summaryOfTerms	The summary of terms given to the user.	I agree to the terms and conditions.
termsAndConditionsBodyText	The body of text for these terms and conditions.	*Device encryption* Enforcement of 6 digits PIN
isDeleted	True or false value for whether this value is deleted.	False
startDateInclusiveUTC	The start date of these terms and conditions.	8/23/2018 4:01:34 AM
endDateEclusiveUTC	The end date of these terms and conditions.	12/31/9999 12:00:00 AM

userDeviceAssociations

The **UserDeviceAssociation** entity contains user device associations in your organization.

⛶ Expand table

Name	Description	Example
userKey	Unique identifier of the user in the data warehouse. (Surrogate key).	123
deviceKey	Unique identifier of the device in the data warehouse.	123
createdDateTimeUTC	Date and time when the user device association was created. Uses UTC format.	11/23/2016 0:00
isDeleted	Indicates that the user unenrolled that device, and that the association is not current anymore.	True/False
endedDateTimeUTC	Date and time in UTC when IsDeleted changed to True.	6/23/2017 0:00

users

The **user** entity lists all the Microsoft Entra users with assigned licenses in your enterprise.

The **user** entity collection contains user data. These records include user states during the data collection period, even if the user has been removed. For example, a user may be added to Intune and then removed during the course of the last month. While this user is not present at the time of the report, the user and state are present in the data from the prior month. You could create a report that would show the duration of the user's historic presence in your data.

⛶ Expand table

Property	Description	Example
userKey	Unique identifier of the user in the data warehouse - surrogate key.	123
userId	Unique identifier of the user - similar to UserKey, but is a natural key.	b66bc706-ffff-7437-0340-032819502773
userEmail	Email address of the user.	John@constoso.com
userPrincipalName	User principal name of the user.	John@constoso.com
displayName	Display name of the user.	John
intuneLicensed	Specifies if this user is Intune licensed	True/False

Property	Description	Example
	or not.	
isDeleted	Indicates whether all of the user's licenses have expired and whether the user was therefore removed from Intune. For a single record, this flag does not change. Instead, a new record is created for a new user state.	True/False
rowLastModifiedDateTimeUTC	Date and time in UTC when the record was last modified in the data warehouse	11/23/2016 0:00

userTermsAndConditionsAcceptances

A **userTermsAndConditionsAcceptance** entity represents the acceptance status of a given Terms and Conditions (T&C) policy by a given user. Users must accept the most up-to-date version of the terms in order to retain access to the Company Portal.

⛶ Expand table

Property	Description	Example
dateKey	A key corresponding to a date values in the 'dates' collection.	20180823
userKey	A user key mapping to a user in the 'users' collection.	20000
termsAndConditionsKey	A key corresponding to an entry in the 'termsAndConditions' collection	1
acceptedDateTimeUTC	The time that the user accepted these terms and conditions	8/23/2018 4:01:34 AM
lastModifiedDateTimeUTC	The last time that this entry was modified.	8/23/2018 4:01:34 AM

vppProgramTypes

The **vppProgramType** entity lists possible VPP program types for an app.

⛶ Expand table

Property	Description
vppProgramTypeID	ID for the type.
vppProgramTypeKey	Surrogate key for the key.
vppProgramTypeName	VPP Program type.

Example

⛶ Expand table

VppProgramID	Name	Description
3DDA2474-470B-4503-9830-2665C21C1945	Microsoft	Microsoft's VPP program.
00000000-0000-0000-0000-000000000000	Not Yet Available	Default value, No VPP.
B54814E0-68EA-4BA4-8088-B5AAB58E737B	Apple	Apple's VPP program.

Next steps

For more about the Intune Data Warehouse, see Data Warehouse data model.

Feedback

Was this page helpful? Yes No

User lifetime representation in the Microsoft Intune Data Warehouse

Article • 03/03/2025

You can use the month of data snapshots stored in the Intune Data Warehouse to answer questions about time-based trends. For example, you can look at the number of users being added over a month. You might also ask about the number of users who have been removed from the system.

To provide this type insight, the data warehouse stores historical information. The data warehouse can track the lifetime of an entity. The warehouse records when an entity was created, when the state of the entity changes, and when an entity is deleted. With the history captured with daily snapshots of quantitative measurements, you can compare one day to the previous day, and so on.

Working with entity lifetimes can be confusing since your entities are changing state. That means if you look at a snapshot on day 30, a user record may not exist in an active state in the data. On day 29 the entity record may exist as active. And then before day 28, the user didn't exist at all.

This scenario may be clearer if you walk through the lifetime of an entity.

Assume a user, **John Smith**, gets assigned a license on 06/01/2017, then the **User** table would have the following entry:

Expand table

DisplayName	IsDeleted	StartDateInclusiveUTC	EndDateExclusiveUTC	IsCurrent
John Smith	FALSE	06/01/2017	12/31/9999	TRUE

John Smith gives up his license on 07/25/2017. The **User** table has the following entries. Changes in existing records are `marked`.

Expand table

DisplayName	IsDeleted	StartDateInclusiveUTC	EndDateExclusiveUTC	IsCurrent
John Smith	FALSE	06/01/2017	`07/26/2017`	`FALSE`
John Smith	TRUE	07/26/2017	12/31/9999	TRUE

The first row indicates John Smith existed in Intune from 06/01/2017 to 07/25/2017. The second record indicates that the user was deleted on 07/25/2017 and is no longer present in Intune.

Now let assume John Smith gets a new license assigned on 08/31/2017, then the User table would have the following entries:

⛶ Expand table

DisplayName	IsDeleted	StartDateInclusiveUTC	EndDateExclusiveUTC	IsCurrent
John Smith	FALSE	06/01/2017	07/26/2017	FALSE
John Smith	TRUE	07/26/2017	`08/31/2017`	`FALSE`
John Smith	FALSE	08/31/2017	12/31/9999	TRUE

A person wanting to see the current state of all users would want to apply a filter where `IsCurrent = TRUE`.

A person wanting to see only existing users would want to apply a filter where `IsCurrent = TRUE AND IsDeleted = FALSE`.

Dimension tables in the entity lifetime

In order to store the history of state changes in entities, Intune doesn't delete records. Instead it marks the record as deleted. This is called a soft-delete. The dimension tables use various metadata columns to track the lifetime of records.

The most commonly used metadata columns are:

⛶ Expand table

Metadata Property Name	Interpretation of Values
IsDeleted	Indicates whether the entity was deleted in Intune.
StartDateInclusiveUTC	The UTC date the entity was loaded into the Intune Data Warehouse. The entity may have been created before it was imported into the Intune Data Warehouse.
DeletedDateUTC	The UTC date that the entity was deleted in Intune.

Any metadata column starting with the prefix **Row**, such as **RowLastModifiedDateTimeUTC**, indicates when a record was created or modified in the Intune Data Warehouse. The warehouse is downstream from the data in Intune. This value has no relationship to the lifetime of the entity in Intune.

Any person wanting to see only those dimension entities that currently exist would want to apply a filter where **IsDeleted** = **FALSE**.

Next steps

- To learn more about the **Current User** entity, see Reference for current user entity.
- To learn more about the **User** entity, see Reference for user entity.

Feedback

Was this page helpful? Yes No

Reference for application entities

Article • 03/03/2025

The **Application** category contains entities for devices that track information such as:

- Versions of an app
- Installation source of an app
- Type of developers who created an app
- Managed software types for an app, for example **sidecar** or **desktop**
- Volume Purchasing Program (VPP) state of an app

appRevisions

The **appRevision** entity lists all the versions of apps.

Expand table

Property	Description	Example
appKey	Unique identifier of the App.	123
applicationId	Unique identifier of the App - similar to AppKey, but this key is a natural.	b66bc706-ffff-7437-0340-032819502773
revision	The version as mentioned by admin during uploading of the binary.	2
title	Title of the app.	Excel
publisher	Publisher of the app.	Microsoft
uploadState	Upload state of the app.	1
appTypeKey	Reference to AppType described in the following section.	
vppProgramTypeKey	Reference to VppProgramType described below.	
creationTime	The time when this revision was created.	11/23/2016 12:00:00 AM
modifiedTime	Last time anything related to this revision was changed.	11/23/2016 12:00:00 AM
size	Size of the binary.	

Property	Description	Example
startDateInclusiveUTC	Date and time in UTC when this App revision was created in the data warehouse.	11/23/2016 12:00:00 AM
endDateExclusiveUTC	Date and time in UTC when this app revision became obsolete.	11/23/2016 12:00:00 AM
isCurrent	Indicates whether this App version is current or not in the data warehouse.	True/False
rowLastModifiedDateTimeUTC	Date and time in UTC when this app version was last modified in the data warehouse.	11/23/2016 12:00:00 AM

appTypes

The **appType** entity lists the installation source of an app.

Expand table

Property	Description
appTypeID	ID for the type
appTypeKey	Surrogate key for the key
appTypeName	App type

Example

Expand table

AppTypeID	Name	Description
0	Android store app	An Android store app.
1	Android LOB app	An Android line-of-business app.
2	Managed Android store app (MAM)	An Android store app that has management enabled.
3	iOS store app	An iOS store app.
4	iOS LOB app	An iOS line-of-business app.

AppTypeID	Name	Description
5	Managed iOS store app (MAM?)	An iOSstore app that is management enabled.
6	Microsoft 365 Apps for enterprise	The Microsoft 365 Apps for Windows 10.
7	Web app	A web app.
8	Windows Phone 8.1 store app	A Windows phone 8.1 store app.
9	Windows store app	A Windows store app.
10	Windows LOB apps	A Windows AppX line-of-business app.
11	Windows Mobile MSI	An MSI line-of-business app.
12	Windows Phone LOB app	A Windows phone line-of-business app.

vppProgramTypes

The **vppProgramType** entity lists possible VPP program types for an app.

⛶ Expand table

Property	Description
vppProgramTypeID	ID for the type.
vppProgramTypeKey	Surrogate key for the key.
vppProgramTypeName	VPP Program type.

Example

⛶ Expand table

VppProgramID	Name	Description
3DDA2474-470B-4503-9830-2665C21C1945	Microsoft	Microsoft's VPP program.
00000000-0000-0000-0000-000000000000	Not Yet Available	Default value, No VPP.
B54814E0-68EA-4BA4-8088-B5AAB58E737B	Apple	Apple's VPP program.

mobileAppInstallStates

The **mobileAppInstallState** entity represents the install state for a mobile application after it has been assigned to a group containing devices, users or both.

⛶ Expand table

Property	Description
appInstallStateKey	The unique ID of the app install state for your account.
appInstallState	Enum value of the app install state.
appInstallStateName	Name of the app install state.

Feedback

Was this page helpful? 👍 Yes 👎 No

Reference for dates entity

Article • 03/03/2025

The **dates** category contains the **date** entity used to define date references in the data model.

dates

The **date** entity represents dates that are referenced across multiple data warehouse entities.

Expand table

Property	Description	Example
dateKey	Unique identifier for this date in the data warehouse.	20160703
fullDate	This date represented in full Date/Time format.	7/3/2016 12:00:00 AM
dayOfWeek	Day of week	1
dayOfMonth	Day of month	3
dayOfYear	Day of year	185
weekOfYear	Week of year	28
monthOfYear	Month of the year	7
calendarQuarter	Calendar quarter	3
calendarYear	Calendar year	2016
dateKey	Unique identifier for this date in the data warehouse.	20160703
fullDate	This date represented in full Date/Time format.	7/3/2016 12:00:00 AM
dayOfWeek	Day of week	1
dayOfMonth	Day of month	3
dayOfYear	Day of year	185
weekOfYear	Week of year	28
monthOfYear	Month of the year	7
calendarQuarter	Calendar quarter	3

Property	Description	Example
calendarYear	Calendar year	2016

Next steps

- Learn more about the Intune Data Warehouse.

Feedback

Was this page helpful? 👍 Yes 👎 No

Reference for devices entities

Article • 03/03/2025

The **devices** category contains entities for mobile devices that track information such as:

- Device type
- Device enrollment and registration status
- Device ownership
- Device management state
- Device membership to Microsoft Entra status
- Enrollment status
- Historic information about the device
- Inventory of apps on the device

deviceTypes

The **deviceTypes** entity represents the device type referenced by other data warehouse entities. The device type typically describes either the device model, manufacturer, or a combination of both.

⛶ Expand table

Property	Description
deviceTypeID	Unique identifier of the device type
deviceTypeKey	Unique identifier of the device type in the data warehouse - surrogate key
deviceTypeName	Device type

Example

⛶ Expand table

deviceTypeID	Name	Description
0	Desktop	Windows Desktop device
1	WindowsRT	WindowsRT device
2	WinMO6	Windows Mobile 6.0 device
3	Nokia	Nokia device

deviceTypeID	Name	Description
4	WindowsPhone	Windows Phone device
5	Mac	Mac device
6	WinCE	Windows CE device
7	WinEmbedded	Windows Embedded device
8	IPhone	iPhone device
9	IPad	iPad device
10	IPod	iPod device
11	Android	Android device-managed using Device Administrator
12	ISocConsumer	iSoc Consumer device
14	MacMDM	OS X device managed with the built-in MDM agent
15	HoloLens	HoloLens device
16	SurfaceHub	Surface Hub device
17	AndroidForWork	Android device-managed using Android Profile Owner
100	Blackberry	Blackberry Device
101	Palm	Palm device
255	Unknown	Unknown device type

enrollmentActivities

The **enrollmentActivity** entity indicates the activity of a device enrollment.

Expand table

Property	Description
dateKey	Key of the date when this enrollment activity was recorded.
deviceEnrollmentTypeKey	Key of the type of the enrollment.
deviceTypeKey	Key of the type of device.
enrollmentEventStatusKey	Key of the status indicating the success or failure of the enrollment.

Property	Description
enrollmentFailureCategoryKey	Key of the enrollment failure category (if the enrollment failed).
enrollmentFailureReasonKey	Key of the enrollment failure reason (if the enrollment failed).
osVersion	The operating system version of the device.
count	Total count of enrollment activities matching the classifications above.

enrollmentEventStatuses

The **enrollmentEventStatus** entity indicates the result of a device enrollment.

Expand table

Property	Description
enrollmentEventStatusKey	Unique identifier of the enrollment status in the data warehouse (surrogate key)
enrollmentEventStatusName	The name of the enrollment status. See examples below.

Example

Expand table

enrollmentEventStatusName	Description
Success	A successful device enrollment
Failed	A failed device enrollment
Not Available	The enrollment status is unavailable.

enrollmentFailureCategories

The **EnrollmentFailureCategory** entity indicates why a device enrollment failed.

Expand table

Property	Description
enrollmentFailureCategoryKey	Unique identifier of the enrollment failure category in the data warehouse (surrogate key)
enrollmentFailureCategoryName	The name of the enrollment failure category. See examples below.

Example

Expand table

enrollmentFailureCategoryName	Description
Not Applicable	The enrollment failure category isn't applicable.
Not Available	The enrollment failure category isn't available.
Unknown	Unknown error.
Authentication	Authentication failed.
Authorization	Call was authenticated, but not authorized to enroll.
AccountValidation	Failed to validate the account for enrollment. (Account blocked, enrollment not enabled)
UserValidation	User couldn't be validated. (User doesn't exist, missing license)
DeviceNotSupported	Device isn't supported for mobile device management.
InMaintenance	Account is in maintenance.
BadRequest	Client sent a request that isn't understood/supported by the service.
FeatureNotSupported	Feature(s) used by this enrollment aren't supported for this account.
EnrollmentRestrictionsEnforced	Enrollment restrictions configured by admin blocked this enrollment.
ClientDisconnected	Client timed out or enrollment was aborted by end user.
UserAbandonment	Enrollment was abandoned by end user. (End user started onboarding but failed to complete it in timely manner)

enrollmentFailureReasons

The **EnrollmentFailureReason** entity indicates a more detailed reason for a device enrollment failure within a given failure category.

Expand table

Property	Description
enrollmentFailureReasonKey	Unique identifier of the enrollment failure reason in the data warehouse (surrogate key)
enrollmentFailureReasonName	The name of the enrollment failure reason. See examples below.

Example

Expand table

enrollmentFailureReasonName	Description
Not Applicable	The enrollment failure reason isn't applicable.
Not Available	The enrollment failure reason isn't available.
Unknown	Unknown Error.
UserNotLicensed	The user wasn't found in Intune or doesn't have a valid license.
UserUnknown	User isn't known to Intune.
BulkAlreadyEnrolledDevice	Only one user can enroll a device. This device was previously enrolled by another user.
EnrollmentOnboardingIssue	Intune mobile device management (MDM) authority isn't configured yet.
AppleChallengeIssue	The iOS management profile installation was delayed or failed.
AppleOnboardingIssue	An Apple MDM push certificate is required to enroll into Intune.
DeviceCap	The user attempted to enroll more devices than maximum allowed.
AuthenticationRequirementNotMet	Intune enrollment service failed to authorize this request.
UnsupportedDeviceType	This device doesn't meet minimum requirements for Intune enrollment.

enrollmentFailureReasonName	Description
EnrollmentCriteriaNotMet	This device failed to enroll due to a configured enrollment restriction rule.
BulkDeviceNotPreregistered	This device's international mobile equipment identifier (IMEI) or serial number wasn't found. Without this identifier, devices are recognized as personal-owned devices which are currently blocked.
FeatureNotSupported	The user was attempting to access a feature that isn't yet released for all customers or isn't compatible with your Intune configuration.
UserAbandonment	Enrollment was abandoned by end user. (End user started onboarding but failed to complete it in timely manner)
APNSCertificateExpired	Apple devices can't be managed with an expired Apple MDM push certificate.

ownerTypes

The **ownerType** entity indicates whether a device is corporate, personally owned, or unknown.

⛶ Expand table

Property	Description	Example
ownerTypeID	Unique identifier of the owner type.	
ownerTypeKey	Unique identifier of the owner type in the data warehouse - surrogate key.	
ownerTypeName	Represents the owner type of the devices: Company - device is enterprise owned. Personal - device is personally owned (BYOD). Unknown - no information on this device.	Company Personal Unknown

ⓘ Note

For the `ownerTypeName` in AzureAD when creating Dynamic Groups for devices, you need to set the filter value `deviceOwnership` as `Company`. For more information, see Rules for devices.

managementStates

The **managementStates** entity provides details on the state of the device. Detail can be useful in the cases where remote actions are applied, the device is jailbroken, or rooted.

Expand table

Property	Description
managementStateID	Unique identifier of the management state.
managementStateKey	Unique identifier of the management state in the data warehouse - surrogate key.
managementStateName	Indicates the state of the remote action applied to this device.

Example

Expand table

managementStateID	Name	Description
0	Managed	Managed with no pending remote actions.
1	RetirePending	There's a retire command pending for the device.
2	RetireFailed	The retire command failed on the device.
3	WipePending	There's a wipe command pending for the device.
4	WipeFailed	The wipe command failed on the device.
5	Unhealthy	Unhealthy state.
6	DeletePending	There's a delete command pending for the device.
7	RetireIssued	A retire command has been issued to the device.
8	WipeIssued	A wipe command has been issued.
9	WipeCanceled	Wipe command has been canceled.
10	RetireCanceled	Retire command has been canceled.
11	Discovered	The device is newly discovered by Intune, once it checks in for the first time it moves to -Managed- state.

managementAgentTypes

The **ManagementAgentType** entity represents the agents used to manage a device.

⛶ Expand table

Property	Description
managementAgentTypeID	Unique identifier of the management agent type.
managementAgentTypeKey	Unique identifier of the management agent type in the data warehouse - surrogate key.
managementAgentTypeName	Indicates what kind of agent is used to manage the device.

Example

⛶ Expand table

ManagementAgentTypeID	Name	Description
1	EAS	The device is managed through Exchange Active Sync.
2	MDM	The device is managed using an MDM agent.
3	EasMdm	The device is managed by both Exchange Active Sync and an MDM agent.
4	IntuneClient	The device is managed by the Intune PC agent.
5	EasIntuneClient	The device is managed by both Exchange Active Sync and the Intune PC agent.
8	ConfigManagerClient	The device is managed by the Configuration Manager agent.
16	Unknown	Unknown management agent type.
2048	IntuneAosp	The device is managed by Intune's MDM for AOSP (Android Open Source Project) devices.

devices

The **devices** entity lists all enrolled devices under management and their corresponding properties.

⛶ Expand table

Property	Description
deviceKey	Unique identifier of the device in the data warehouse - surrogate key.
deviceId	Unique identifier of the device.
deviceName	Name of the device on platforms that allow naming a device. On other platforms, Intune creates a name from other properties. This attribute can't be available for all devices.
deviceTypeKey	Key of the device type attribute for this device.
deviceRegistrationState	Key of the client registration state attribute for this device.
ownerTypeKey	Key of the owner type attribute for this device: corporate, personal, or unknown.
enrolledDateTime	Date and time that this device was enrolled.
lastSyncDateTime	Last known device check-in with Intune.
managementAgentKey	Key of the management agent associated with this device.
managementStateKey	Key of the management state associated with this device, indicating latest state of a remote action or if it was jailbroken/rooted.
azureADDeviceId	The Azure deviceID for this device.
azureADRegistered	Whether the device is Microsoft Entra registered.
deviceCategoryKey	Key of the category associated with this device.
deviceEnrollmentType	Key of the enrollment type associated with this device, indicating method of enrollment.
complianceStateKey	Key of the Compliance state associated with this device.
osVersion	Operating system version of the device.
easDeviceId	Exchange ActiveSync ID of the device.
serialNumber	SerialNumber
userId	Unique Identifier for the user associated with the device.

Property	Description
rowLastModifiedDateTimeUTC	Date and time in UTC when this device was last modified in the data warehouse.
manufacturer	Manufacturer of the device
model	Model of the device
operatingSystem	Operating system of the device. Windows, iOS/iPadOS, etc.
isDeleted	Binary to show whether the device is deleted or not.
androidSecurityPatchLevel	Android security patch level
MEID	MEID
isSupervised	Device supervised status
freeStorageSpaceInBytes	Free Storage in Bytes.
totalStorageSpaceInBytes	Total Storage in Bytes.
encryptionState	Encryption state on the device.
subscriberCarrier	Subscriber carrier of the device
phoneNumber	Phone number of the device
IMEI	IMEI
cellularTechnology	Cellular technology of the device
WiFiMacAddress	Wi-Fi MAC
ICCD	Integrated Circuit Card Identifier
windowsOsEdition	Windows Operating System edition.
ethernetMacAddress	The unique network identifier of this device.
model	The device model.
office365Version	The version of Microsoft 365 that is installed on the device. `Office365Version` is only collected when the Intune management extension agent is installed on a Windows machine. The admin must also create and assign a PowerShell or Win32 App for the agent to be installed. For more information, see Use PowerShell scripts on Windows 10 devices in Intune and Win32 app management in Microsoft Intune. NOTE: There's a known issue with the Intune Data Warehouse **devices**

Property	Description
	table. The `office365Version` property for the device record may be null. This property is currently under maintenance and may be subject to deprecation. Therefore, you should consider not using this property value for reporting purposes.
SubnetAddressV4Wifi	The subnet address for IPV4 Wifi connection.
IpAddressV4Wifi	The IP address for IPV4 Wifi connection.

ⓘ Note

For more information about Windows SKU enum values, see Device properties.

devicePropertyHistories

The **devicePropertyHistory** entity has the same properties as the devices table and daily snapshots of each device record per day for the past 60 days. The DateKey column indicates the day for each row.

Expand table

Property	Description
dateKey	Reference to date table indicating the day.
deviceKey	Unique identifier of the device in the data warehouse - surrogate key. This is a reference to the Device table that contains the Intune device ID.
deviceName	Name of the device on platforms that allow naming a device. On other platforms, Intune creates a name from other properties. This attribute can't be available for all devices.
deviceRegistrationStateKey	Key of the device registration state attribute for this device.
ownerTypeKey	Key of the owner type attribute for this device: corporate, personal, or unknown.
managementStateKey	Key of the management state associated with this device, indicating latest state of a remote action or if it was jailbroken/rooted.
azureADRegistered	Whether the device is Microsoft Entra registered.
complianceStateKey	A key to ComplianceState.

Property	Description
OSVersion	OS version.
jailBroken	Whether the device is jail broken or rooted.
deviceCategoryKey	Key of device category attribute for this device.
physicalMemoryInBytes	The physical memory in bytes.
totalStorageSpaceInBytes	Total storage capacity in bytes.

Feedback

Was this page helpful? 👍 Yes 👎 No

Reference for Intune Management Extensions

Article • 03/03/2025

The **intuneManagementExtensions** category contains entities for mobile devices that track information such as:

- Versions of an IntuneManagementExtension
- Installation status of an IntuneManagementExtension

intuneManagementExtensionVersions

The **intuneManagementExtensionVersion** entity lists all the versions used by intuneManagementExtensions.

Expand table

Property	Description	Example
extensionVersionKey	Unique identifier of the intuneManagementExtensions version.	1
extensionVersion	The 4 digit version number.	1.0.2.0

intuneManagementExtensionHealthStates

The **intuneManagementExtensionHealthState** lists all possible health states of the intuneManagementExtensions.

Expand table

Property	Description	Example
extensionStateKey	Unique identifier of health state.	2
extensionState	Health state of a IntuneManagementExtension.	Healthy

intuneManagementExtensions

The **intuneManagementExtension** lists the IntuneManagementExtensions health on each Windows 10 device per day. The data is retained for the last 60 days.

Expand table

Property	Description	Example
dateKey	Unique identifier of the Date.	123
tenantKey	Unique identifier of the Tenant.	456
deviceKey	Unique identifier of the Device.	789
extensionVersionKey	Unique identifier of the intuneManagementExtension version.	1
extensionStateKey	Unique identifier of health state.	2

Feedback

Was this page helpful? Yes No

Reference for mobile app management (MAM) entities

Article • 03/03/2025

The **Mobile App Management** category contains entities for mobile apps such as:

- Apps
- Instances
- Check-in status
- Health status
- Policy status
- Enrollment status
- Platform types

mamApplications

The **mamApplication** entity lists Line-of-Business (LOB) apps that are managed through Mobile Application Management (MAM) without enrollment in your enterprise.

Expand table

Property	Description	Example
mamApplicationKey	Unique identifier of the MAM application.	432
mamApplicationName	Name of the MAM application.	MAM Application Example Name
mamApplicationId	Application ID of the MAM application.	123
isDeleted	Indicates whether this MAM app record has been updated. True- MAM app has a new record with updated fields in this table. False- the latest record for this MAM app.	True/False
startDateInclusiveUTC	Date and time in UTC when this MAM app was created in the data warehouse.	11/23/2016 12:00:00 AM
deletedDateUTC	Date and time in UTC when IsDeleted changed to True.	11/23/2016 12:00:00 AM
rowLastModifiedDateTimeUTC	Date and time in UTC when this MAM app was last modified in the data	11/23/2016 12:00:00 AM

Property	Description	Example
	warehouse.	

mamApplicationInstances

The **mamApplicationInstance** entity lists managed Mobile Application Management (MAM) apps as singular instances per user per device. All users and devices listed with in the entity are protected, as in, they have at least one MAM Policy assigned to them.

Expand table

Property	Description	Example
applicationInstanceKey	Unique identifier of the MAM app instance in the data warehouse - surrogate key.	123
userId	User ID of the user who has this MAM app installed.	b66bc706-ffff-7437-0340-032819502773
applicationInstanceId	Unique identifier of the MAM app instance - similar to ApplicationInstanceKey, but the identifier is a natural key.	b66bc706-ffff-7437-0340-032819502773
mamApplicationId	Application ID of the Mam Application for which this Mam Application Instance was created.	11/23/2016 12:00:00 AM
applicationVersion	Application version of this MAM app.	2
createdDate	Date when this record of the MAM app instance was created. Value can be null.	11/23/2016 12:00:00 AM
platform	Platform of the device on which this MAM app is installed.	2
platformVersion	Platform version of the device on which this MAM app is installed.	2.2
sdkVersion	The MAM SDK version that this MAM app was wrapped with.	3.2
mamDeviceId	Device ID of the device with which MAM Application Instance is associated with.	11/23/2016 12:00:00 AM
mamDeviceType	Device type of the device with which MAM Application Instance is associated with.	11/23/2016 12:00:00 AM

Property	Description	Example
mamDeviceName	Device name of the device with which MAM Application Instance is associated with.	11/23/2016 12:00:00 AM
isDeleted	Indicates whether this MAM app instance record has been updated. True- this MAM app instance has a new record with updated fields in this table. False - the latest record for this MAM app instance.	True/False
startDateInclusiveUtc	Date and time in UTC when this MAM app instance was created in the data warehouse.	11/23/2016 12:00:00 AM
deletedDateUtc	Date and time in UTC when IsDeleted changed to True.	11/23/2016 12:00:00 AM
rowLastModifiedDateTimeUtc	Date and time in UTC when this MAM app instance was last modified in the data warehouse.	11/23/2016 12:00:00 AM

mamCheckins

The **mamCheckin** entity represents data gathered when a Mobile Application Management (MAM) app instance has checked in with the Intune Service.

> ⓘ Note
>
> When an app instance checks in multiple times a day, the data warehouse stores it as single check-in.

Expand table

Property	Description	Example
dateKey	Date Key when the MAM app check-in was recorded in the data warehouse.	20160703
applicationInstanceKey	Key of the app instance associated with this MAM app check-in.	123
userKey	Key of the user associated with this MAM app check-in.	4323

Property	Description	Example
mamApplicationKey	Application Key of Application associated with MAM Application check in.	432
deviceHealthKey	Key of DeviceHealth associated with this MAM app check-in.	321
platformKey	Represents the platform of the device associated with this MAM app check-in.	123
effectiveAppliedPolicyKey	Represents the effective applied policy associated with the MAM app that has checked in. An effective applied policy results from merging all policies relevant to a particular app and user.	322
pastCheckInDate	Date and time when this MAM app last checked in. Value can be null.	11/23/2016 12:00:00 AM

mamDeviceHealth

The **mamDeviceHealth** entity represents devices that have Mobile Application Management (MAM) policies deployed to them even if they are jailbroken.

Expand table

Property	Description	Example
deviceHealthKey	Unique identifier of the device and its associated health in the data warehouse - surrogate key.	123
deviceHealth	Unique identifier of the device and its associated health - similar to DeviceHealthKey, but the identifier is a natural key.	b66bc706-ffff-7777-0340-032819502773
deviceHealthName	Represents the status of the device. Not available - no information on this device. Healthy - device is not jailbroken. Unhealthy - device is jailbroken.	Not Available Healthy Unhealthy
rowLastModifiedDateTimeUtc	Date and time in UTC when this specific MAM Device Health was last modified in the data warehouse.	11/23/2016 12:00:00 AM

mamEffectivePolicies

The **mamEffectivePolicy** entity lists all Mobile Application Management (MAM) effective policies applied in your organization. An effective applied policy results from merging all policies relevant to a particular app and user.

Expand table

Property	Description	Example
effectivePolicyKey	Unique identifier of the MAM effective policy in the data warehouse.	2
realPolicyKey	Unique identifier of the MAM policy authored by the IT Pro.	1
rowCreatedDateTimeUtc	Date and time in UTC when this MAM effective policy was created in the data warehouse.	11/23/2016 12:00:00 AM

mamPlatforms

The **mamPlatform** entity lists platform names and types on which a Mobile Application Management (MAM) app was installed.

Expand table

Property	Description	Example
platformKey	Unique identifier of the platform in the data warehouse - surrogate key.	123
platform	Unique identifier of the platform - similar to PlatformKey, but is a natural key.	123
platformName	Platform name	Not Available None Windows IOS Android.
rowLastModifiedDateTimeUtc	Date and time in UTC when this platform was last modified in the data warehouse.	11/23/2016 12:00:00 AM

Feedback

Was this page helpful? 👍 Yes 👎 No

Reference for Policy entities

Article • 03/03/2025

The **policies** category contains entities for mobile devices that track information such as:

- Inventory of device configuration profiles, app configuration profiles, and compliance policies
- Number of devices in the succeeded, pending, failed, or error state per day
- Number of users in the succeeded, pending, failed, or error state per day
- Cumulative number of devices in the succeeded, pending, failed, or error state

policies

The **policy** entity lists device configuration profiles, app configuration profiles, and compliance policies. You can assign the policies with Mobile Device Management (MDM) to a group in your enterprise.

⛶ Expand table

Property	Description	Example
policyKey	Unique Key to represent the policy in the data warehouse.	123
policyId	Unique identifier of the Policy in the data warehouse.	b66bc706-ffff-7437-0340-032819502773
policyName	Name of the Policy.	"Windows 10 Baseline"
policyVersion	Version of the Policy. When the policy is edited or changed, a newer version is created.	1, 2, 3
isDeleted	Indicates whether the Policy record has been updated. True- policy has a new record with updated fields. False- the latest record for the policy.	True/False
startDateInclusiveUTC	Date and time in UTC when the policy was created in the data warehouse.	11/23/2016 12:00:00 AM
deletedDateUTC	Date and time in UTC when IsDeleted changed to True.	11/23/2016 12:00:00 AM

Property	Description	Example
rowLastModifiedDateTimeUTC	Date and time in UTC when the policy was last modified in the data warehouse.	11/23/2016 12:00:00 AM

policyTypes

The **policyType** entity lists types of device configuration profiles, app configuration profiles, and Compliance policies. You can assign the policies with Mobile Device Management (MDM) to a group in your enterprise.

⛶ Expand table

Property	Description	Example
policyTypeId	Unique identifier of the policy in the source system.	123
policyTypeKey	Unique identifier of the policy in the data warehouse.	1
policyTypeName	Name of the policy type.	Windows 10 Compliance policy.

Device Configuration

The **deviceConfigurationProfileDeviceActivity** entity lists the number of **devices** in the succeeded, pending, failed, or error state per day. The number reflects the Device configuration profiles assigned to the entity. For example, if a **device** is in the succeeded state for all its assigned policies, it increments the succeeded counter up one for that day. If a device has two profiles assigned to it, one in the succeeded state and another in an error state, the entity increments the Succeeded counter and place the device in the error state. The entity lists how many devices are in which state on a given day over the last 30 days.

⛶ Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703

Property	Description	Example
pending	Number of unique Devices in pending state.	123
succeeded	Number of unique Devices in success state.	12
error	Number of unique Devices in error state.	10
failed	Number of unique Devices in failed state.	2

The **deviceConfigurationProfileUserActivity** entity lists the number of **users** in the succeeded, pending, failed, or error state per day. The number reflects the Device configuration profiles assigned to the entity. For example, if a **user** is in the succeeded state for all their assigned policies, it moves up the succeeded counter by one for that day. If a user has two profiles assigned to them, one in the succeeded state and the other is in an error state, the user in the error state is counted. The **deviceConfigurationProfileUserActivity** entity lists how many users are in which state on a given day over the last 30 days.

Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703
pending	Number of unique Users in pending state.	123
succeeded	Number of unique Users in success state.	12
error	Number of unique Users in error state.	10
failed	Number of unique Users in failed state.	2

policyTypeActivities

The **policyTypeActivity** entity lists the cumulative number of devices in the succeeded, pending, failed, or error state. It lists these states with respect to a device configuration profile, app configuration profile, or compliance policy per day.

Expand table

Property	Description	Example
dateKey	dateKey when the device Configuration profile check-in was recorded in the data warehouse.	20160703

Property	Description	Example
policyKey	policyKey, can be joined with policy to get the policyName.	Windows 10 baseline
policyTypeKey	Type of Policy Key, can be joined with Policy Type to get the policy type name.	Windows10 Compliance Policy
pending	Number of unique devices in pending state.	123
succeeded	Number of unique devices in success state.	12
error	Number of unique devices in error state.	10
failed	Number of unique devices in failed state.	2

Compliance Policy

The Compliance Policy API Reference contains entities that provide status information about compliance policies assigned to devices.

compliancePolicyStatusDeviceActivities

The following table summarizes the assignment status of compliance policies to devices. It lists the count of devices found in each compliance state.

⛶ Expand table

Property	Description	Example
dateKey	Date key when the summary was created for the compliance policy.	20161204
unknown	Number of devices that are offline or failed to communicate with Intune or Microsoft Entra ID for other reasons.	5
notApplicable	Number of devices where device compliance policies targeted by the admin are not applicable.	201
compliant	Number of devices that successfully applied one or more device compliance policies targeted by the admin.	4083
inGracePeriod	Number of devices that are not compliant but that are in the grace-period defined by the admin.	57
nonCompliant	Number of devices that failed to apply one or more device compliance policies targeted by the admin or where the user hasn't complied with the policies targeted by the admin.	43

Property	Description	Example
error	Number of devices that failed to communicate with Intune or Microsoft Entra ID, and returned an error message.	3

compliancePolicyStatusDevicePerPolicyActivities

The following table summarizes the assignment status of compliance policies to devices on a per policy and a per policy type basis. It lists the count of devices found in each compliance state for each assigned compliance policy.

Expand table

Property	Description	Example
dateKey	Date key when the summary was created for the compliance policy.	20161219
policyKey	Key for the compliance policy for which the summary was created.	10178
policyPlatformKey	Key for the platform type of the compliance policy for which the summary was created.	5
unknown	Number of devices that are offline or failed to communicate with Intune or Microsoft Entra ID for other reasons.	13
notApplicable	Number of devices where device compliance policies targeted by the admin are not applicable.	3
compliant	Number of devices that successfully applied one or more device compliance policies targeted by the admin.	45
inGracePeriod	Number of devices that are not compliant but that are in the grace-period defined by the admin.	3
nonCompliant	Number of devices that failed to apply one or more device compliance policies targeted by the admin or where the user hasn't complied with the policies targeted by the admin.	7
error	Number of devices that failed to communicate with Intune or Microsoft Entra ID, and returned an error message.	3

policyPlatformTypes

The following table contains the platform types of all assigned policies. Policies platform types that have never been assigned to any devices are not present in this table.

Expand table

Property	Description	Example
policyPlatformTypeKey	The unique key for the policy platform type.	20170519
policyPlatformTypeId	The unique identifier for the policy platform type.	1
policyPlatformTypeName	The name for the policy platform type.	AndroidForWork

policyDeviceActivities

The following table lists the number of devices in the succeeded, pending, failed, or error state per day. The number reflects the data per Policy Type profiles. For example, if a device is in the succeeded state for all its assigned policies, it increments the succeeded counter up one for that day. If a device has two profiles assigned to it, one in the succeeded state and another in an error state, the entity increments the Succeeded counter and place the device in the error state. The policyDeviceActivity entity lists how many devices are in which state on a given day over the last 30 days.

Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703
pending	Number of unique Devices in pending state.	123
Succeeded	Number of unique Devices in success state.	12
policyKey	policyKey, can be joined with policy to get the policyName.	Windows 10 baseline
error	Number of unique Devices in error state.	10
failed	Number of unique Devices in failed state.	2

policyUserActivities

The following table lists the number of users in the succeeded, pending, failed, or error state per day. The number reflects the data per Policy Type profiles. For example, if a user is in the succeeded state for all their assigned policies, it moves up the succeeded counter by one for that day. If a user has two profiles assigned to them, one in the succeeded state and the other is in an error state, the user in the error state is counted.

The PolicyUserActivity entity lists how many users are in which state on a given day over the last 30 days.

Expand table

Property	Description	Example
dateKey	Date Key when the Device Configuration Profile check-in was recorded in the data warehouse.	20160703
pending	Number of unique Devices in pending state.	123
succeeded	Number of unique Devices in success state.	12
policyKey	policyKey, can be joined with policy to get the policyName.	Windows 10 baseline
error	Number of unique Devices in error state.	10

Feedback

Was this page helpful? Yes No

Reference for User Device Association entity

Article • 03/03/2025

The **userDeviceAssociation** entity contains user device associations in your organization.

userDeviceAssociations

Expand table

Name	Description	Example
userKey	Unique identifier of the user in the data warehouse. (Surrogate key).	123
deviceKey	Unique identifier of the device in the data warehouse.	123
createdDateTimeUTC	Date and time when the user device association was created. Uses UTC format.	11/23/2016 12:00:00 AM
isDeleted	Indicates that the user unenrolled that device, and that the association is not current anymore.	True/False
endedDateTimeUTC	Date and time in UTC when IsDeleted changed to **True**.	06/23/2017 12:00:00 AM

Next steps

- Learn more about the Intune Data Warehouse.

Feedback

Was this page helpful? Yes No

Reference for User entity

Article • 03/03/2025

The **Users** category contains the **user** entity that defines user properties in the data model.

users

The **user** entity lists all the Microsoft Entra users with assigned licenses in your enterprise.

The **user** entity collection contains user data. These records include user states during the data collection period, even if the user has been removed. For example, a user may be added to Intune and then removed during the course of the last month. While this user is not present at the time of the report, the user and state are present in the data from the prior month. You could create a report that would show the duration of the user's historic presence in your data.

Expand table

Property	Description	Example
userKey	Unique identifier of the user in the data warehouse - surrogate key.	123
userId	Unique identifier of the user - similar to UserKey, but is a natural key.	b66bc706-ffff-7437-0340-032819502773
userEmail	Email address of the user.	John@contoso.com
userPrincipalName	User principal name of the user.	John@contoso.com
displayName	Display name of the user.	John
intuneLicensed	Specifies if this user is Intune licensed or not.	True/False
isDeleted	Indicates whether all of the user's licenses have expired and whether the user was therefore removed from Intune. For a single record, this flag does not change. Instead, a new record is created for a new user state.	True/False
RowLastModifiedDateTimeUTC	Date and time in UTC when the record was last modified in the data	11/23/2016 0:00

Property	Description	Example
	warehouse	

Next steps

- You can use the **Current User** entity collection to limit the user data to users who are currently active. For more information, see Reference for current user entity.
- To learn more about how the data warehouse tracks a user's lifetime in Intune, see User lifetime representation in the Intune Data Warehouse.

Feedback

Was this page helpful? 👍 Yes 👎 No

Move your Intune Data Warehouse account data

Article • 03/03/2025

By requesting an account move, you're requesting that your data center is changed to another location. After the move, your Data Warehouse will reset and begin recording data at the new location based on the specified day your move begins. To back up your previous Data Warehouse data, complete the following steps **prior** to your account move. Most Data Warehouse tables retain data for 30 days, so any data gap in these tables will no longer be available 30 days after your account move. To learn more about the retention periods for specific tables, see Data Warehouse data model.

Back up your Data Warehouse data

To back up your Data Warehouse data, you must save your Data Warehouse data into a *.csv* file using the Data Warehouse API:

1. If you're a first-time user of the Data Warehouse API, follow the one-time process provided in the following article, Get data from the Intune Data Warehouse API with a REST client.
2. Use the PowerShell sample titled Access the Intune Data Warehouse with PowerShell to download all your data into CSV files.

Back up your trend charts from the Microsoft Intune admin center

Some trend charts in your view of the Microsoft Intune admin center resets. You may back up these charts by running the following script in **Graph**:

Terms & Conditions Acceptance reports

1. In theMicrosoft Intune admin center, select **Tenant administration** > **Terms & Conditions**.
2. For each **Terms & Condition** item that you select, select **Acceptance Report** > **Export**.
3. Save the report locally.

App Protection reports

1. In the Microsoft Intune admin center ↗, select **Apps** -> **Monitor** -> **App protection status**.
2. Select the download icon (⤓) to save each report.

Device Configuration charts

1. In the Microsoft Intune admin center ↗, select **Devices** > **Manage devices** > **Configuration** > **Export**.

2. Using Microsoft Graph Explorer, download the data behind the charts.

   - For deployment status of all device configuration profiles for all devices, see Device deployment status ↗.

   - For deployment status of all device configuration profiles for all users, see User deployment status ↗.

   - For profile deployment status, see Provide deployment status ↗.

   > ⓘ **Note**
   >
   > You must have a valid authenticaltion token to access the device configuration and deployment status information.

Device Enrollment charts

1. In the Microsoft Intune admin center ↗, select **Devices** > **Monitor** > **Assignment status** > **Export**.

2. Using Microsoft Graph Explorer, download the data behind the charts.

   - For enrollment status, copy this enrollment status query ↗ and paste it into Graph Explorer.
   - For top enrollment failures this week, copy this enrollment failures query ↗ and paste it into Graph Explorer.

   > ⓘ **Note**
   >
   > You must have a valid authenticaltion token to access the device enrollment data.

After a Data Warehouse account move

After the Data Warehouse account move, you'll see in Intune that the Data Warehouse was reset, and your data is now stored in the new location. The charts and export options reset, and you see a notification, which upon clicking will direct you to an article explaining why the charts have reset.

Data Warehouse move example

Customer X requests an account move to begin on 1/06/2018. In response to the request, the customer receives a link to see documentation detailing steps to take if they wish to back up their previous Data Warehouse. On 1/06/2018, the Data Warehouse and the charts it supports will reset and begin storing data in the new data center.

Next steps

- Learn what's new each week in Intune. You can also find out about upcoming changes, important notices about the service, and information about past releases.
- Read the Microsoft Intune Blog ↗.

Feedback

Was this page helpful? Yes No

Privacy and personal data in Intune

Article • 04/10/2025

Microsoft Intune operates as a data processor on behalf of the customer as necessary to provide customers with the requested service as set forth in the Microsoft Online Services Terms (OST). Personal data is provided directly through Customer Administrator use of Intune through the Azure portal or Microsoft Intune admin center, or from customer devices when enrolled for management. Personal data is also collected at third-party services per the customer’s instructions such as setting up Apple Volume Purchasing Program. Customers can receive, transmit, and store data on devices managed by Intune. Personal data is processed and stored within the audited compliance boundary of the Intune service under the technical security measures assured through Microsoft Online Services Terms (OST).

To help Intune admins understand how your data's privacy is protected, this article explains how Intune collects, stores, retains, processes, secures, shares, audits, and exports personal data. It also covers how to review, correct, and delete your personal data.

Microsoft Intune doesn't use any personal data collected as part of providing the service for profiling, advertising, or marketing purposes.

> ⓘ Note
>
> If you're interested in viewing or deleting personal data, please see the Azure Data Subject Requests for the GDPR article. If you're looking for general info about GDPR, see the GDPR section of the Service Trust portal.

Your company terms and conditions

In addition to the Microsoft Privacy Statement, you can include privacy statements in your company's terms and conditions for end users. Such privacy statements can include information about the usage and privacy of the end user's personal data.

You can display your company's terms and conditions in the Intune Company Portal app. This way, users can review the terms and conditions, including the privacy statement, before they enroll in Intune and access company assets and data.

Next steps

Find out more about how Intune collects, stores and processes, and shares personal data.

Compliance in Microsoft Intune

Article • 03/03/2025

Intune supports compliance features to help organizations meet national, regional, and industry-specific regulations. Intune aligns with Microsoft's commitment to data protection, privacy, and compliance by offering tools to help secure and manage data effectively.

Shared responsibility model

Microsoft ensures that Intune complies with various industry standards and regulatory frameworks. However, customers are responsible for implementing their data protection and compliance strategies to align with their specific organizational requirements.

Compliance certifications

Intune is covered under several compliance certifications, and regulatory standards. The following table provides a sample of the key certifications that are covered:

Expand table

Certification or Standard	Description	Applicability
GDPR	EU General Data Protection Regulation for data privacy	European Union
ISO 27001	International standard for information security management	Global
HIPAA	U.S. Health Insurance Portability and Accountability Act	United States
SOC 2 Type 2	Service Organization Controls for data security	Global

ⓘ Note

Microsoft Intune helps your organization meet regulatory compliance standards. Intune supports additional certifications, such as ISO 22301, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 1 Type 2, SOC 3, and WCAG.

For a complete list, see Microsoft compliance offerings.

Compliance dependencies

Intune leverages other Microsoft services for compliance, including:

- Microsoft Purview: A suite of data governance and compliance tools.
- Microsoft Entra ID: Identity and access management, formerly known as Azure Active Directory (Azure AD).
- Microsoft Purview Compliance Manager: Tools for managing compliance across your organization.
- Microsoft Defender for Endpoint: An enterprise endpoint security platform.

Microsoft Intune capabilities for compliance

Microsoft Intune helps enforce compliance policies and protect organizational data specifically for Intune:

- **Conditional Access**: Ensures only compliant devices and apps managed by Intune can access sensitive data. See Conditional Access.
- **Device Compliance Enforcement**: Enforces device compliance policies to meet organizational security requirements. See Device Compliance Policies.

For more information about Intune compliance capabilities, visit the Microsoft Intune documentation.

Data residency and protection

Intune supports compliance with data residency requirements by supporting Microsoft Cloud's regional and global data storage policies. These policies include:

- **Data location**: Data is stored in Microsoft-managed data centers. For more information, see Data storage and processing in Intune.
- **EU Data Boundary**: Ensures that data belonging to EU customers is stored and processed within the EU. For more information, see EU Data Boundary and Configure Microsoft Tunnel for Intune.
- **Encryption**: Data is encrypted at rest and in transit. For more information, see Access requirements policy mapping from Basic Mobility and Security to Intune.

Compliance features

Intune includes several compliance features that help organizations meet regulatory requirements, manage data lifecycles, and protect sensitive information. These features are designed to ensure your organization can effectively monitor, classify, and safeguard its data while maintaining compliance with industry standards.

Data lifecycle management

> ⓘ **Important**
>
> Microsoft Intune doesn't use any personal data collected as part of providing the service for profiling, advertising, or marketing purposes.

Intune supports data lifecycle management through retention policies and labels. These features help organizations retain or delete data based on compliance requirements. For more information, see Privacy and personal data in Intune.

Auditing and reporting

Microsoft Purview (included in the **Microsoft 365 E5** license) supports auditing and reporting for Intune. IT administrators can monitor data usage and ensure adherence to organizational compliance policies. Features include:

- eDiscovery: Enables organizations to locate data for legal or regulatory needs.
- Data Retention Policies: Helps organizations manage data lifecycles.

For more information, see the Protect your sensitive data with Microsoft Purview.

Privacy controls

Intune includes privacy controls to manage data collection, storage, and sharing:

For details about privacy, see Privacy and personal data in Intune.

Related articles

- Microsoft Privacy Statement
- Microsoft Trust Center
- Microsoft Purview compliance portal

Feedback

Was this page helpful? Yes No

Optional diagnostic data from Intune Client apps

Article • 03/03/2025

Intune collects various optional data to detect, diagnose, and fix problems from users through various Intune client apps. These optional diagnostic data we collect help to proactively detect problems in your organization so they can be addressed before they become an issue. Intune client apps include:

- iOS/iPadOS Company Portal
- macOS Company Portal
- Windows Company Portal
- Android Company Portal
- Android Intune app
- Microsoft Intune Management Agent for macOS
- Microsoft Intune Management Extension
- Android Mobile App Management (MAM)

The optional data collected from clients aren't required to successful run Intune services. The data collected helps:

- Provides enhanced information to help us proactively detect, diagnose, and fix issues.
- Makes product and service improvements.

Data collected

Optional diagnostic data collected by Intune client apps may cover the following areas:

- Microsoft-generated user information
  - Microsoft Entra user ID
  - Device ID
  - Correlation ID
  - App Session ID
  - User Session ID
- Admin and account information
  - Tenant ID
  - Microsoft Entra tenant ID
- Hardware and software information
  - Device OS version

  - Device model
  - Device make
  - Application ID
  - User language
  - User time zone
- Service events and error information
  - Enrollment event
  - Failure event
    - Network failure
    - Runtime failure
    - Task schedule failure
    - Enrollment failure
    - Microsoft Entra authentication failure
  - Crash report
  - Consent state
  - Compliance status
  - Policy status
- Company Portal events
  - Company Portal error
  - Company Portal page action
  - Company Portal page view
  - Company Portal version
- Performance measurement
  - Duration
  - Response time

Data not collected

The data do not include any customer information, like:

- Device name
- Phone number
- Contents to the user's files or photo.

Turn off data collection

We think there are compelling reasons for people to share this optional data. All optional diagnostic data Microsoft collects during the use of any Microsoft 365 Apps for enterprise applications and services is pseudonymized as defined in the ISO/IEC 19944-1:2020 (section 8.3.3) standard.

Users can turn off usage data collection for their individual devices.

Next steps

Find out more about data collection in Intune.

Feedback

Was this page helpful? 👍 Yes 👎 No

Data collection in Intune

Article • 04/07/2025

When users enroll their corporate or personal devices with Intune, Intune collects, processes, and shares some personal data to support business operations, and customer service. Intune collects personal data from the following sources:

- The administrators use of the Intune in the Microsoft Intune admin center.
- End-user devices (when devices are enrolled for Intune management and during usage).
- Customer accounts at third party services (per admin's instructions).
- Diagnostic, performance, and usage information.

From these sources, Intune collects information that falls into the following two categories: required, optional. Each category is divided into customer data, personal data, diagnostic data, and service-generated data.

ⓘ Note

We don't sell any data collected by our service to any third parties for any reason.

Required data

Data in the required category consists of data in the default feature set that is necessary to make our service work as expected by the customer. Most of the data collected by Intune is required data. This data is tied to a user, device, or application and is essential to the nature of management. The data collected contains both personal data and non-personal data. Personal data includes identifiable data that might directly identify the end user, or pseudonymized data with a unique identifier generated by the system that's used to deliver the enterprise service to users, support data, and account data. Non-personal data includes service-generated system metadata and organizational/tenant information. Intune also collects access control data to manage access to administrative roles and functions through features like Role Based Access Control.

Required data collected by Intune includes, but isn't limited to:

Expand table

Category	Data	MAM workload [1]
Access control information	Private keys for certificates	No
	Static authenticators (customer's password)	No

Category	**Data**	**MAM workload** [1]
Admin and account information	Active Directory ID of each customer IT admin	Yes
	Admin user first name and family name	Yes
	Admin user name	Yes
	Email address of account owner	Yes
	Payment data for customer billing	Yes
	Phone number	Yes
	Subscription key	Yes
	UPN (email)	Yes
Admin created data, like:	Compliance policies	No
	Group policy	No
	Line-of-Business (LOB) application	Yes
	PowerShell scripts	No
	Profile names	Yes
Admin usage data from across all Intune tenants (for example, admin controls selected when interacting with the Admin console)		Yes
Application inventory, like:	app ID	Yes (Managed apps only)
	app name	Yes (Managed apps only)
	installation location	No
	size	No
	version	Yes (Managed apps only)
	Note: Application inventory data is only collected when marked by the Admin as a corporate-owned device or the compliant app feature is turned on.	

Category	Data	MAM workload [1]
Audit log information, including data about the following activities	Assign	Yes
	Create	Yes
	Delete	Yes
	Manage	Yes
	Remote tasks	Yes
	Update (edit)	Yes
Customer third party tenant IDs (like Apple ID)		No
Device Data	Account ID	Yes
	AppleID for iOS/iPadOS devices	No
	Microsoft Entra device ID	Yes (If device is Microsoft Entra joined)
	Intune device ID	Yes (If device is MDM enrolled with Intune)
	Device storage space	No
	EAS device ID	No
	Intune device management ID	Yes (If device is MDM enrolled with Intune)
	Location (corporate devices only)	No
	Mac Address for Mac devices	No
	Network information	No
	Platform-specific IDs	No
	Tenant ID	Yes
	Windows ID for Windows devices	No
Hardware inventory information	Device name	Yes (Device Friendly Name)
	Device type	Yes

Category	Data	MAM workload [1]
	ICCID	No
	IMEI number	No
	IP address	No
	Manufacturer	Yes
	Model	Yes
	Operating system	Yes
	Operating system version	Yes
	Serial number	No
	Wi-Fi MacAddress	No
Managed application information	Microsoft Entra device ID	Yes (If device is Microsoft Entra joined)
	Device enrollment status	Yes
	Device health status	Yes (Includes threat status if a Mobile Threat Defense connector is configured)
	Encryption keys	Yes
	Intune device management ID	Yes (If device is MDM enrolled with Intune)
	Last application check-in date/time	Yes
	Managed application device tag	Yes
	Managed application ID	Yes
	Managed application SDK version	Yes
	Managed application version	Yes
	MAM enrollment data/time	Yes
	MAM enrollment status	Yes
Support information	Contact information (name, phone number, email address)	No

Category	Data	MAM workload [1]
	Email discussions with Microsoft support, product, and/or customer experience team members	No
Tenant account information (this data is available from the Microsoft Intune admin center	installedDeviceCount: The number of devices on which the application is installed.	Yes
	Number of devices or users enrolled	No
	Number of identified device platforms	No
	Number of installed devices	No
	notApplicableDeviceCount: The number of devices for which the application isn't applicable.	No
	notInstalledDeviceCount: The number of devices for which the application is applicable but not installed.	No
	pendingInstallDeviceCount: The number of devices for which the application is applicable and installation is pending.	No
User information	Owner name/user display (the Azure-registered name of the user as identified by AzureUserID)	Yes
	Phone number	No
	Third-party user identifies (like AppleID)	No
	User Principal Name or email address	Yes

[1] Intune Mobile Application Management (MAM) can be deployed independent of other Intune workloads. For customers only using Intune MAM, this column identifies which required data is collected.

Optional data

Data in the required category consists of data in the default feature set that is necessary to make our service work as expected by the customer.

Your organization might enable optional features within Intune which enable collection of additional information from devices:

- Device query for Corporate-owned Windows Devices

  When a customer enables Device query, the admin can query device details such as File Name and File Path. For a complete list of data, see Intune data platform schema.

- Enhanced device inventory

  When a customer enables enhanced device inventory, the admin can see non-sensitive device details such as CPU, disk drive, and memory info. For a complete list of data, see Intune data platform schema.

Customers can control the collection of pseudonymized diagnostics and telemetry data from Intune components installed on their devices. We think there are compelling reasons for people to share this optional data as it helps Microsoft improve the reliability and performance of its products and we understand the importance of providing users the opportunity to make these choices for themselves.

Examples of the optional data fall into the following categories as defined by the ISO/IEC 19944-1:2020 Information technology - Cloud computing - Cloud services and devices: Data flow, data categories :

- Details about the device, its configuration and connectivity capabilities, and status.
- Details about the usage of the device, operating system, applications, and services.
- Details about the health of the device, operating system, apps, and drivers.
- Software installation and update information on the device.

Certain End User Data or Content is never Collected

Intune doesn't collect nor allow an Admin to see the following data:

- An end users' calling or web browsing history
- Personal email
- Text messages
- Contacts
- Passwords to personal accounts
- Calendar events
- Photos, including those pictures in a photo app or camera

For more information, see Getting started enrolling devices.

For more information on the data types and definition, see How Microsoft categorizes data for online services .

Next steps

Learn more about how Intune stores and processes and shares personal data.

Data storage and processing in Intune

Article • 03/03/2025

Storing customer data

After Intune collects the data, Intune follows the Data Handling Standard policy for Microsoft 365 that specifies how customer data is stored and processed. See Where your Microsoft 365 customer data is stored. Personal data is processed within the audited compliance boundary of the Intune service under the technical security measures assured through Microsoft Online Services Terms (OST).

Storage locations

Microsoft offers and operates Intune services in many regions worldwide. Intune respects the storage location elections made by the administrator for Customer Data.

For more information, see Data Center Locations.

Data residency option

We open new datacenter geographies for Intune to add capacity and compute resources to support our ongoing customer demand and usage growth. Additionally, the new datacenter geographies offer in-region data residency for Customer Data.

Existing customers that have their Customer Data stored in an already existing datacenter geography aren't impacted by the launch of a new datacenter geography. We introduce no unique capabilities, features, or compliance certifications with the new datacenter geography. As a customer, you'll experience the same quality of service, performance, and security controls in any of those two geographies.

We offer existing customers an option to request migration of their organization's Customer Data at rest to the datacenter geography that matches their signup Country or region.

With this option, eligible customers with data residency requirements can request migration of their organization's Customer Data at rest to their new datacenter geography if minimal data loss and reconfiguration is acceptable. Microsoft offers a committed deadline to all eligible customers who request migration. Contact support to request your data move. Our support team guides you through the preparation steps that you need to take and limitations you should be aware of. Data moves can take up to 24 months after the request period ends to complete.

During migration, certain features might not be accessible. The actual down time and impact to end-users depends on the volume of data to be migrated and features in use. When migration is complete, the support team contacts you to make sure everything is working.

Data moves to the new datacenter geographies are completed at no extra cost to the customer.

Personal data retention

Microsoft 365 Data Handling Standard policy specifies how long customer data is retained after deletion. There are two scenarios in which customer data is deleted:

-**Active Deletion**: The tenant has an active subscription and a user or administrator deletes data, or administrators delete a user. -**Passive Deletion**: The tenant subscription ends.

For each of the deletion scenarios, see Data Retention, Deletion, and Destruction in Microsoft 365.

In general, personal data collected by Intune is removed within 30 days after deletion. Audit logs are retained for up to one year for security purposes.

Processing personal data

Intune processes personal data with ISO certified systems. For more information, see the Service Trust Portal.

Profiling and marketing

Microsoft Intune doesn't use any personal data collected as part of providing the service for profiling or marketing purposes.

Next steps

Find out more about how Intune secures and shares personal data.

Feedback

Was this page helpful? 👍 Yes 👎 No

Data security and sharing in Intune

Article • 03/03/2025

Data security

Microsoft Intune is a key component of the Microsoft Enterprise Mobility and Security Suite cloud service offering. To support the data governance strategy, all Microsoft cloud services are developed with Microsoft Privacy and Microsoft Security methodologies.

Microsoft Intune follows the same technical and organizational measures that the Microsoft Azure service teams take for securing against data breach processes.

For more information, see the Service Trust Portal.

Data breach reporting

When a Customer-Reportable Security Incident (CRSI) is identified, customers are notified. This process includes working with the Microsoft 365 team to communicate breach notification for any Microsoft 365 customers using Intune.

Data sharing

When tenant admins turn on certain functionality (like the Apple Device Enrollment Program), Microsoft Intune obtains admin consent for sharing data with the appropriate third parties. In such cases, Intune may share personal data with:

- Third parties acting as Microsoft's agents.
- Third parties not acting as Microsoft's agents, but only when tenant admins explicitly grant Intune permission to do so.

All third parties acting as Microsoft agents are included in the Online Services Subcontractor list.

Sharing data with such entities is done to aid customer and technical support, service maintenance, and other operations.

A tenant's contract with the third party governs the Intune personal data held in the third party's service. It also grants Intune the permission to transmit data to the third party service.

For information about data shared with certain third parties, see the following articles:

- Data Intune sends to Apple
- Data Intune sends to Google
- Data Apple sends to Intune
- Data Google sends to Intune
- Data Jamf Pro sends to Intune

Microsoft Configuration Manager data sharing

Microsoft Intune doesn't share any data with Configuration Manager. Configuration Manager is an on-premise product deployed, managed, and operated directly by the customer. The diagnostics and usage data that is collected by Configuration Manager are only to improve the installation experience, quality, and security of future releases.

To learn more, see Diagnostics and usage data for Configuration Manager.

Next steps

Find out how to view and correct personal data in Intune.

Feedback

Was this page helpful? 👍 Yes 👎 No

Data Apple sends to Intune

Article • 03/03/2025

When any of the following Apple services are enabled on a device, Microsoft Intune establishes a connection with Apple to share user and device information:

- Apple Device Enrollment Program (DEP)
- Apple MDM Push certificate (APNs)
- Apple School Manager (ASM)
- Apple Volume Purchase Program (VPP)

Before Microsoft Intune can establish a connection, you must create an Apple account for each of the Apple services.

ⓘ **Note**

Consistent with Microsoft and Apple policy, we do not sell any data collected by our service to any third parties for any reason.

The following table lists the data that an Apple device sends to Intune. Intune also sends data to Apple.

Expand table

Service	Message	Data sent to Intune	Used for
APNs	Authenticate	MessageType	The message type: authenticate.
APNs	Authenticate	Topic	The topic the device will listen to.
APNs	Authenticate	MesUDID	The devices UDID.
APNs	Authenticate	OSVersion	The device's OS version.
APNs	Authenticate	BuildVersion	The device's build version.
APNs	Authenticate	ProductName	The device's product name.
APNs	Authenticate	SerialNumber	The device's serial number.
APNs	Authenticate	IMEI	The device's International Mobile Station Equipment Identity.
APNs	Authenticate	MEID	The device's Mobile Equipment Identifier

Service	Message	Data sent to Intune	Used for
APNs	TokenUpdate	Topic	The topic the device will listen to.
APNs	TokenUpdate	UDID	The device's UDID.
APNs	TokenUpdate	Token	The push token for the device. The server should use this updated token when sending push notifications to the device.
APNs	TokenUpdate	PushMagic	The magic string that must be included in the push notification message.
APNs	TokenUpdate	UnlockToken	A data blob that can be used to unlock the device.
APNs	TokenUpdate	AwaitingConfiguration	If set to true, the device is awaiting a DeviceConfigured MDM command before proceeding through Setup Assistant.
APNs	Checkout	MessageType	The type of message: checkout.
APNs	Checkout	Topic	The topic the device will listen to.
APNs	Checkout	UDID	The device's UDID
APNs	MDM Protocol	Status	Status.
APNS	MDM Protocol	UDID	The device's UDID.
APNs	MDM Protocol	CommandUUID	UUID of the command that this response is for.
APNs	MDM Protocol	ErrorChain	Array of dictionaries representing the chain of errors that occurred.
ASM/DEP	Enrollment Program token	Serial number	The device's serial number.
ASM/DEP	Enrollment Program token	model	The device's model name.
ASM/DEP	Enrollment Program token	Description	A description of the device.
ASM/DEP	Enrollment Program token	Color	The color of the device.
ASM/DEP	Enrollment	Asset tag	The device's asset tag.

Service	Message	Data sent to Intune	Used for
	Program token		
ASM/DEP	Enrollment Program token	Profile status	The status of the profile installation.
ASM/DEP	Enrollment Program token	Profile UUID	The UUID of the assigned profile.
ASM/DEP	Enrollment Program token	Profile assign time	A time stamp in ISO 8601 format indicating when a profile was assigned to the device.
ASM/DEP	Enrollment Program token	Profile push time	A time stamp in ISO 8601 format indicating when a profile was pushed to the device.
ASM/DEP	Enrollment Program token	Device assigned date	A time stamp in ISO 8601 format indicating when the device was enrolled in the Device Enrollment Program.
ASM/DEP	Enrollment Program token	Device assigned by	The email of the person who assigned the device.
ASM/DEP	Enrollment Program token	OS	The device's operating system.
ASM/DEP	Enrollment Program token	Device family	The device's Apple product family.
VPP	Apple Business Manager location token	Apple User ID	A user ID generated by Apple.
VPP	Apple Business Manager location token	application description	The description of a VPP application.
VPP	Apple Business Manager location token	application icon	The URL of an Apple hosted icon for a VPP app.
VPP	Apple Business Manager location token	Application ID	Apple Application ID, also known as adamsId.
VPP	Apple Business Manager location token	application name	The name of a VPP application.

Service	Message	Data sent to Intune	Used for
VPP	Apple Business Manager location token	assignedCount	The number of assigned licenses for an app.
VPP	Apple Business Manager location token	availableCount	The number of unassigned licenses for an app.
VPP	Apple Business Manager location token	bundleId	The bundleId of an app.
VPP	Apple Business Manager location token	copyright	The copyright info of an app.
VPP	Apple Business Manager location token	CountryCode	The country code of a VPP program.
VPP	Apple Business Manager location token	deviceAssignable	Apple returns true if the admin can assign a device license for an app. If not, false is returned.
VPP	Apple Business Manager location token	facilitatorMemberId	The member ID of a VPP account facilitator.
VPP	Apple Business Manager location token	genres	The genres of an app.
VPP	Apple Business Manager location token	Intune UserId guid	The GUID generated by Intune.
VPP	Apple Business Manager location token	isIrrevocable	Apple returns true if the license can't be revoked. If it can be revoked, false is returned.
VPP	Apple Business Manager location token	License ID	The ID generated by apple to identify a specific license.
VPP	Apple Business Manager location token	Location	Location stored in apple VPP config data.

Service	Message	Data sent to Intune	Used for
VPP	Apple Business Manager location token	Managed AppleId UPN	The AppleID email for user, admin, and facilitator member.
VPP	Apple Business Manager location token	OrganizationId	The Apple assigned organization ID.
VPP	Apple Business Manager location token	pricingParam	The Apple pricing type for an app.
VPP	Apple Business Manager location token	productType	The product type of a VPP application.
VPP	Apple Business Manager location token	retiredCount	The number of retired licenses for an app.
VPP	Apple Business Manager location token	totalCount	The total number of licenses purchased for an app.
VPP	Apple Business Manager location token	url	The iTunes store URL of an app.
VPP	Apple Business Manager location token	User Status	The user status in apple VPP programs.

To stop using Apple services with Microsoft Intune and delete the data, you must both disable the Microsoft Intune Apple token and also delete your Apple account. Refer to Apple account how to perform account management.

Feedback

Was this page helpful? Yes No

Data Google sends to Intune

Article • 03/03/2025

When Android enterprise device management is enabled on a device, Microsoft Intune establishes a connection with Google and user and device information is shared between Intune and Google. Before Microsoft Intune can establish a connection, you must create a Google account.

The following table lists the data that Google sends to Intune when device management is enabled on an Android device:

Expand table

Data Google sends to Intune	Details	Used for	Example
Enterprise data	Customer's enterprise identifiers in Google.	Links the customer's information between Intune and Google.	**enterpriseId** example: LC04eik8a6. **Name**. The Administrator name as entered when configuring Android enterprise. Example: Joe Smith. **Admin email**. YourAdmin@gmail.com that was used when configuring Android enterprise.
Application data	Data for managed Play Store applications.	Targeting the application to users or devices as available or required.	**Application Name** example: Contoso Warehouse Inventory Application. **Unique Identifier to represent application** example: app:com.Contoso.Warehouse.InventoryTracking
Service account	Unique internal Google service account for use with specific customer calls.	Used for making calls into Google on the customer behalf (to view apps, devices, and more)	**Name** example: InternalAccount@InternalService.com. **Keys** example: ServiceAccountPassword

To stop using Android enterprise device management with Microsoft Intune and delete the data, you must both disable the Microsoft Intune Android enterprise device management and also delete your Google account. Refer to Google account how to perform account management.

Data Intune sends to Apple

Article • 03/03/2025

When any of the following Apple services are enabled on a device, Microsoft Intune establishes a connection with Apple and shares user and device information with Apple:

- Apple Device Enrollment Program (DEP)
- Apple MDM Push certificate (APNS)
- Apple School Manager (ASM)
- Apple Volume Purchase Program (VPP)

Before Microsoft Intune can establish a connection, you must create an Apple account for each of the Apple services.

The following table lists the data that Microsoft Intune sends from a device to the enabled Apple services.

Expand table

Service	Data sent to Apple	Used for
APNS	Token, PushMagic	If the server accepts the device, the device provides its push notification device token to the server. The server should use this token to send push messages to the device. This check-in message also contains a PushMagic string. The server must remember this string and include it in any push messages it sends to the device.
ASM/DEP	Server token	Push notification device token used to authenticate to Apple service.
ASM/DEP	server_name	An identifiable name for the MDM server.
ASM/DEP	server_uuid	A system-generated server identifier.
ASM/DEP	admin_id	Apple ID of the person who generated the current tokens that are in use.
ASM/DEP	org_name	The organization's name.
ASM/DEP	org_email	The organization's email address.
ASM/DEP	org_phone	The organization's phone.
ASM/DEP	org_address	The organization's address.
ASM/DEP	org_id	DEP customer ID. This key is available only in protocol

Service	Data sent to Apple	Used for
		version 3 and later.
ASM/DEP	serial_number	The device's serial number (string).
ASM/DEP	model	The model name (string).
ASM/DEP	description	A description of the device (string).
ASM/DEP	asset_tag	The device's asset tag (string).
ASM/DEP	profile_status	The status of profile installation. Possible values: **empty**, **assigned**, **pushed**, or **removed**.
ASM/DEP	profile_uuid	The unique ID of the assigned profile.
ASM/DEP	device_assigned_by	The email of the person who assigned the device.
ASM/DEP	os	The device's operating system: iOS/iPadOS, OSX, or tvOS. This key is valid in X-Server-Protocol-Version 2 and later.
ASM/DEP	device_family	The device's Apple product family: iPad, iPhone, iPod, Mac, or AppleTV. This key is valid in X-Server-Protocol-Version 2 and later.
ASM/DEP	profile_name	String. A human-readable name for the profile.
ASM/DEP	support_phone_number	Optional. String. A support phone number for the organization.
ASM/DEP	support_email_address	Optional. String. A support email address for the organization. This key is valid in X-Server-Protocol-Version 2 and later.
ASM/DEP	department	Optional. String. The user-defined department or location name.
ASM/DEP	devices	Array of strings containing device serial numbers. (Might be empty.)
VPP	Intune UserId guid	GUID generated by Intune.
VPP	Location Token	Secure token used to link Intune with an Apple Business Manager or Apple School Manager tenant.
VPP	Managed AppleId UPN	AppleID that was specified by Admin when configuring the Apple Business Manager or Apple School Manager location token (VPP token) connection with Apple.
VPP	Serial Number	Serial number of the managed device.

To stop using Apple services with Microsoft Intune and delete the data, you must both disable the Microsoft Intune Apple token and also delete your Apple account. Refer to Apple account how to perform account management.

Feedback

Was this page helpful? 👍 Yes 👎 No

Data Intune sends to Google

Article • 03/03/2025

When Android enterprise device management is enabled on a device, Microsoft Intune establishes a connection with Google and shares user and device information with Google. Before Microsoft Intune can establish a connection, you must create a Google account.

The following table lists the data that Microsoft Intune sends to Google when device management is enabled on a device:

Expand table

Data sent to Google	Details	Used for	Example
EnterpriseId	Originated in Google upon binding your Gmail account to Intune.	Primary identifier used to communicate between Intune and Google. This communication includes setting policies, managing devices, and binding/unbinding of Android enterprise with Intune.	Unique identifier, Example format: LC04eik8a6
Policy Body	Originated in Intune when saving a new app or configuration policy.	Applying policies to devices.	A collection of all configured settings for an application or configuration policy. Policy Body can contain customer information if provided as part of a policy, such as network names, application names, and app-specific settings.
Device Data	Devices for Android Enterprise Corporate-Owned Personally-Owned Work Profile scenarios begin with enrollment in Intune. Devices for Managed device scenarios	Device Data information is sent between Intune and Google for various actions such as applying policies, managing the device and general reporting.	**Unique identifier to represent Device Name.** Example: enterprises/LC04ebru7b/devices/3592d971168f9ae4 **Unique Identifier to represent User Name.** Example: Enterprises/LC04ebru7b/users/116838519924207449711 **Device state.** Examples: Active, Disabled, Provisioning. **Compliance states.** Examples: Setting not supported, missing required apps **Software Info.** Examples: software versions & patch level. **Network Info.** Examples: IMEI, MEID, WifiMacAddress **Device Settings.** Examples: Information on encryption levels & whether device allows unknown apps. See the following example of a JSON message.

Data sent to Google	Details	Used for	Example
	begin with enrollment into Google.		
newPassword	Originated in Intune.	Resetting device passcode.	String representing new password.
Google User	Google	Managing the work profile for Personally-Owned Work Profile (BYOD) scenarios.	Unique identifier to represent the linked Gmail account. Example: 114223373813435875042
Application Data	Originated in Intune when saving application policy.		Application Name string. Example: app:com.microsoft.windowsintune.companyportal
Enterprise Service Account	Originated in Google upon Intune request.	Used for authentication between Intune and Google for transactions involving this customer.	There are several parts: **Enterprise Id**: documented previously. **UPN**: generated UPN used in authentication on behalf of customer. Example: w49d77900526190e26708c31c9e8a0@pfwp-commicrosoftonedfmdm2.google.com.iam.gserviceaccount.com **Key**: Base64 encoded blob used in auth requests, stored encrypted in the service, but this is what the blob looks like: Unique Identifier to represent the customer's key Example: a70d4d53eefbd781ce7ad6a6495c65eb15e74f1f
Registration Token	Originated in Google upon device enrollment.	Used to identify device when sending push notifications to the Company Portal app.	
User Principal Name (UPN)	Only the UPN of the user signed-in to the Intune console initiating the process to connect Google and Intune is sent as a pre-filled hint.	Used to prefill the admin email address field of the Google enterprise signup form.	

To stop using Android enterprise device management with Microsoft Intune and delete the data, you must disable both Microsoft Intune Android enterprise device management and also delete your Google account. Refer to Google account how to perform account management.

Feedback

Was this page helpful? 👍 Yes 👎 No

Data Intune sends to Zebra

Article • 03/03/2025

When Zebra LifeGuard Over-the-Air (LG OTA) is enabled for your tenant, Microsoft Intune establishes a connection with Zebra and shares the following data with Zebra:

The following table lists the data that Microsoft Intune sends to Google when device management is enabled on a device:

Expand table

Data sent to Zebra	Used for	Example
Serial number	Used to prove ownership of device against a known service contract with Zebra, determine current state of the device, and for the Android update process.	Unique identifier, example format: 124411614K0593
Deployment settings	Used to deliver Android updates.	• Device Model: TC8300 • Update type: Custom Time zone offset in minutes: 300 • BSP (Board Support Package): 11.15.05.00 • OS Version: 11 • Patch Number: U20 • Schedule mode: Latest • Schedule duration in days: 20 • Download network type: Wifi • Download start date and time: • 2022-03-25T15:04:51.8607086Z • Installation start date and time: • 2022-03-25T15:04:51.8607086Z • Installation window start time: 19:00:00 • Installation window end time: 19:00:00 • Minimum Battery level percentage: 30 • Require device to be on charger: true

To stop using Zebra services with Microsoft Intune and delete the data, you must both disconnect from Zebra LifeGuard OTA in Microsoft Intune, and also delete the data from your Zebra account by filing a customer request with Zebra.

Feedback

Was this page helpful? 👍 Yes 👎 No

Enable use of Windows diagnostic data by Intune

Article • 03/03/2025

Before you can use some Intune features, you must enable *Windows diagnostic data in processor configuration* for your tenant. Doing so enables you as the controller of Windows diagnostic data collected from your devices to then allow its use by Intune when it's required by features that are dependent on that data.

In addition, several of the features that require Windows diagnostic data also require you to have Windows E3 (or equivalent) licenses, and you must attest to having these licenses to enable use of those features.

Both configuration of the Windows diagnostic data in processor configuration and the license attestation are configured on the **Windows data** page of the Microsoft Intune admin center.

Manage Windows data configurations

To manage Windows data configurations for your tenant, open the Microsoft Intune admin center and go to **Tenant administration** > **Connectors and tokens** > **Windows data**.

On the *Windows data* page, you can configure your tenant to support Windows diagnostic data in processor configuration, and to attest ownership of the required Windows E3 or equivalent licenses. It's possible that some features require only one of the available configurations to be enabled, while other features could require both.

Windows data

Use the *Windows data* category to enable use of Intune features in your tenant that require diagnostic data in processor configuration.

The following features require you to enable this support:

- Windows feature update device readiness report
- Windows feature update compatibility risks report
- Windows driver updates report
- Windows feature update report
- Windows expedited Update Report

- Driver update policies with alerts / Windows driver update failures
- Expedited quality update policies with alerts / Windows expedited update failures
- Feature update policies with alerts / Feature update failures

To enable support, set **Enable features that require Windows diagnostic data in processor configuration** to **On**. By default, it's *Off*.

- While there are other methods to enable this support for a tenant, this toggle only reflects your configuration choice for Intune features.
- Changing this toggle from *On* to *Off* disables use of Intune features that require this configuration but might not turn off processor configuration configured by other methods.

To learn more about this configuration, see Enable Windows diagnostic data processor configuration in the Windows privacy documentation.

Windows license verification

Use the *Windows license verification* category to enable use of Intune features in your tenant that require Windows E3 or equivalent licenses.

The following features require you to attest to having Windows E3 or equivalent licenses:

- Windows update app and driver compatibility reports

Supported licenses include the following options:

- Windows 10 or later Enterprise E3 or E5; or Microsoft 365 F3, E3, or E5.
- Windows 10 or later Education A3 or A5; or Microsoft 365 A3 or A5.
- Windows Virtual Desktop Access E3 or E5.

To confirm you own the required licenses for these features, set **I confirm that my tenant owns one of these license** to **On**. By default, it's *Off*.

- Other features can require these same licenses, but only the features listed in this section currently require this toggle to be set to *On*.
- Features that require this attestation aren't available for use when this toggle is set to *Off*.

Next steps

To learn more about Windows diagnostic data collection, see Configure Windows diagnostic data in your organization in the Windows privacy documentation.

Feedback

Was this page helpful? 👍 Yes 👎 No

Data Jamf Pro sends to Intune

Article • 03/03/2025

When you use Jamf Pro to manage your end-users Macs with Intune, Jamf Pro captures inventory information about managed macOS devices.

Data

For the list of data that Jamf Pro shares with Intune, see Appendix: Inventory Information Shared with Microsoft Intune in the Jamf Pro technical documentation.

Next steps

Get information on how to remove a Jamf-managed device from Intune and Microsoft Entra ID. You can also file a support ticket with Jamf support for more help.

Feedback

Was this page helpful? Yes No

View and correct personal data

Article • 03/03/2025

Based on their access permissions, Intune admins can view some personal data that's been collected by Intune but can't change that data. Only end users can change their device's personal data that has been collected by Intune.

> ⓘ **Note**
>
> If you're interested in viewing or deleting personal data, please see the Azure Data Subject Requests for the GDPR article. If you're looking for general info about GDPR, see the GDPR section of the Service Trust portal.

View personal data

Admins can see end user personal information in various Nodes of the Intune UI in the Microsoft Intune admin center. The following articles explain what information admins do and don't have access to:

- See device details in Intune explains how you can review details about an end user's device.
- Monitor app information and assignments explains how to see details about apps installed on an end user's device.
- The What information can my company see when I enroll my device? article gives end users a list of data that their company can and can't see. It's best to clearly tell your users what kind of data you're collecting and why you're collecting it. This article can be the first step in that transparency.

Who can view the data?

Microsoft uses strict controls to govern access to customer data, granting the lowest level of access required to complete key tasks and revoking access when it's no longer needed.

You can secure and control access to end user personal data by using role-based administration control (RBAC). For more information, see RBAC with Microsoft Intune.

You can learn more about Microsoft data practices by reading the Online Services Terms and Microsoft Online Services Privacy Statement.

Correct end user personal data

Admins can't update device or app specific information. If an end user wants to correct any personal data (like the device name), they must do so directly on their device. Such changes are synchronized the next time they connect to Intune.

Next steps

Find out how to audit, export, or delete personal data in Intune.

Feedback

Was this page helpful? 👍 Yes 👎 No

Audit export or delete personal data in Intune

Article • 04/10/2025

Intune admins can use audit logs to track activities surrounding personal data. Admins can also export and delete personal data.

> ⓘ **Note**
>
> This article provides steps for how to delete personal data from the device or service and can be used to support your obligations under the GDPR. If you're looking for general info about GDPR, see the GDPR section of the Service Trust portal.

Audit personal data

Audit logs provide tenant admins with a record of activities that generate a change in Microsoft Intune. Audit logs are available for many manage activities and typically create, update (edit), delete, and assign actions. Remote tasks that generate audit events can also be reviewed. These audit logs might contain personal data from users whose devices are enrolled in Intune.

For security purposes, Intune maintains audit logs for user and device actions for one year. These logs are automatically deleted after the one-year retention period.

To review audit logs, see Audit logs for Intune activities.

Admins can't delete audit logs.

These audit events are retained for one year. Tenant admins can request audit logs using this support request form.

Export personal data

Admins can export end user personal data, including accounts, service data, and associated logs to comply with Data Subject Rights Requests. You and your organization can decide whether to provide the data subject with a copy of their personal data or withhold it if you have a legitimate business reason. If you choose to provide it, you can give them a copy of the document, a redacted version, or a screenshot of the parts you want to share.

To export a user's personal data, you can use:

- the *Export* option on the *All devices* node of the Microsoft Intune admin center to export a list of devices. You can also copy device data directly.
- the Export-IntuneData.ps1 script.

Delete end user personal data

There are three ways to remove personal data from Intune management:

- Delete the user from Microsoft Entra ID
- Reset the device to factory settings
- User self-removal

Delete a user from Intune

To delete an end user's personal data from Intune, an admin must delete the user from Microsoft Entra ID. When the user is deleted from Microsoft Entra ID (hard deleted), Intune receives the *Delete* signal from Microsoft Entra ID and then automatically begins purging all of that user's personal data from the Intune service. The user's information is deleted from Intune service within 30 days of the removal action.

Reset device to factory settings

Resetting to factory settings restores all company and personal data and settings to the original factory settings. It's useful before providing a device to the next employee. User files, user installed applications, and non-default settings are removed and this data is deleted from the Intune service within 30 days of the removal action.

User self-removal from Intune management

Users can remove their Android, Apple, or Windows personal device from Intune management without admin assistance.

Retire

The **Retire** action removes Intune provisioned data like company applications, data about apps that Intune is managing, policy settings, and email profiles that are provisioned through Intune. This action leaves the user's personal data on the device.

BIOS passwords

If Intune has configured a BIOS password for the device as part of BIOS configuration management, the BIOS password remains on the device until explicitly removed. BIOS passwords could be removed by editing the **BIOS configuration and other settings** policy, or locally on the device by changing the existing password.

Delete a tenant from Microsoft Intune

If an Intune tenant customer cancels their Intune account, all tenant data is deleted within 180 days after the customer closes the Intune account. If the Microsoft Entra tenant is associated with other Microsoft enterprise subscriptions (Azure, Microsoft 365), then only the Intune Customer Data is deleted. The Microsoft Entra tenant resource is maintained for use by the other subscriptions. If the Intune account is the only subscription associated with the Microsoft Entra tenant, then the tenant is deleted and all resources and Customer Data are also deleted.

Next steps

Find out how to view and correct personal data personal data in Intune.

Learn about Windows Information Protection and Microsoft Intune

Article • 03/03/2025

> ⓘ **Note**
>
> Microsoft Intune has discontinued future investments in managing and deploying Windows Information Protection.
>
> Support for the Windows Information Protection without enrollment scenario in Microsoft Intune has been removed.
>
> For more information, see End of support guidance for Windows Information Protection.
>
> For information about Intune MAM on Windows, see MAM for Windows and App protection policy settings for Windows.

With the increase of employee-owned devices in the enterprise, there's also an increasing risk of accidental data leaks through apps and services, like email, social media, and the public cloud, which are outside of the enterprise's control. For example, an employee sends the latest engineering pictures from a personal email account, copies and pastes product info into a tweet, or saves an in-progress sales report to public cloud storage.

Windows Information Protection helps to protect against this potential data leakage without otherwise interfering with the employee experience. It also helps to protect enterprise apps and data against accidental data leaks on enterprise-owned devices and personal devices that employees bring to work without requiring changes to your environment or other apps.

You can use the Intune Windows Information Protection policy to manage the list of apps protected by Windows Information Protection, enterprise network locations, protection level, and encryption settings.

> ⓘ **Note**
>
> To use the Company Portal app with Windows Information Protection, you must add the Company Portal app under the Windows Information Protection mode of **Exempt**.

For more information, see:

- Protect your enterprise data using Windows Information Protection.
- Create a Windows Information Protection (WIP) policy using the Azure portal for Microsoft Intune

Feedback

Was this page helpful? 👍 Yes 👎 No

View details about your Tenant on the Intune tenant status page

Article • 03/03/2025

The Microsoft Intune tenant status page is a centralized hub where you can view important details about your tenant. Details include:

- Your tenant name and location
- Service release versions
- Licensed users and enrolled devices

> ⓘ **Important**
>
> To access the Tenant administration page, you need to have the following Intune permissions: Organization.Read, ManagedDevice.Read, and ManagedApp.Read. These permissions are granted to the **Intune Read Only Operator** RBAC built-in role. You can create a custom role that contains those permissions (recommended for least-permission), or you can use one of the EntraID privileged roles: "Intune Administrator" or "Global Administrator". Use of Entra Identity Management (PIM) roles is supported when elevated prior to viewing the tenant status page.

You can also view the status of the Intune connectors you've configured, and health messages for the Intune service and general messages for Tenants.

> **Tip**
>
> A tenant is an instance of Microsoft Entra ID. Your subscription to Intune is hosted by a Microsoft Entra tenant. For more information, see Set up a tenant in the Microsoft Entra documentation.

To view the dashboard, sign in to the Microsoft Intune admin center go to **Tenant administration**, and then select **Tenant Status**.

The page is divided into three tabs:

Tenant details

Tenant details provide at-a-glance information about your tenant. View details like your tenant name and location, your MDM Authority, and your tenants service release number. The service release number is a link that opens What's new in Intune. In *What's new*, you can read about the latest features and updates to the Intune service.

On this tab, you'll also find basic information about your available licenses and how many are assigned to users. Licenses for devices aren't shown.

> ⓘ Important
>
> Note that *Total licensed users* refers to all users which have one license containing an Intune SKU, if the Intune SKU is enable or disable they still count as a licensed user.

Connector status

Connector status is a one-stop location to review the status of all available connectors for Intune.

Connectors are:

- **Connections you configure to external services**. For example, the *Apple Volume Purchase Program* service or the *Windows Autopilot* service. Status for this type of connector is based on the last successful synchronization time.
- **Certificates or credentials that are required to connect to an external unmanaged service**, like *Apple Push Notification Services* (APNS) certificates. Status for this type of connector is based on the expiry timestamp of the certificate or credential.

When you open the *Connector status* tab, any unhealthy connectors display at the top of the list. Next are connectors with warnings, and then the list of healthy connectors. Connectors you haven't yet configured appear last as *Not Enabled*.

When there's more than a single connector of any one type, the status is a summary for all of those same connectors. The least healthy status of any single connector is used as the health for the group.

> ⓘ Important
>
> Some connectors can report a status of *Healthy* or *Connected* but might not be functioning correctly. If you encounter issues with a specific connector, review any applicable connector logs or open a case with support to investigate further.

Connector status:

- **Unhealthy:**
  - The certificate or credential has expired
  - The last synchronization was three or more days ago
- **Warning:**
  - The certificate or credential will expire within seven days
  - The last synchronization was more than one day ago
- **Healthy:**
  - The certificate or credential won't expire within the next seven days
  - The last synchronization was less than one day ago

When you select a connector from the list, the portal presents the portal page that is relevant to that connector. From the connectors page, you can view the status for previously configured connectors. You can also select options to add or create a new connector of that type.

For example, if you select the **VPP Expiry Date** connector, the **iOS Volume-Purchased Program Tokens** page opens. On this page you can view more details about that connector, create a new configuration, or edit and fix issues with an existing one.

Service health and message center

The Service health and message center page is where you can view details about the Intune *Service health*, *Issues in your environment that require action*, and *Message center* posts that can provide information about updates and planned changes.

You can only set up your communication preferences for Intune Message center through the Microsoft 365 admin center. To do so, sign in to the Microsoft 365 admin center and go to **Health** > **Service health**. Select **Customize**, and then open the **Email** tab. On the *Email* tab, select the checkbox for **Send me email notifications about service health**, and then configure the additional preferences to meet your requirements.

Service health

View details for active incidents and advisories in the Microsoft Intune admin center. Only incidents that affect your tenant are shown. This information is also available in on the Service health page of the Microsoft 365 admin center.

When you select an incident, the incident details are presented directly in the Tenant Status page. To view past advisories and incidents, select **See past Incidents/Advisories**.

The Microsoft 365 admin center opens and you can then view advisories and incidents from the last 30 days for your tenant.

To view information for *Service health*, your account must have the **Global Administrator** or **Service support administrator** role in Microsoft Entra ID or the Microsoft 365 admin center. To assign these permissions, sign in to the Microsoft 365 admin center ↗ with Global Administrator permissions. Select **Users** > **Active Users**, and then select the account that requires access. Select **Edit** for Roles, select *Service support administrator* or *Global Administrator*, and then **Save** your edit to assign the permissions.

Issues in your environment that require action

The **Issues in your environment that require action** section displays messages that are sent to alert tenant administrators about issues that might require action to resolve.

To view information for *Issues in your environment that require action*, your account must have the **Global Administrator** or **Service support administrator** role in Microsoft Entra ID or the Microsoft 365 admin center. To assign these permissions, sign in to the Microsoft 365 admin center ↗ with Global Administrator permissions. Select **Users** > **Active Users**, and then select the account that requires access. Select **Edit** for Roles, select *Service support administrator* or *Global Administrator*, and then **Save** your edit to assign the permissions.

Intune Message center

View informational communications from the Intune service team without having to navigate to the Office Message Center. Communications include messages about changes that have recently happened to the Intune service, or that are on the way for your tenant.

By default, the 10 most recent and active messages display. To view older messages, select **See past Messages** to open the *Message center* in the Microsoft 365 admin center.

To view information for Intune News, your account must have the **Global Administrator** or **Service support administrator** role in Microsoft Entra ID, or the **Message Center reader** role in the Microsoft 365 admin center. To assign this permission, sign in to the Microsoft 365 admin center ↗ with administrator permissions. Select **Users** > **Active Users**, and then select the account that requires access. Select **Edit** for *Roles*, select *Teams Communications Administrator*, and then **Save** your edit to assign the permissions.

Next steps

- Walkthrough the Microsoft Intune admin center
- Get support for Intune

Feedback

Was this page helpful? 👍 Yes 👎 No

Use the troubleshooting dashboard to help users at your company

Article • 03/03/2025

The troubleshooting pane lets help desk operators and Intune administrators view user information to address user help requests. Organizations that include a help desk can assign the Help desk operator role to a group of Intune users. The help desk operator role can use the **Troubleshooting + support** pane help end users.

The **Troubleshooting + support** pane provides three options:

- Guided scenarios to provide a customized series of steps centered around one end-to-end use-case. For more information, see Guided scenarios.
- **Troubleshooting** to help determine any issues with **Assignments**, **App protection status**, and **Enrollment failures**.
- Help and support to provide global technical, pre-sales, billing, and subscription support for device management cloud-based services related to Intune. For more information, see Help and support.

Details about the issue and suggested remediation steps can help administrators and help desk operators troubleshoot problems. Certain enrollment issues aren't captured and some errors might not have remediation suggestions.

> ⓘ Note
>
> For steps on adding a help desk operator role, see Role-based administration control (RBAC) with Intune

When a user contacts support with a technical issue with Intune, the help desk operator enters and finds the user's name. Additionally, the help desk operator can filter by device if the user has multiple managed devices.

The **Troubleshooting** pane provides the following tabs for a selected user and allows you to quickly narrow the troubleshooting focus:

- **Summary** - Provides specific counts of issues related to policy, compliance, app protection, applications, devices, roles, and scopes.
- **Devices** - Provides details for devices, such as OS, OS Version, Intune compliance, and last check-in.
- **Groups** - Provides details for groups, such as membership type.

- **Policy** - Provides policy details, such as assignment, type, platform, and last modified.
- **Applications** - Provides app install status, assigned, platform, type, and last modified.
- **App protection policy** - Provides the name, platform, and enrollment details for app protection policies.
- **Updates** - Provides the name, platform, and update type.
- **Enrollment restrictions** - Provides the policy type, name, platform, and device limit.
- **Diagnostics** - Provides the device name or application, platform, created date, and diagnostic log.
- **ServiceNow incidents** - Provides a list of associated incidents for the selected user. For more information, go to ServiceNow integration with Intune.

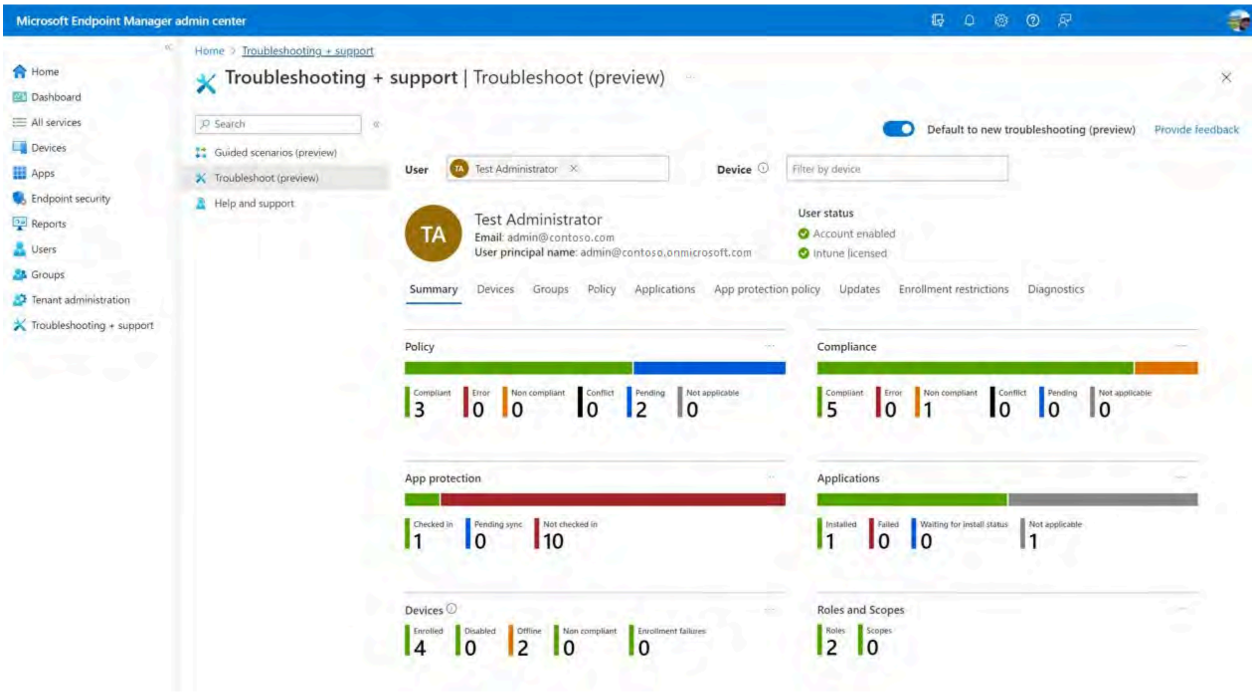
View user troubleshooting details

In the **Troubleshooting** pane provides specific details for each Intune end-user. User information can help you understand the current state of users and their devices.

1. Sign in to Microsoft Intune admin center ↗.
2. Select **Troubleshooting + support** > **Troubleshoot**.
3. Find and select a **User** by entering a display name or email.
4. If the user has multiple devices, filter by **Device**.
5. Review the provided information to help troubleshoot end-user issues.

Areas of the troubleshooting dashboard

You can use the **Troubleshooting + support** pane to review a variety of managed user and device information.



Troubleshooting + support | Troubleshoot (preview)

Default to new troubleshooting (preview)

User Test Administrator

Device Filter by device

Test Administrator
Email: admin@contoso.com
User principal name: admin@contoso.onmicrosoft.com

User status
Account enabled
Intune licensed

Policy

Compliant	Error	Non compliant	Conflict	Pending	Not applicable
3	0	0	0	2	0

Compliance

Compliant	Error	Non compliant	Conflict	Pending	Not applicable
5	0	1	0	0	0

App protection

Checked in	Pending sync	Not checked in
1	0	10

Applications

Installed	Failed	Waiting for install status	Not applicable
1	0	0	1

Devices

Enrolled	Disabled	Offline	Non compliant	Enrollment failures
4	0	2	0	0

Roles and Scopes

Roles	Scopes
2	0

Summary

The **Summary** tab provides overall details for the user who is managed by Intune.

Expand table

Column	Description
Policy	The status of the policies available for the user or device.
Compliance	The compliance status for the user or device.
App protection	App protection details.
Applications	The state of the applications for the user or device.
Devices	The status of the device(s) related to the user.
Role and scope	The role and scope for the user.

Devices

The **Devices** tab provides details for devices, such as OS, OS Version, Intune compliance, and last check-in.

Expand table

Column	Description
Name	The name of the device.
Managed by	Identifies how the device is managed. For more information, see Available details by management type.
Ownership	The type of device ownership (**Company**, **Personal**, or **Unknown**).
Intune compliant	Identifies whether the device is compliant with Intune. Should be **Yes**. If **No** is shown, there may be an issue with compliance policies, or the device isn't connecting to the Intune service. For example, the device may be turned off, or may not have a network connection. Eventually, the device becomes non-compliant, possibly after 30 days. For more information, see Use compliance policies to set rules for devices you manage with Intune.
Microsoft Entra compliant	Identifies whether the device is compliant with Microsoft Entra ID. Should be **Yes**. If **No** is shown, there may be an issue with compliance policies, or the device isn't connecting to the Intune service. For example, the device may be turned off, or may not have a network connection. Eventually, the device becomes non-compliant, possibly after 30 days. For more information, see Use compliance policies to set rules for devices you manage with Intune.
App lifecycle status	Denotes whether an app install failure or success has occurred on the individual device.
OS	The Operating System installed on the device.
OS version	The Operating System version number of the device.
Last check-in	The timestamp of the last time the device checked in.

Groups

The **Groups** tab provides the group membership of all Microsoft Entra groups for a specific managed device. For related information, see Device group membership report.

Expand table

Column	Description
Name	The name of the group.
Object ID	The Object ID is used by Microsoft Entra ID. Intune commonly refers to them as Group ID.
Membership type	Provides how you assign and add users. **Assigned** denotes you manually assign users or devices to the group, and manually remove users or devices. **Dynamic User** denotes you create membership rules to automatically add and remove

Column	Description
	members. **Dynamic Device** denotes you create dynamic group rules to automatically add and remove devices.
Direct or Transitive	Identifies whether the device is a direct member or a transitive member.

Policy

The **Policy** tab provides the policies applied to devices, which include policy details, such as assignment, type, platform, and last modified.

⛶ Expand table

Column	Description
Name	The name of the device policy.
Assignment	Identifies the assignment status of the device.
Type	The type of policy.
Platform	The type of device platform.
Last Modified	The timestamp of the last time the device synchronized with Intune.

Applications

The **Applications** tab provides managed app install status, assigned, platform, type, and last modified.

⛶ Expand table

Column	Description
Name	The name of the application.
App install status	The installation status of the app.
Assigned	Provides whether the app has been assigned.
Platform	The type of device platform.
Type	You can choose an assignment type for each app. **Available** denotes that users install the app from the Company Portal app or website. **Not Applicable** denotes that the

Column	Description
	app is not installed or shown in the Company Portal. **Uninstall** denotes that the app is uninstalled from devices in the selected groups. **Available with or without enrollment** denotes that this app is assigned to groups of users whose devices are not enrolled with Intune.
Last modified	The timestamp of the last time the device synchronized with Intune.

App protection policy

The **App protection policy** tab provides the name, platform, and enrollment details for app protection policies. An app protection policy is available to mobile apps that integrate with EMS technologies. These policies give a baseline of protection for your corporate data when it is downloaded to mobile apps, including the Office mobile apps.

⛶ Expand table

Column	Description
Name	The name of the app protection policy.
Platform	The platform of the device.
Enrollment	The enrollment status of the device.

Updates

The **Updates** tab provides an overall view of updates that are deployed to users. This information also provides filtering, searching, paging, and sorting.

⛶ Expand table

Column	Description
Name	The update name.
Platform	The platform of the device intended for the update.
Update type	The type of update.

Enrollment restrictions

The **Enrollment restrictions** tab provides the policy type, name, platform, and device limit. Enrollment restrictions are use to prevent (block) personally owned devices from enrolling, you will need to add the devices using corporate device identifiers, prior to enrollment.

Properties

Expand table

Column	Description
Policy type	The type of policy.
Name	The name of the policy.
Platform	The platform of the device.
Device limit	The enrollment restriction to limit the number of devices a user can enroll in Microsoft Intune.

Diagnostics

The **Diagnostics** tab provides the device name or application, platform, created date, and diagnostic log.

> ⓘ Note
>
> To collect and access diagnostics you must have the Collect diagnostics permission added to your role. For more information, see Role-based administration control (RBAC) with Intune.

Expand table

Column	Text
Device name or application	The name of the device or application.
Platform	The platform of the device.
Created date	The timestamp of when the event occurred.
Diagnostic log	The diagnostic log file.

Collect available data from mobile device

Use the following resources to help collect device data when troubleshooting user's device issues:

- Report a problem in Company Portal for iOS
- Report a problem in Company Portal or Intune app for Android

You can access and download user-submitted logs under **Diagnostics**.

Next steps

You can learn more about Role-based administration control (RBAC) to define roles in your organizational device, mobile application management, data protection tasks. For more information, see Role-based administration control (RBAC) with Intune.

Learn about any known issues in Microsoft Intune. For more information, see Known issues in Microsoft Intune.

Learn how to create a support ticket a get help when you need it. Get support.

Feedback

Was this page helpful? Yes No

ServiceNow Integration with Microsoft Intune

Article • 03/03/2025

Remote Help, an add-on to Microsoft Intune, provides a secure cloud based remote assistance solution for Windows commercial users. The integration between Intune and ServiceNow makes it possible for helpdesk agents to use Intune to troubleshoot endpoint related issues.

Support organizations need all the tools at their disposal to resolve workers' technology issues quickly and efficiently. With ServiceNow integration, helpdesk agents licensed to use Remote Help and who use ServiceNow can view incidents to see the details of the tech issue that an employee is facing. This integration allows helpdesk agents to view ServiceNow incidents directly from the Troubleshooting pane in the Microsoft Intune admin center.

About ServiceNow connector Integration

ServiceNow is a third party platform for IT Service Management and helps to automate IT Business Management. For more information on ServiceNow, go to:

- ServiceNow

The Intune ServiceNow Connector Integration focuses on creating a basic ticketing flow to enable IT admins to view the history of ServiceNow incidents in the MEM portal, device inventory, MEM insights enhanced ticket flows, and software licensing and reclamation.

Prerequisites

To get started, review the following steps:

- ServiceNow integration is now Generally Available. An active Intune Suite or Remote Help trial or add-on license is required. Go to Remote Help trial or add-on license.

- You must have the Microsoft Entra Global Admin Role or Microsoft Entra Intune Admin role to make updates to the connector. To view the incidents, you must have the Microsoft Entra Global Admin Role or Microsoft Entra Intune Admin role or have an Intune Role with the Organization | Read permission. Admins that aren't assigned the Microsoft Entra roles, need one of these two permissions to either modify the connector or view incidents respectively; **Update Connector** and **View Incidents**. These permissions are part of the ServiceNow permission category. For information on roles, see Role-based administration control with Intune

- You must have ServiceNow permissions to view incidents when using the **Test connection** action. You can assign the *itil* role to grant appropriate permissions to view incidents. A ServiceNow license needs to be assigned to admins who view incidents.

- You must have the Troubleshooting Preview enabled. To enable the Troubleshooting Preview, select **Preview upcoming changes to Troubleshooting and provide feedback** in the Troubleshooting pane. After reviewing the Troubleshooting preview information, select **Try it now** to enable the preview.

- To configure the ServiceNow connector to establish a connection between Intune and your ServiceNow instance. See the steps outlined in Configure the ServiceNow integration with Microsoft Intune.

Configure the ServiceNow integration with Microsoft Intune

1. Sign into Microsoft Intune admin center and go to **Tenant Administration** > **Connectors and Tokens** > **ServiceNow connector**.

2. You can see the **Connection Status** and the **Last Connection** date time stamp.

3. Use the toggle to either turn on or off the ability to **Exchange data with the ServiceNow instance**.

4. Next, define the following properties for how you're going to connect with ServiceNow.

Expand table

Field	Description
ServiceNow Instance Host	A URL that points to your organization's ServiceNow instance. For example, 'https://contoso.service-now.com'
ServiceNow Incident API URL	The table in the ServiceNow database that contains incidents. Incidents are retrieved from this table. For example, /api/now/table/incident

Field	Description
ServiceNow Client appID	The unique identifier assigned in ServiceNow to the application used to represent Intune. Provide the client ID of the app. You need to have a client app created in ServiceNow to copy over the appID and use it here to establish the connection. Go to How to create a ServiceNow app.

5. Select **Test connection** to verify if your settings are correct. You see a verification message to connect to your ServiceNow account. Select **Allow**.

6. The **Connection Status** field is updated and now displays Verified.

7. Select **Save** to save your connection settings.

8. The ServiceNow connector is configured successfully. Let's see how to use it in the ServiceNow incident view in Microsoft Intune.

How to create a ServiceNow app

In your ServiceNow developer instance you need to:

- create a new OAuth application
- create a new CORS Rule

To create a new OAuth application,

1. In the developer instance, select **All** and navigate to **System OAuth** > **Application Registry**.

2. Set up a new OAuth application.

3. Choose 'OAuth API endpoint for external clients'

4. Complete the following OAuth client application details and select **Save**.

Expand table

Field	Description
Client ID	The ServiceNow OAuth server automatically generates the ClientID. This value is used as an input in the **ServiceNow client appID** field for the Serv
Client Secret	Client Secret for the OAuth generation. Leave it empty for auto-generation.
Redirect URL	The authorization server redirects to this URL. They must be an absolute URL and comma separated. For example, you can set the URL to 'https://intune.microsoft.com/TokenAuthorize/ExtensionName/Microsoft_Intune_DeviceSettings,https://intune.microsoft.com/TokenAuthorize/Exte
Logo URL	Provide the URL to the publicly hosted company logo, which is displayed when authenticating with ServiceNow. For example, you can set it to: 'htt SJfnMq3/0/XL/i-SJfnMq3-XL.png'
Application	By default, set to **Global** and isn't editable when creating the OAuth app.
Accessible from	By default, set to **All application scopes**.
Active	Select the checkbox.
Refresh Token Lifespan	Enter the max time for which the refresh token remains valid in seconds.
Access Token Lifespan	Enter the max time for which the access token remains valid in seconds. The recommended setting is 15 minutes. A warning message appears If co

To create a new CORS rule,

1. In the developer instance, select **All** and navigate to **System Web Services** > **Rest**> **CORS Rules**.

2. Create a new CORS rule. Configure CORS rules to allow cross-domain requests to REST APIs from a browser-based application in a different domain.

3. Complete the following CORS rule details and select **Save**.

Expand table

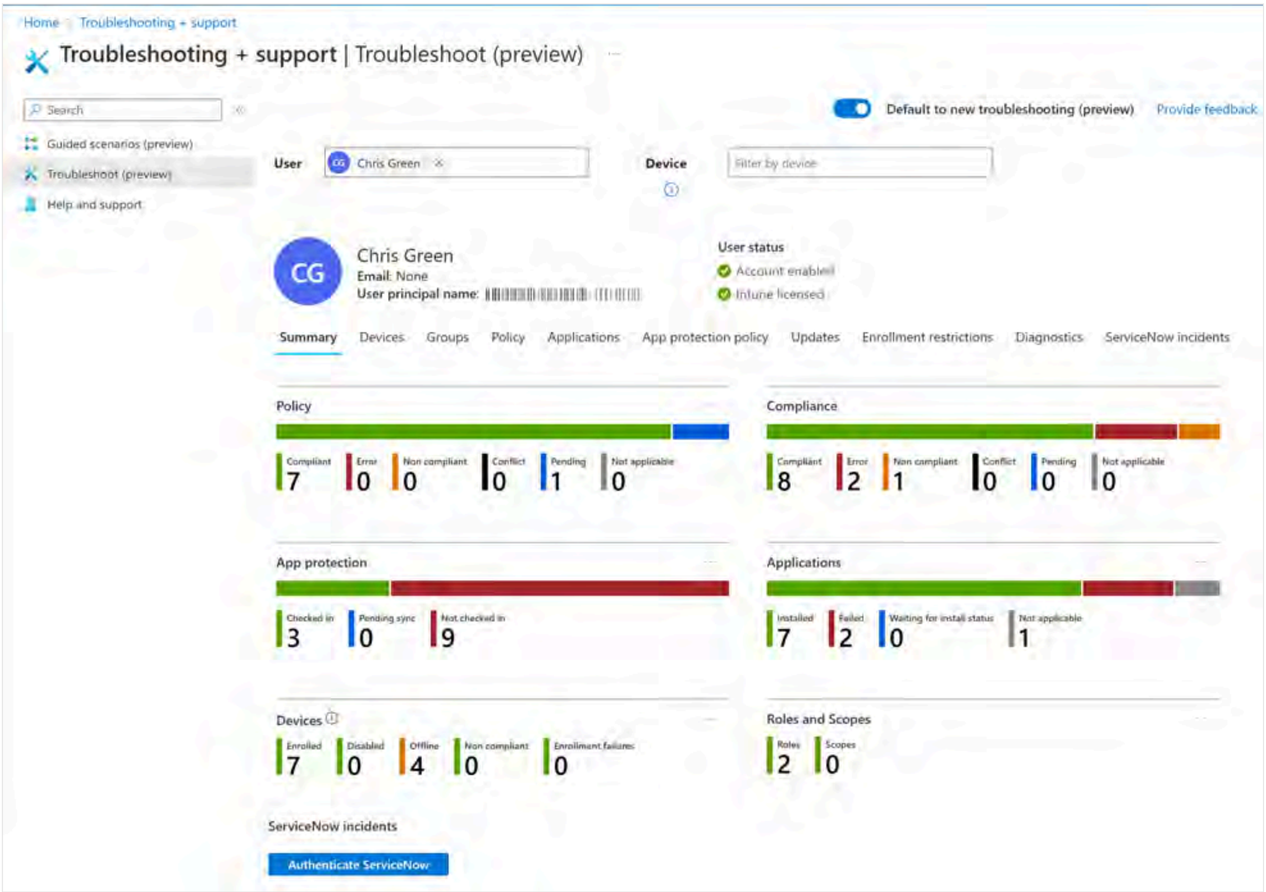
Field	Description
Application	By default, Application is set to **Global** and isn't editable.
REST API	Set to Table API.
Domain	Set the domain. For example, 'https://*.portal.azure.net'
HTTP Methods	Select GET and POST.

> ⓘ **Note**
>
> CORS rules can take up to 30 minutes to propagate.

ServiceNow incident view in Microsoft Intune

With the ServiceNow connector verified and enabled, you can view a real time list of ServiceNow incidents for a worker from the Troubleshooting pane. The incident view with details helps you understand if there are other issues previously submitted by employees that might be related or have recurred.

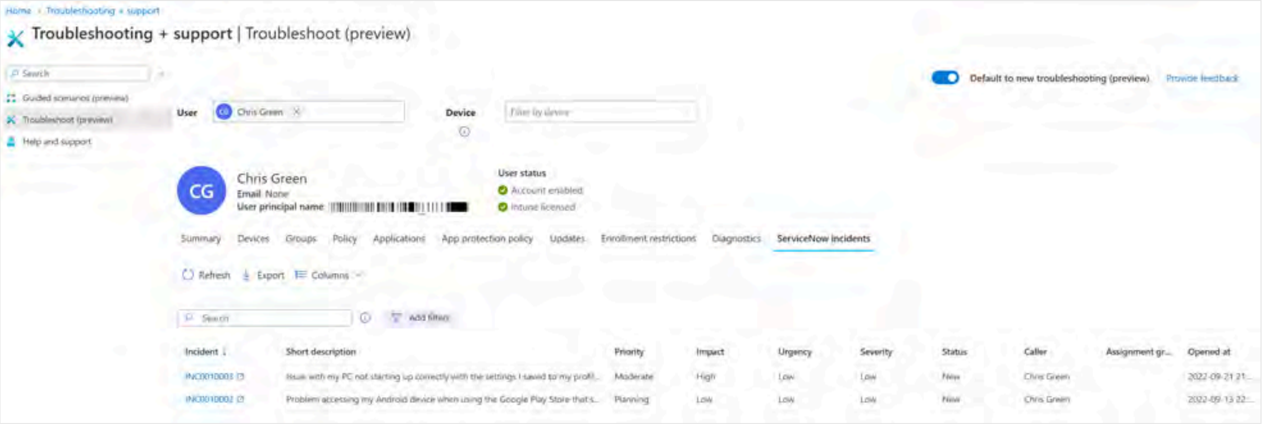
1. Sign in to Microsoft Intune admin center.
2. Select **Troubleshooting + support** > **Troubleshoot**. The **Troubleshooting** pane provides specific details for each Intune end-user.
3. Find and select a **User** by entering a display name or email.
4. In the **Summary** tab, scroll down and select **Authenticate ServiceNow**. Enter the credentials to authenticate you as a help-desk operator with ServiceNow.



5. Choose **Allow**. You can now see the number of incidents associated with the user you selected.
6. Alongside the **Summary** tab, find and select the **ServiceNow Incidents** tab. Selecting the tab brings up a list of associated incidents for the selected user. The incident view helps you understand if there are other issues previously submitted by employees that might be related or have recurred.

   - The columns visible in the list view can be modified by selecting or deselecting the ones to show in the **Column** field.
   - You can also add some filters for the incidents that you need to be displayed. For example, you might only want new incidents to appear in the list. To add a filter, select **Add Filters**, set **Status** to New and select **Apply**.

7. The **Incident** column list in the **ServiceNow Incidents** tab includes a link to the source incident in ServiceNow.



Home > Troubleshooting + support

Troubleshooting + support | Troubleshoot (preview)

Search
Guided scenarios (preview)
Troubleshoot (preview)
Help and support
Default to new troubleshooting (preview)
Provide feedback

User Chris Green

Device Filter by device

Chris Green
Email None
User principal name [redacted]

User status
Account enabled
Intune licensed

Incident	Short description	Priority	Impact	Urgency	Severity	Status	Caller	Assignment gr...	Opened at
INC0010003	Issue with my PC not starting up correctly with the settings I saved to my profil...	Moderate	High	Low	Low	New	Chris Green		2022-09-21 21:...
INC0010002	Problem accessing my Android device when using the Google Play Store that's...	Planning	Low	Low	Low	New	Chris Green		2022-09-13 22:...

8. Select the Incident link to launch the incident view in ServiceNow. Help-desk agents must be given the appropriate permissions in ServiceNow, to launch the incident view in ServiceNow and view the full incident details.
9. Review the provided information to help troubleshoot end-user issues.

Data Exchange

Intune exchanges the following information with ServiceNow: CALLERID, NAME, NUMBER, UNIVERSAL PRINCIPAL NAME, URGENCY, IMPACT, SEVERITY, ASSIGNMENT_GROUP, OPENEDAT, STATE, PRIORITY, SHORT DESCRIPTION, SYSID.

Next steps

- Get support in Microsoft Intune admin center
- Use Remote Help

Feedback

Was this page helpful? Yes No

Use Remote Help with Microsoft Intune

Article • 05/12/2025

> ⓘ **Note**
>
> This capability is available as an Intune add-on. For more information, see Use Intune Suite add-on capabilities.

Remote Help is a cloud-based solution for secure help desk connections with role-based access controls. With the connection, your support staff can remote connect to the user's device.

In this article, users who provide help are referred to as *helpers*, and users that receive help are referred to as *sharers* as they share their session with the helper. Both helpers and sharers sign in to your organization to use the app. It's through your Microsoft Entra ID that the proper trusts are established for the Remote Help sessions.

Remote Help uses Intune role-based access controls (RBAC) to set the level of access a helper is allowed. Through RBAC, you determine which users can provide help and the level of help they can provide.

> ⓘ **Important**
>
> This article describes the capabilities and configuration tasks that are applicable in general for Remote Help across supported platforms. For specific capabilities, prerequisites, and other details based on the platform that you are using, go to:

> - Remote Help on Windows with Microsoft Intune
> - Remote Help on Android with Microsoft Intune
> - Remote Help on macOS with Microsoft Intune

> **Tip**
>
> As a companion to this article, see our Intune Suite add-ons guide to review the step-by-step process to assign licenses, configure settings, and enable add-ons across your organization's devices. For a customized experience based on your environment, you can access the Intune Suite add-ons guide in the Microsoft 365 admin center.

Remote Help capabilities and requirements

The Remote Help app supports the following capabilities in general across the supported platforms.

> ⓘ Note
>
> To know more about specific capabilities and requirements based on the platform that you're using, go to:
>
> - Remote Help on Windows with Microsoft Intune
> - Remote Help on Android with Microsoft Intune
> - Remote Help on macOS with Microsoft Intune

- **Enable Remote Help for your tenant**: By default, Intune tenants aren't enabled for Remote Help. If you choose to turn on Remote Help, its use is enabled tenant-wide. Remote Help must be enabled before users can be authenticated through your tenant when using Remote Help.

- **Use Remote Help with unenrolled devices**: Remote Help is supported on enrolled devices that also need to be Entra registered devices. This setting is disabled by default. To allow Remote Help on devices that aren't enrolled in Intune, you must turn on this setting.

- **Requires Organization login**: To use Remote Help, both the helper and the sharer must sign in with a Microsoft Entra account from your organization. You can't use Remote Help to assist users who aren't members of your organization.

- **Compliance Warnings**: Before a helper connects to a user's device, the helper will see a non-compliance warning about that device if it's not compliant with its assigned policies.

- **Role-based access control**: Admins can set RBAC rules that determine the scope of a helper's access, such as:
  - The users who can help others and the range of actions they can do while providing help. For example, who can run elevated privileges while helping.
  - The users who can only view a device, and who can request full control of the session while assisting others.

- **Monitor active Remote Help sessions, and view details about past sessions**: In the Microsoft Intune admin center, you can view reports that include details about who helped who, on what device, and for how long. You can also find details about active sessions. An administrator can also reference audit log sessions created for Remote Help in Intune under **Tenant Administration** > **Audit Logs**.

  For unenrolled devices, auditing the Remote Help sessions is limited.

Prerequisites

General prerequisites that apply to Remote Help:

- Intune subscription
  - Remote Help add on license or an Intune Suite license for all IT support workers (helpers) and users (sharers) that are targeted to use Remote Help and benefit from the service.
  - Supported platforms and devices

For specific prerequisites based on the platform that you're using, go to:

- Remote Help on Windows with Microsoft Intune
- Remote Help on Android with Microsoft Intune
- Remote Help on macOS with Microsoft Intune

Limitations:

- You cannot establish a Remote Help session from one tenant to a different tenant.

- Remote Help might not be available in all markets or localizations.

- Remote Help is supported in Government Community Cloud (GCC) environments on the following platforms:

  - Windows 10/11

  - Windows 10/11 on ARM64 devices

  - Windows 365

  - Samsung and Zebra devices enrolled as Android Enterprise dedicated devices

  - macOS 13, 14, and 15

    Remote Help isn't supported on GCC High or DoD (U.S. Department of Defense) tenants. For more information, go to Microsoft Intune for US Government GCC High and DoD service description.

Supported platforms and devices

This feature applies to:

- Windows 10/11
- Windows 11 on ARM64 devices

- Windows 10 on ARM64 devices
- Windows 365
- Android Enterprise Dedicated (Samsung and Zebra devices)
- macOS 13, 14, and 15
- Azure Virtual Desktop

Data and privacy

Microsoft logs a small amount of session data to monitor the health of the Remote Help system. This data includes the following information:

- Start and end time of the session. This information is stored on Microsoft servers for 30 days.
- Who helped whom and on what device. This information is stored on Microsoft servers for 30 days.
- Errors arising from Remote Help itself, such as unexpected disconnections. This information is stored on the sharer's device in the event viewer.
- Features used inside the app such as view only and elevation. This information is stored on Microsoft servers for 30 days.

Remote Help logs session details to the Windows Event Logs on the device of both the helper and sharer. Microsoft can't access a session or view any actions or keystrokes that occur in the session.

The helper and sharer both see the following information about the other individual, taken from their organizational profiles:

- Their organization profile picture (if present)
- Company name
- Verified domain
- First and Last name
- Job title

Microsoft doesn't store any data about either the sharer or the helper for longer than 30 days.

Configure Remote Help for your tenant

To configure your tenant to support Remote Help, review and complete the following tasks. These tasks are important to configure for all Remote Help platforms that are supported.

Task 1: Enable Remote Help

1. Sign in to Microsoft Intune admin center and go to **Tenant administration** > **Remote Help**.

2. On the **Settings** tab:
   a. Set **Enable Remote Help** to **Enabled** to allow the use of remote help. By default, this setting is *Disabled*.
   b. Set **Allow Remote Help to unenrolled devices** to **Enabled** if you want to allow this option. By default, this setting is *Disabled*.
   c. Set **Disable chat** to **Yes** to remove the chat functionality in the Remote Help app. By default, chat is enabled and this setting is set to **No**.

3. Select **Save**.

> ⓘ Note
>
> When you purchase licenses or start a trial, it could take a while to become active (anywhere between 30 minutes to 8 hours). When you try to create a Remote Help session you may continue to see messages indicating that Remote Help isn't enabled for the tenant even if you enabled Remote Help in the tenant after activation.

Task 2: Configure permissions for Remote Help

Remote Help uses Intune role-based access controls (RBAC) to set the level of access a helper is allowed. Through RBAC, you determine which users can provide help and the level of help they can provide.

To protect the privacy of users who may be using the sharer device, helpers should use the minimum level of privilege required to remotely assist the device. Only request an Unattended session if you know that there's no user at the sharer device to accept the remote help session.

The following Intune RBAC permissions manage the use of the Remote Help app. Set each to *Yes* to grant the permission:

- Category: **Remote Help app**
- Permissions:
  - **Elevation** : Yes/No
  - **View screen** : Yes/No
  - **Take full control** : Yes/No
  - **Unattended control** : Yes/No

> ⓘ Note

If the **Take full control** permission is set to *Yes*, then by default, the user will have additional permission to **View screen**, even if the user's **View screen** permission is set to *No*. If the **Elevation** permission is set to *Yes*, then by default, the user will have additional permission to **View screen** and **Take full control**, even if the user's **View screen** and **Take full control** permission is set to *No*. If the **Unattended control** permission is set to *Yes*, then, by default, the user will have additional permission to **View screen**, **Take full control**, and **Elevation**, even if the user's **View screen**, **Take full control**, and **Elevation** permissions is set to *No*.

- Category: **Remote tasks**
- Permissions:
  - **Offer remote assistance** : Yes/No

By default, the built-in **Help Desk Operator** role sets all of these permissions to **Yes**. You can use the built-in role or create custom roles to grant only the remote tasks and Remote Help app permissions that you want different groups of users to have. For more information on using Intune RBAC, see Role-based access control.

Task 3: Assign user to roles

After creating the custom roles that you can use to provide different users with Remote Help permissions, proceed to assign users to those roles.

1. Sign into Microsoft Intune admin center and go to **Tenant administration** > **Roles** > and select a role that grants Remote Help app permissions.

2. Select **Assignments** > **Assign** to open **Add Role Assignment**.

3. On the *Basics* page, enter an **Assignment name** and optional **Assignment description**, and then choose **Next**.

4. On the **Admin Groups** page, select the group that contains the user you want to give the permissions to. Choose **Next**.

5. On the **Scope (Groups)** page, choose a group containing the users/devices that a member is allowed to manage. You also can choose all users or all devices. Choose **Next** to continue.

   > ⓘ **Important**
   >
   > If a sharer or a sharer's device isn't in the scope of a helper, that helper cannot provide assistance. When assisting an unenrolled device, the "All Devices" scope

> group will not include these devices. Instead, you should use the user scope group during the assignment process.

6. On the **Review + Create** page, when you're done, choose **Create**. The new assignment is displayed in the list of assignments.

Monitoring and reports

You can monitor the use of Remote Help from within the Microsoft Intune admin center. For unenrolled devices, reporting on Remote Help sessions is limited.

1. Sign into the Microsoft Intune admin center and go to **Tenant admin** > **Remote Help**.

2. On the Monitor tab, you can see a count of active sessions and historical data about past sessions.

3. On the Remote Help sessions tab, you can see the records of past sessions, including:

   - The helper (Provider ID) and sharer (Recipient ID) of each session.
   - The device that received assistance.
   - The start and end time of the Remote Assistance session.
   - The type of control session.

> ⓘ **Note**
>
> The Recipient ID and Recipient name display "--" for Android Enterprise Dedicated devices, as these devices do not have user affinity.

Try an interactive demo

The Remote Help interactive demo walks you through scenarios step-by-step with interactive annotations and navigation controls.

Next steps

Get support in Microsoft Intune admin center.

Remote Help on Windows with Microsoft Intune

Article • 04/30/2025

> ⓘ Note
>
> This capability is available as an Intune add-on. For more information, see Use Intune Suite add-on capabilities.

Remote Help is a cloud-based solution for secure help desk connections with role-based access controls. With the connection, your support staff can remotely connect to the user's device. During the session, the support staff can view the device's display and if permitted by the device user, take full control. Full control enables a helper to directly make configurations or take actions on the device.

In this article, users who provide help are referred to as *helpers*, and users that receive help are referred to as *sharers* as they share their session with the helper. Both helpers and sharers sign in to your organization to use the app. It's through your Microsoft Entra ID that the proper trusts are established for the Remote Help sessions.

Remote Help uses Intune role-based access controls (RBAC) to set the level of access a helper is allowed. Through RBAC, you determine which users can provide help and the level of help they can provide.

The Remote Help app is available from Microsoft to install on both devices enrolled with Intune and devices that aren't enrolled with Intune. The app can also be deployed through Intune to your managed devices.

Remote Help capabilities and requirements on Windows

The Remote Help app supports the following capabilities on Windows:

- **Conditional Access**: Administrators can now utilize Conditional Access capability when setting up policies and conditions for Remote Help. For example, multi-factor authentication, installing security updates, and locking access to Remote Help for a specific region or IP addresses. For more information on setting up Conditional Access, go to Setup Conditional Access for Remote Help

- **Compliance Warnings**: Before a helper can connect to a user's device, the helper sees a non-compliance warning about that device if it's not compliant with its assigned policies. This warning doesn't block access but provides transparency about the risk of using sensitive data like administrative credentials during the session.
  - Helpers who have access to device views in Intune will see a link in the warning to the device properties page in the Microsoft Intune admin center. The link allows a helper to learn more about why the device isn't compliant.
  - If the user's device isn't enrolled, the helper sees a prompt that the user's device is unenrolled.
- **Elevation of privilege** - When needed, a helper with the correct RBAC permissions can interact with the UAC prompt on the sharer's machine to enter credentials. For example, your Help Desk employees might enter their administrative credentials to complete an action on the sharer's device that requires administrative permissions.
- **Enhanced chat** - Remote Help includes enhanced chat that maintains a continuous thread of all messages. This chat supports special characters and other languages including Chinese and Arabic. For more information on languages supported, see Languages Supported.
- **Remotely start session** - The helper is able to launch Remote Help seamlessly on the helper and user's device from Intune by sending a notification to the user's device. The notification allows helpdesk and the sharer to be connected to a session quickly without exchanging session codes.

Prerequisites for Remote Help on Windows

General prerequisites for Remote Help are listed here.

The prerequisites for Remote Help on Windows are:

- Set up the Remote Help app for Windows. See Install and update Remote Help
- The helper and sharer can be on an enrolled or unenrolled device.

To remotely start a session:

- The helper can be on an enrolled or unenrolled device.
- The sharer's device needs to be enrolled device with Intune management extension.
  - Intune management extension is required for the remote launch feature and that is supported on Windows 10 and 11. Specifically for Windows 10 the OS builds need to be greater than or equal to version 19042 and have KB5018410 patch installed. The OS

version should be greater than or equal to 10.0.19042.2075 or 10.0.19043.2075 or 10.0.19044.2075. For more information on the Intune management extension, see Intune management extension

- Optional Windows updates for higher notification reliability:
  - Win 11: July 25, 2023—KB5028245 (OS Build 22000.2245) Preview - Microsoft Support
  - Win 10: August 22, 2023—KB5029331 (OS Build 19045.3393) Preview - Microsoft Support
- We do not recommend remotely starting a session to users on azure virtual desktops. For more information, see How to provide help on an AVD

Network considerations

Remote Help communicates over port 443 (https) and connects to the Remote Assistance Service at `https://remotehelp.microsoft.com` by using the Remote Desktop Protocol (RDP). The traffic is encrypted with TLS 1.2.

Both the helper and sharer must be able to reach these endpoints over port 443. Go to Network endpoints for Remote Help for a list of endpoints needed for Remote Help.

Remote Help modes available for Windows

Remote Help offers three different session modes for Windows:

- **Request screen sharing**: Request view of the remote screen. To minimize effect on end user privacy, this option is recommended unless full control is necessary.
- **Request full control**: Request full control of the remote device.
- **Elevation**: Allows helpers to enter UAC credentials when prompted on the sharer's device. Enabling elevation also allows the helper to view and control the sharer's device when the sharer grants the helper access.

Install and update Remote Help

Remote Help is available as download from Microsoft and must be installed on each device before that device can be used to participate in a Remote Help session. By default, Remote Help opts users into automatic updates and updates itself when an update is available.

Some users may choose to opt out of automatic updates. However, when a new version of Remote Help is necessary, the app prompts users to install that version upon opening. You can use the same process to download and install Remote Help to install an updated version. There's no need to uninstall the previous version before installing the updated version.

- Intune admins can download and deploy the app to enrolled devices. For more information about app deployments, see Install apps on Windows devices.
- Individual users who have permissions to install apps on their devices can also download and install Remote Help.

> ⓘ Note
>
> - On May 2022, existing users of Remote Help will see a recommended upgrade screen when they open the Remote Help app. Users will be able to continue using Remote Help without upgrading.
> - On May 23, 2022, existing users of Remote Help will see a mandatory upgrade screen when they open the Remote Help app. They will not be able to proceed until they upgrade to the latest version of Remote Help.
> - Remote Help will now require Microsoft Edge WebView2 Runtime. During the Remote Help installation process, if Microsoft Edge WebView2 Runtime is not installed on the device, then Remote Help installation will install it. When uninstalling Remote Help, Microsoft Edge WebView2 Runtime will not be uninstalled.

Download Remote Help

Download the latest version of Remote Help direct from Microsoft at aka.ms/downloadremotehelp .

The most recent version of Remote Help is **5.1.1998.0**

Deploy Remote Help as an Enterprise App Catalog app

The Enterprise App Catalog is a collection of prepackaged Win32 apps that have been designed and prepared by Microsoft to support Intune. An Enterprise App Catalog app is a Windows app that you can add via the Enterprise App Catalog in Intune. This app type leverages the Win32 platform and has support for customizable capabilities. Remote Help is available in the Enterprise App Catalog. To learn more, see Add an Enterprise App Catalog app to Microsoft Intune.

Deploy Remote Help as a Win32 app

To deploy Remote Help with Intune, you can add the app as a Windows Win32 app, and define a detection rule to identify devices that don't have the most current version of Remote Help installed. Before you can add Remote Help as a Win32 app, you must repackage *remotehelpinstaller.exe* as a *.intunewin* file, which is a Win32 app file you can deploy with Intune. For information on how to repackage a file as a Win32 app, see Prepare the Win32 app content for upload.

After you repackage Remote Help as a *.intunewin* file, use the procedures in Add a Win32 app with the following details to upload and deploy Remote Help. In the following, the repackaged remotehelpinstaller.exe file is named *remotehelp.intunewin*.

> ⓘ Important
>
> Make sure the file you dowloaded is renamed to **remotehelpinstaller.exe**.

1. On the App information page, select **Select app package file**, and locate the *remotehelp.intunewin* file you've previously prepared, and then select **OK**.

   Add a *Publisher* and then select **Next**. The other details on the App Information page are optional.

2. On the Program page, configure the following options:

   - For *Install command line*, specify **remotehelpinstaller.exe /quiet acceptTerms=1**
   - For *Uninstall command line*, specify **remotehelpinstaller.exe /uninstall /quiet acceptTerms=1**

   To opt out of automatic updates, specify enableAutoUpdates=0 as part of the install command **remotehelpinstaller.exe /quiet acceptTerms=1 enableAutoUpdates=0**

   > ⓘ Important
   >
   > The command line options *acceptTerms* and *enableAutoUpdates* are always case sensitive.

   You can leave the rest of the options at their default values and select **Next** to continue.

3. On the Requirements page, configure the following options to meet your environment, and then select **Next**:

   - *Operating system architecture*
   - *Minimum operating system*

4. On the Detection rules page, for *Rules format*, select **Manually configure detection rules**, and then select **Add** to open the *Detection rule* pane. Configure the following options:

   - For *Rule type*, select **File**
   - For *Path*, specify **C:\Program Files\Remote Help**
   - For *File or folder*, specify **RemoteHelp.exe**
   - For *Detection method*, select **String (version)**
   - For *Operator*, select **Greater than or equal to**
   - For *Value*, specify the Remote Help version that you're deploying. For example, **10.0.22467.1000**. See the following note for details on how to get the Remote Help version.
   - Leave *Associated with a 32-bit app on 64-bit clients* set to **No**

> ⓘ **Note**
>
> To get the version of the **RemoteHelp.exe**, install RemoteHelp manually to a machine and run the following Powershell command **(Get-Item "$env:ProgramFiles\Remote Help\RemoteHelp.exe").VersionInfo**. From the output make a note of the FileVersion and use it to specify the *Value* in the detection rule.

5. Proceed to the Assignments page, and then select an applicable device group or device groups that should install the Remote Help app. Remote Help is applicable when targeting group(s) of devices and not for User groups.

6. Complete creation of the Windows app to have Intune deploy and install Remote Help on applicable devices.

How to use Remote Help

The use of Remote Help depends on whether you're requesting help or providing help. In this section, both scenarios are covered.

Request help

To request help, you must reach out to your support staff to request assistance. You can reach out through a call, chat, email, and so on, and you'll be the sharer during the session.

As a sharer, when you've requested help and both you and the helper are ready to start:

1. The helper locates the device in the Microsoft Intune admin center and selects **New remote assistance session**. A notification is sent to the sharer's device.

2. The sharer must select **Launch Remote Help** to join the session. The sharer may need to sign in to authenticate. As an alternative, both the helper and sharer can manually launch the app and exchange a session code.

3. After opening the Remote Help app, the sharer has to wait for the helper to set up the session. The helper sees information about the sharer including the full name, job title, company, profile picture, and verified domain. As the sharer, your app displays similar information about the helper.

   At this time, the helper might request a session with full control of your device or choose only screen sharing. If they request full control, you can select the option to *Allow full control* or choose to *Decline the request*.

4. After the helper establishes the type of session (full control or screen sharing), the session is established, and the helper can then help in resolving any issues on the device.

   During assistance, helpers that have the *Elevation* permission can enter local admin permissions on your shared device. *Elevation* allows the helper to run executable programs or take similar actions when you lack sufficient permissions.

5. After the issues are resolved, or at any time during the session, both the sharer and helper can end the session. To end the session, select **Leave** in the upper right corner of the Remote Help app.

Request help on an unenrolled device

The device might not need to be enrolled to Intune if your administrator allows you to get help on unenrolled devices. If your device is unenrolled and you're trying to receive help, be prepared to enter a security code that you'll get from the individual who is assisting you. You'll enter the code in your Remote Help instance to establish a connection to the helper's instance of Remote Help.

As a sharer, when you've requested help and both you and the helper are ready to start:

1. Start the Remote Help app on the device and sign in to authenticate to your organization.

2. After signing into the app, get the security code from the individual assisting you and enter the code. Then select **Submit**.

3. After submitting the security code from the helper, the helper sees information about you including your full name, job title, company, profile picture, and verified domain. As the sharer, your app displays similar information about the helper.

4. At this time, the helper might request a session with full control of your device or choose only screen sharing. If they request full control, you can select the option to **Allow full control** or choose to **Decline the request**. Full control must be established before the help session starts.

5. After establishing the type of session (full control or screen sharing), the session is established, and the helper can now help resolving any issues on the device.

Provide help

As a helper, after receiving a request from a user who wants assistance by using the Remote Help app:

1. Launch a session on the remote device from within the Microsoft Intune admin center:

   a. Sign into Microsoft Intune admin center and go to **Devices** > **All devices** and select the device on which assistance is needed.

   b. From the remote actions bar across the top of the device view, select **New remote assistance session** and select **Remote Help**, and then **Continue**.

> **Note**
>
> If you are launching the session from the Intune, login with the same credentials to the Remote Help app for a successful connection.

2. A notification is sent to the sharer's device, and you'll see an update that the notification was successfully sent. Select **Launch Remote Help** to join the session.

   a. If the notification is sent but not received by the user, you can resend the notification by selecting **Retry**.

   b. If the sharer's device isn't online or not connected to the internet, an error message is displayed.

   c. If the device that you're trying to connect to is noncompliant, a warning banner is displayed.

3. When Remote Help opens, you must sign in to authenticate to your organization.

4. After the sharer opens the Remote Help app through the notification, as the helper you'll see information about the sharer, including their full name, job title, company, profile picture, and verified domain. The sharer sees similar information about you.

   At this time, you can request a session with full control of the sharer's device or choose only screen sharing. If you request full control, the sharer can choose to *Allow full control* or to *Decline the request*.

5. After establishing that the session uses a shared display or full control, Remote Help will display a **Compliance Warning* if the sharer's device fails to meet the conditions of its assigned compliance policies.

   During assistance, helpers that have the *Elevation* permission can enter local admin permissions on your shared device. *Elevation* allows the helper to run executable programs or take similar actions when you lack sufficient permissions.

6. After the issues are resolved, or at any time during the session, both the sharer and helper can end the session. To end the session, select **Leave** in the upper right corner of the Remote Help app. If a helper performs elevated actions on a user's device and the sharer ends the session, at the end of the session the sharer is automatically signed out.

Provide help on an unenrolled device

If the device that you're trying to help isn't enrolled in Intune, you must follow the process described in this section to give help:

1. Locate the Remote Help app on your device and manually start it. After the Remote Help app opens, you'll need to sign in to authenticate your organization.

2. After signing into the app, under **Give help** select **Get a security code**. Remote Help generates a security code that you'll share with the person who has requested assistance. The sharer enters the code in their instance of the Remote Help app to establish a connection to your Remote Help instance.

After the sharer enters the security code, as the helper you'll see information about the sharer, including their full name, job title, company, profile picture, and verified domain. The sharer sees similar information about you. At this time, you can request a session with full control of the sharer's device or choose only screen sharing. If you request full control, the sharer can choose to **Allow full control** or to **Decline the request**.

Now you'll be in a session with the user with the same experience and procedure outlined in the section Provide help.

> ⓘ **Important**
>
> During a Remote Help session, when a helper has the Elevation permission, the helper will not automatically be able to view the sharer's UAC prompt. Instead, for a non-admin

sharer, a button will appear on the helper's Remote Help toolbar that will allow them to request access to the UAC prompt on the sharer's device. Once requested and accepted, the helper will be able to perform elevated actions on the sharer's device. When the sharer ends the Remote Help session, they will be shown a dialog box that will warn them that if they continue, they will be logged off. If the helper ends the session, the sharer will not be logged off.

Provide help on an AVD

If you are trying to help an Azure Virtual Desktop (AVD) that could have multiple users on the device, you must follow the process described in this section to give help:

1. Locate the Remote Help app on your device and manually start it. After the Remote Help app opens, you need to sign in to authenticate your organization.

2. After signing into the app, under **Give help** select **Get a security code**. Remote Help generates a security code that you'll need to share with the person who has requested assistance active on the AVD. The sharer enters the code in their instance of the Remote Help app to establish a connection to your Remote Help instance.

ⓘ Note

If you initiate the Remote Help request from Intune, then the notification is delivered to all active users on the Azure Virtual Desktop.

ⓘ Note

The restart option is not available for helpdesk agents remotely helping AVD.

Log files

Remote Help logs data during installation and during Remote Help sessions, which can be of use when investigating issues with the app.

Installation of Remote Help - When Remote Help installs or uninstalls, the following two logs are created in the device users' Temp folder, for example, `C:\Users\<username>\AppData\Local\Temp`. The * in the log file name represents a date and time stamp of when the log was created.

- Remote_help_*_QuickAssist_Win10_x64.msi.log

- Remote_help_*.log

Operational logs - During use of Remote Help, operational details are logged in the Windows Event Viewer:

- Event Viewer > Application and Services > Microsoft > Windows > RemoteHelp

Installation details

Automatic firewall rule creation from the Remote Help installer has been removed. However, if needed, System administrators can create firewall rules.

Depending on the environment that Remote Help is utilized in, it may be necessary to create firewall rules to allow Remote Help through the Windows Firewall. In some situations when it's necessary, the following Remote Help executables should be allowed through the firewall:

- C:\Program Files\Remote help\RemoteHelp.exe
- C:\Program Files\Remote help\RHService.exe
- C:\Program Files\Remote help\RemoteHelpRDP.exe

Setup Conditional Access for Remote Help

This section outlines the steps for provisioning the Remote Help service on the tenant for Conditional Access.

1. Open PowerShell in admin mode.

   - It may be necessary to install Microsoft Graph PowerShell

2. Within PowerShell enter the following commands:

Installation

PowerShell

```powershell
Install-Module Microsoft.Graph -Scope CurrentUser
```

Sign in

Use the `Connect-MgGraph` command to sign in with the required scopes. You'll need to sign in with an admin account to consent to the required scopes.

PowerShell

```
Connect-MgGraph -Scopes "Application.ReadWrite.All"
```

Create the service principal

Create a Service Principal using the `Remote Assistance Service` AppId "1dee7b72-b80d-4e56-933d-8b6b04f9a3e2".

PowerShell

```
New-MgServicePrincipal -AppId "1dee7b72-b80d-4e56-933d-8b6b04f9a3e2"
```

Output

```
DisplayName                                     Id AppId
ServicePrincipalType
----                                         ------- -----------
---------------
RemoteAssistanceService                      3d5ff82b-a5f2-483a-xxxx-9514ed66f7c5
1dee7b72-b80d-4e56-933d-8b6b04f9a3e2
```

This output has been shortened for readability.

The ID corresponds to the app ID for the Remote Assistance Service.

The display name is **Remote Assistance Service**, which is the backend service for Remote Help.

Sign out

Use the `Disconnect-MgGraph` command to sign out.

PowerShell

```
Disconnect-MgGraph
```

Building a Conditional Access policy

After the Remote Help service principal is created, learn more on how to set up a conditional access policy.

To apply conditional access policies to Remote Help, follow these steps:

1. Navigate to the conditional access policy that you created.
2. Select **Target resources**
    a. Select **Resources (formerly cloud apps)** to specify what this policy applies to.
    b. Select **Exclude**.
    c. Select **Select resources**.
    d. Under **Select**, check the **RemoteAssistanceService** with the app ID of 1dee7b72-b80d-4e56-933d-8b6b04f9a3e2

Languages Supported

Remote Help is supported in the following languages:

- Arabic
- Bulgarian
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Latvian
- Lithuanian
- Norwegian
- Polish
- Portuguese
- Romanian
- Russian
- Serbian
- Slovak
- Slovenian

- Spanish
- Swedish
- Thai
- Turkish
- Ukrainian

Troubleshooting Remote Help on Windows for Edge WebView2

You might see an error code in a dialog box if you're having trouble installing and running Remote Help. The error might be related to Microsoft Edge WebView 2, which is required to use Remote Help. Here are some error codes you might see along with a short description of the problem.

Expand table

Error Code	General Problem
1001	Remote Help failed to initialize one of its internal components.
1002	Remote Help failed to load WebView2.
1003	Remote Help failed to install WebView2.

Solutions

1. Ensure that Microsoft Edge is installed properly and is up to date.

Remote Help uses the Microsoft Edge browser control. If your device has Microsoft Edge installed, then it's likely that Remote Help will run properly. If you have problems, the common troubleshooting tips here may help get Remote Help working. Learn more about Troubleshooting tips for installing and updating Microsoft Edge. After installing or updating Microsoft Edge, try opening Remote Help again. If Remote Help doesn't run or you get an error message that Microsoft Edge WebView2 isn't installed, go to the next step.

2. Install Microsoft Edge WebView 2

Microsoft Edge WebView2 is required to use Remote Help. If you get an error message that WebView2 isn't installed when you try to open Remote Help, then download and install Microsoft Edge WebView2 from the Microsoft website. After you've downloaded WebView2, try opening Remote Help again.

ⓘ Note

WebView2 should already be installed if your device is running Windows 11 or has Microsoft Edge.

Known Issues

For remotely starting a session on the user's device, notifications that are sent to the sharer's device when a helper launches a Remote Help session fails if the Microsoft Intune Management Service isn't running. After the user's device is restarted, there's a delay for the service to start. You can either manually wait for the service to start (30 minutes after restart), or manually start the service through services.msc. For newly enrolled devices, there's a 1 hour delay before the user's device begins receiving notifications when a helper initiates a session.

What's New for Remote Help

Updates for Remote Help are released periodically. When we update Remote Help, you can read about the changes here.

March 21, 2025

Version: 5.1.1998.0

- Added support for users on multi-session AVD
- Resolved accessibility bugs

June 25, 2024

Version 5.1.1419.0

- Resolve issue where the screen may be blank on first launch.

March 13, 2024

Version: 5.1.1214.0

- Changed the primary endpoint for Remote Help from https://remoteassistance.support.services.microsoft.com to https://remotehelp.microsoft.com.

> ⓘ **Note**
>
> This could cause a breaking change for some organizations that have not yet allowed remotehelp.microsoft.com through their firewall after 5/30/2024.

- Resolved various bugs including an issue with Conditional Access. If a tenant had a **Terms of Use** policy enabled for Office 365, Remote Help wouldn't know how to respond and would instead present an authentication error message to the user.
- Enabled a shortcut to open context menus with the keyboard shortcut 'Alt + Space'

October 25, 2023

Version: 5.0.1311.0

- Disabled the relaying of system audio from the Sharer device to the Helper device, which caused an echo when both users were using another app to communicate (such as Teams).
- Added the capability for Helpers that have elevation permissions to also be able to elevate apps on devices where the Sharer is an Administrator.

September 7, 2023

Version: 5.0.1045.0

With Remote Launch, the helper can launch Remote Help seamlessly on the helper and sharer's device from Intune by sending a notification to the sharer's device.

July 13, 2023

Version: 5.0.1045.0 This version of Remote Help provides support for ARM64 devices including the Microsoft Surface Pro X and Parallels Desktop on macOS.

June 20, 2023

Version: 4.2.1424.0 With Remote Help 4.2.1424.0, a new in-session connection mode feature provides users with a way to seamlessly switch between full control and view-only modes during a remote assistance session.

May 1, 2023

Version: 4.2.1270.0

This version includes a minor update that enables future functionality.

- Added support for slashes within the Remote Help URI (to enable future functionality)

March 27, 2023

Version: 4.2.1167.0 - Changes in this release:

This release addresses a bug in the Laser Pointer and includes some updates to prepare for future releases.

- Updated product name from **Remote help** to **Remote Help**
- Updated application description to better localize it for non-US locales
- Resolved a bug where the app would flash a white screen when launched in dark mode
- Fixed a bug with the Laser pointer color change

February 6, 2023

Version: 4.1.1.0 - Changes in this release:

A new Laser Pointer feature has been added to better assist a helper guide a sharer during a session. A helper can use the Laser Pointer in both Full Control and View Only sessions. Other updates include improvements to localization, and error handling.

Various bug fixes included in this release:

- Fixed an issue where in some cases a helper is unable to interact with elevated applications
- Resolved an accessibility issue where a helper was unable to use some keyboard navigation hotkeys
- Reliability fixes and improved logging for WebView2 integration

September 6, 2022

Version: 4.0.1.13 - Changes in this release:

Fixes were introduced to address an issue that prevented people from having multiple sessions open at the same time. The fixes also addressed an issue where the app was launching without focus, and prevented keyboard navigation and screen readers from working on launch.

For more information, go to Use Remote Help with Intune.

July 26, 2022

Version: 4.0.1.12 - Changes in this release:

Various fixes were introduced to address the 'Try again later' message that appears when not authenticated. The fixes also include an improved auto-update capability.

May 11, 2022

Version 4.0.1.7 - Webview 2 release

April 5, 2022

Version 4.0.0.0 - GA release

Next steps

Get support in Microsoft Intune admin center.

Remote Help on macOS with Microsoft Intune

Article • 03/03/2025

ⓘ Note

This capability is available as an Intune add-on. For more information, see Use Intune Suite add-on capabilities.

Overview

Remote Help is a cloud-based solution for secure help desk connections with role-based access controls. With this connection, your support staff can remotely connect to a user's device and view their display.

In this article, users who provide help are referred to as *helpers*, and users that receive help are referred to as *sharers* as they share their session with the helper.

Remote Help is available for macOS as both a native application, and as a Web App that runs within the user's web browser. The native application is required on the helpers machines to perform the *Full control* capability.

Expand table

Capability	Client requirement	Helper app
Screen sharing: View the remote screen.	✅ Web app ✅ Native app	✅ Web app
Full control: View the display and control the devices mouse and keyboard.	✅ Native app	✅ Web app

Remote Help capabilities

The Remote Help web app supports the following capabilities on macOS:

- **Use Remote Help with unenrolled devices**: Disabled by default, you can choose to allow help to devices that aren't enrolled with Intune.

- **Conditional Access**: Administrators can now utilize Conditional Access capability when setting up policies and conditions for Remote Help. For more information on setting up Conditional Access, see Setup Conditional Access for Remote Help.
- **Compliance Warnings**: Remote Help will show non-compliance warnings if the device the helper is connecting to isn't compliant with its assigned policies. This warning doesn't block access but provides transparency about the risk of using sensitive data like administrative credentials during the session.
- **Enrollment status**: If the user's device that the helper is trying to connect to isn't enrolled, the helper sees a prompt notifying them of the device status.
- **Chat functionality**: Remote Help includes enhanced chat that maintains a continuous thread of all messages. This chat supports special characters and other languages including Chinese and Arabic. For more information on languages supported, see Languages supported.

Remote Help Native macOS App

Most organizations install the Remote Help application for macOS on their users' devices. Remote Help for macOS provides the helper with view only and full control capabilities where they can control the Sharer's mouse and keyboard.

Remote Help Web App

In situations where the Sharer needs assistance but is unable to install the native application for macOS, the Sharer can use the Web App to share their screen to a helper. This web app provides view only capabilities to the helper, allowing them to guide the user through resolving issues.

Helpers always use the Remote Help Web App to provide support to a Sharer that is on macOS. For more details, go to Remote Help Web app.

Authentication and Permissions

Both helpers and sharers sign in to your organization using Microsoft Entra ID, which ensures that proper trusts are established for the Remote Help sessions.

Remote Help uses Intune role-based access controls (RBAC) to set the level of access a helper is allowed. Through RBAC, you determine which users can provide help and the level of help they can provide.

For details about configuring and setting up of permissions, go to Using Remote Help.

Remote Help requirements

General prerequisites for Remote Help are listed here Prerequisites for Remote Help.

Remote Help Native macOS App supported operating systems

- macOS 13 (Ventura)
- macOS 14 (Sonoma)
- macOS 15 (Sequoia)

Remote Help Web App supported browsers

- Safari (version 16.4.1+)
- Chrome (version 109+)
- Edge (version 109+)
- Firefox (version 122+)

> ⓘ **Note**
>
> Virtual Machines (VMs) are currently not supported.

Network considerations

Both the helper and sharer must be able to reach specific endpoints over port 443. For more information, see Network endpoints for Remote Help.

Requirements if Remote Help is restricted to enrolled devices

If your organization, restricts Remote Help to enrolled devices only there are two extra requirements:

1. **Single sign-on (SSO)**. For more information, see Use Enterprise SSO Plug-in on macOS.
2. **Open and sign in to Company Portal**. The user must open and sign into Company Portal for Remote Help to recognize the device is enrolled.

> ⓘ **Note**

Company Portal isn't supported on devices enrolled without user affinity. To use Remote Help on these devices, you need to change your tenant settings to set **Remote Help to unenrolled devices** to **Allowed**.

Native app operating system permissions

On macOS, applications that access and control the screen require permission. By default, users must accept these permissions. macOS allows some control capabilities for each type of privacy setting using *Privacy Preferences Policy Control*.

Expand table

Permission	MDM control capabilities
Accessibility	☑ Allow ☑ Allow Standard User To Set System Service macOS allows this property to be set on behalf of the user to *Allow*, reducing the number of steps required to use the Remote Help native client
Screen sharing	☑ Allow Standard User To Set System Service This permission by default requires administrator privileges to allow it. macOS doesn't allow this property to be set to *Allow* by MDM but you can enable the ability for standard users to accept this permission.

With settings catalog, we can streamline the end users experience for allowing these permissions.

Intune Admin Console

1. Sign in to the Intune admin center and go to **Devices** > **Manage devices** > **Configuration** > **Create** > **macOS** > **Settings catalog**

2. Enter a name and description for the profile. For example, "macOS Remote Help privacy permissions" and select **Next**

3. Select **Add settings** and in the settings picker, navigate to **Privacy** > **Privacy Preferences Policy Control** > **Services**
 a. Under **Accessibility** select:

   - **Authorization**
   - **Code Requirement**

   - **Identifer**
   - **Identifer type**
   - **Static code**

   a. Under **Screen Capture** select:

   - **Authorization**
   - **Code Requirement**
   - **Identifer**
   - **Identifer type**
   - **Static code**

4. Close the **Add settings** pane and select **+ Edit instance** under **Accessibility** and configure the following settings:

   Expand table

Name	Configuration
Authorization	Allow
Code Requirement	`identifier "com.microsoft.remotehelp" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = UBF8T346G9`
Identifier	com.microsoft.remotehelp
Identifier type	bundle ID
Static Code	False

5. Select **Save** and select **+ Edit instance** under **Screen Capture** and configure the following settings:

   Expand table

Name	Configuration
Authorization	Allow Standard User To Set System Service
Code Requirement	`identifier "com.microsoft.remotehelp" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = UBF8T346G9`
Identifier	com.microsoft.remotehelp

Name	Configuration
Identifier type	bundle ID
Static Code	False

6. Select **Next**, configure scope tags as required, assign the profile to groups as required, review settings and **Create** the policy.

Supported Languages

Remote Help is supported in the following languages:

- Arabic
- Bulgarian
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Latvian
- Lithuanian
- Norwegian
- Polish
- Portuguese
- Romanian
- Russian
- Serbian

- Slovak
- Slovenian
- Spanish
- Swedish
- Thai
- Turkish
- Ukrainian

Install and update Remote Help native app

The Remote Help native app is available to download from Microsoft and must be installed on the device you're trying to help before that device can be used to participate in a Remote Help session.

> **Tip**
>
> The native app is only required if full control of the helpers device is required, otherwise you can use Remote Help web app.

Download Remote Help

Download the latest version of Remote Help directly from Microsoft at https://aka.ms/downloadremotehelpmacos.

The most recent version of Remote Help is **1.0.2404171**.

Deploy Remote Help

For enrolled devices, you can streamline the user experience by installing Remote Help on behalf of your users.

For more information on installing Remote Help through Intune as a required install, see Add an unmanaged macOS PKG app to Microsoft Intune.

For more information on making Remote Help available in Company Portal for the user to install, see How to add macOS line-of-business apps to Microsoft Intune.

Update Remote Help

Remote Help receives the latest versions through the Microsoft AutoUpdate (MAU) application. Users can opt in for automatic updates to ensure Remote Help is up to date.

Request help

This section covers the steps for using the macOS native app to request Remote Help.

> **Tip**
>
> If you can't just want to share your screen and don't need the helper to be able to control your screen or you can't install the native app, you can use the web app. For more information on using the web app to request help, see Remote Help web app

To request help, you must reach out to your support staff to request assistance, and enter a code they provide to start the session.

When you as the sharer and your helper are ready to begin the session:

1. Open Remote Help app on the device **Finder** > **Applications** > **Microsoft Remote Help**.

2. When opening Remote Help for the first time, you must allow Remote Help access to control and share your screen. Click on each of the required permissions to open Settings and ensure the permission is allowed for Microsoft Remote Help.
   a. **Accessibility** (also available to set in **Settings** > **Privacy & Security** > **Accessibility**)
   b. **Screen and System Audio Recording** (also available to set in **Settings** > **Privacy & Security** > **Screen and System Audio Recording**)

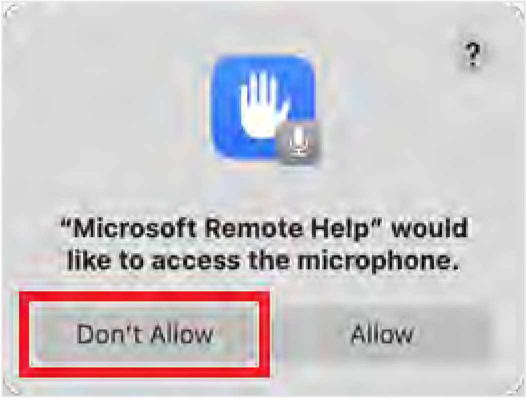
3. If prompted, sign in with your organization credentials to authenticate. to your organization.

4. Enter the 8-digit security code provided by the helper. After entering the code, select **Share screen** to continue.

5. When the session connection begins, a trust screen is displayed with the Helpers information including their full name, job title, company, profile picture, and verified domain. At this time, the helper requests a session with Full control of your device or View Only screen sharing. You can either choose to *Allow* or to *Decline* the request.

6. You might see a prompt to allow `remotehelp.microsoft.com` to use your microphone.

   - Select **Don't Allow** as this permission isn't needed for screen sharing.

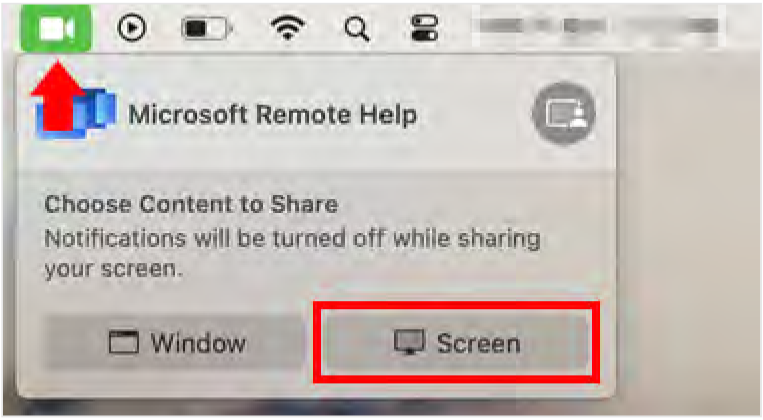


"Microsoft Remote Help" would like to access the microphone.

7. Select **Share screen** to continue. You might see a prompt to allow `remotehelp.microsoft.com` share your screen. Select **Allow** to continue.

8. macOS displays a dialogue menu in the top right corner as one of two options:

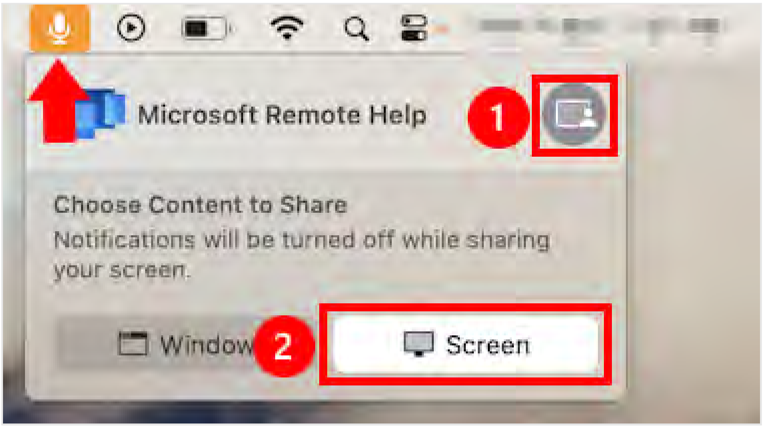
   - **Green camera icon**: Choose **Screen**, and then move your mouse to select the screen share.



Microsoft Remote Help

Choose Content to Share
Notifications will be turned off while sharing your screen.

   - **Yellow microphone icon** (if you selected to allow the microphone permission): Select the microphone icon, then to the right of the application name Microsoft Remote Help, select the grey icon, and then **Screen**. Move your cursor to the screen you want to share and select **Share this screen**.



Microsoft Remote Help

Choose Content to Share
Notifications will be turned off while sharing your screen.

9. After the session is established, the helper can then help in resolving any issues on the device.

> ⓘ Note
>
> If Remote Help wasn't installed by your administrator you can install Remote Help yourself by following the download instructions in the Install and update Remote Help section.

Provide help

As a helper, you can provide remote assistance to their device by providing them with a code to start the session. The web app can be started from any supported browser on Windows or macOS.

Intune admin center

1. Navigate to the device you're trying to help from the Microsoft Intune admin center:

   a. Sign into Microsoft Intune admin center and go to **Devices** > **All devices** and select the macOS device on which assistance is needed.

   b. From the remote action bar across the top of the device view, select **New remote assistance session** and select **Remote Help**, and then **Continue**.

2. Copy and share the 8-digit session code with the sharer that you're trying to help, before selecting **Start** to launch a new Remote Help session.

3. When Remote Help opens in a new tab for the first time, you must sign in to authenticate to your organization.

4. After the sharer navigates to the Remote Help session, as the helper you'll see information about the sharer, including their full name, job title, company, profile picture, and verified domain. The sharer sees similar information about you.

5. At this time, you can request a session with full control of the sharer's device or choose only screen sharing. The sharer can choose to *Allow* or to *Decline* the request.

ⓘ Note

- Remote Help displays a *Compliance Warning* if the sharer's device fails to meet the conditions of its assigned compliance policies.
- If the tenant is configured to allow Remote Help on unenrolled devices, you will receive a warning when connecting to unenrolled devices. This warning doesn't block access but provides transparency about the risk of using sensitive data like administrative credentials during the session.

Known Issues

- If the sharer exits from a Remote Help session early, the helper might not be notified for 60+ seconds.
- If using Edge, the sharer might have to sign in to Edge before starting a session or the device reports as Unenrolled.
- Verify that your browser is up to date.
- If you're screen sharing using another application like Teams or recording during the session, it might take longer for the session to connect.

Feedback

Was this page helpful? Yes No

Remote Help Web App

Article • 03/03/2025

Remote Help is a cloud-based solution for secure help desk connections with role-based access controls (RBAC). With this connection, your support staff can remotely connect to the user's device and view their display.

In this article, users who provide help are referred to as Helpers, and users that receive help are referred to as Sharers as they share their session with the helper.

In situations where the sharer needs assistance but is unable to install the Remote Help native application on a device, the sharer can share their screen to a helper by using the Remote Help Web App. This web app provides View Only capabilities to the helper, which allows them to guide the user through support scenarios.

Remote Help Web App Capabilities

The Remote Help web app supports the following capabilities:

Use Remote Help with unenrolled devices: Disabled by default, you can choose to allow help to devices that aren't enrolled with Intune.

- **Conditional Access**: Administrators can now utilize Conditional Access capability when setting up policies and conditions for Remote Help. For more information on setting up Conditional Access, go to Setup Conditional Access for Remote Help.
- **Compliance Warnings**: Before connecting to a user's device, a helper will see a non-compliance warning about that device if it's not compliant with its assigned policies. This warning doesn’t block access but provides transparency about the risk of using sensitive data like administrative credentials during the session.

If the user’s device that they're trying to connect to isn't enrolled, the helper sees a prompt that the user’s device is unenrolled.

- **Chat functionality**: Remote Help includes enhanced chat that maintains a continuous thread of all messages. This chat supports special characters and other languages including Chinese and Arabic. For more information on languages supported, see Languages Supported.

Authentication and Permissions

Both Helpers and Sharers sign in to your organization using Microsoft Entra ID, which ensures that proper trusts are established for the Remote Help sessions.

Remote Help uses Intune role-based access controls (RBAC) to set the level of access a helper is allowed. Through RBAC, tenant administrators determine which users can provide help and the level of help they can provide.

Prerequisites and supported devices for Remote Help Web App

In addition to the general prerequisites for Remote Help, there are other prerequisites for the Remote Help web app.

- SSO(Single-Sign-On)
- For sessions with unenrolled devices
  - Allow Remote Help to unenrolled devices (**Tenant Administration** > **Remote Help** > **Settings**)

Supported Devices

Device support is dependent on both the users operating system, and their web browser.

macOS Versions

- 11 Big Sur (Web app only)
- 12 Monterey
- 13 Ventura
- 14 Sonoma

Windows Versions

- Windows 10
- Windows 11

Linux Versions

Linux isn't officially supported by Remote Help. However, the Remote Help Web App might function for most Linux devices that are using a supported browser.

Browser Versions

- Safari (version 16.4.1+)
- Chrome (version 109+)
- Edge (version 109+)
- Firefox (version 122+)

Network Considerations

Both the helper and sharer must be able to reach Remote Help endpoints over port 443. Go to Network endpoints for Remote Help for a complete list of Remote Help endpoints.

Using Remote Help web app

The web app allows support teams to view the sharer's device during a connected session. The use of Remote Help depends on whether you're requesting help or providing help. In this section, we cover both scenarios.

Establishing a session

During a session there are two roles, a helper, and a sharer. The helper obtains the security code, and then provides it to the sharer. After the session is established, the helper can view the Sharer's screen.

Enrolled macOS device

1. The helper navigates to the device to connect to the Microsoft Intune admin center.

- Sign into Microsoft Intune admin center and go to **Devices** > **All devices** and select the macOS device on which assistance is needed.
- From the remote action bar across the top of the device view, select **New remote assistance session** and select **Remote Help**, and then **Continue**.

2. To invite a user to a session, provide the user with the security code.

- If the sharer is also using the web app:
- Copy and share the session link with the user (the link is limited to View Only) (For example: https://aka.ms/rh?passcode=4060r0gx). The link opens in the user's web browser. You can only request a screen sharing session of the device.
- If the sharer is using the macOS application:
- Share the 8-character security code with the user. You can request a screen sharing session (view only, and full control are supported)

3. After the sharer either selects the link or enters the code into Remote Help for macOS, they're joined to the session.

- If the user isn't already logged in to the application, they're prompted to do so.

4. At the start of the session, the trust screen is displayed which shows the other person’s full name, job title, company, profile picture, and verified domain.

- Helpers can see information about the sharer.
- Sharer can see information about the helper.

5. The sharer can choose to *Allow* or to *Decline* the request, after viewing the trust screen.

6. If the Sharers device isn't compliant with your organizations policies, Remote Help displays a *Compliance Warning* that encourages the helper to be cautious.

Unenrolled device

If the device that you're trying to help isn't enrolled in Intune, follow the process described in this section to provide help:

1. The helper navigates to https://aka.ms/rhh in their web browser, then signs in to authenticate with their organization.
2. After authenticating, a security code is displayed.
3. Copy and share the 8-digit security code with the person to be helped.
4. The sharer then navigates to https://aka.ms/rh and logs in with their organization’s credentials.

5. After the sharer enters the code, and both users accept the prompts, the sessions begin.

Remote Help displays a warning if the sharer’s device isn't enrolled in Microsoft Intune. This warning doesn’t block access but provides transparency about the risk of using sensitive data like administrative credentials during the session.

More details are outlined in Provide help.

Known Issues

- If the sharer exits from a Remote Help session early, the helper may not be notified for 60+ seconds.
- If using Edge, it may require the sharer to sign in to Edge before starting a session or the device is reported as Unenrolled.
- SSO must be enabled for the tenant to use the Remote Help web app.

Feedback

Was this page helpful? 👍 Yes 👎 No

Remote Help on Android with Microsoft Intune

Article • 05/27/2025

> ⓘ **Note**
>
> This capability is available as an Intune add-on. For more information, see **Use Intune Suite add-on capabilities**.

Remote Help is an add-on application that works with Intune and enables your support staff to remotely connect to a user's device. Remote Help is available on multiple platforms including Android.

During the session, you can view the device's display via screen sharing and if permitted by the device user, take full control to directly make configurations or take actions on the device. Remote Help for Android also supports unattended control allowing you to take full control of the device without needing user interaction on the device. This feature is helpful in cases like digital signage or for devices that need to be accessed during maintenance windows when no operators are on site.

In this article, we refer to the users who provide help as *helpers*, and devices that receive help as *sharers* as they share their session with the helper.

> ⓘ **Important**
>
> Remote Help on Android is now generally available.

Remote Help capabilities and requirements on Android

The Remote Help app supports the following capabilities on Android:

- **Screen sharing**: View of the remote screen. To minimize the effect on end user privacy, this option is recommended unless full control is necessary.
- **Full control**: Full control of the remote device.
- **Unattended control**: Full control of the device without the presence of an end user.
- **Compliance warnings**: Before a helper connects to a user's device, the helper sees a non-compliance warning about that device if it's not compliant with its assigned policies. This warning doesn't block access but provides transparency about the risk of using sensitive data like administrative credentials during the session.

Supported devices

- Samsung devices
- Zebra devices
  - Running MX version 8.3 or higher
  - Unattended control is only supported on MX version 9.3 and higher
- Devices must be either Samsung or Zebra and enrolled with Android Enterprise Dedicated.

Prerequisites for Remote Help on Android

For general prerequisites, go to Prerequisites for Remote Help

- Set up Managed Google Play for your tenant. For more information, go to Connect your Intune account to your Managed Google Play account
- Install the Intune app on devices with a version higher than 5.0.5541.0
- Devices must NOT have device configuration policy set to block Screen capture
- Zebra devices only: Set up Zebra OEMConfig for your tenant. For more details, go to Use OEMConfig on Android Enterprise devices in Microsoft Intune
- The helper must be licensed to use the Remote Help add-on. For more details on licensing, go to Use Intune Suite add-on capabilities - Microsoft Intune

- The helper must have appropriate RBAC permissions to use Remote Help on Android:
  - Category: Remote Help app
  - Permissions:
    - Take full control: Yes (required for control)
    - View screen: Yes (required for screen share)
    - Unattended control: Yes (required for unattended control)
    - If the user doesn't have the correct RBAC permissions for a particular mode, the corresponding options are disabled when attempting to start a Remote Help session.

Setting up Remote Help for Android

To set up Remote Help for Android, you need to complete the following steps:

1. Deploy the Remote Help app.
2. Grant permissions.
   - Configure camera permissions.
   - Configure permission setup for Zebra devices.
   - Configure permission setup for Samsung devices.

Deploy Remote Help app

1. Using Managed Google Play, add the Remote Help app from Microsoft ↗.
2. On devices that you want to use Remote Help, assign the app as **Required**. This setting allows automatic installation of the app on those devices.

Grant permissions

To protect user privacy on the device, both the Android OS and device OEMs require certain permissions to be granted to the Remote Help app.

> ⓘ Note
>
> We do not recommend installing or allow-list apps capable of screen recording or mirroring if you intend to use unattended mode in your organization for risky operations.

Camera

The Remote Help app requires Camera permissions.

> ⓘ Note
>
> Remote Help doesn't store camera input. These permissions are only used to initiate a remote help session between the device and the Intune service.

You can autogrant them through app configuration policy:

1. Go to **Apps** > **Configuration** > **Create** a new policy for **Managed devices**.
2. Create the policy for **Android Enterprise** with type **Fully managed, Dedicated, and Corporate-Owned Work Profile Only**. Target the policy to the **Remote Help** app that you approved earlier.
3. Under **Permissions**, add **CAMERA** permissions. Then, set the permission state to **Auto grant**.
4. Assign the profile to the devices on which you want to use Remote Help.

Permission setup for Zebra devices

On Zebra devices, permissions are granted through Zebra OEMConfig profiles.

For instructions on how to set up OEMConfig, go to Use OEMConfig on Android Enterprise devices in Microsoft Intune.

If you're planning to use Remote Help on a device running on Android 11, you need to enable another Zebra package as a system app. For more information on how to enable system apps, see Manage Android Enterprise system apps in Microsoft Intune

Expand table

Build	System app to be enabled
Any build of Android 11 that is earlier than 11-20-18.00-RG-U00	com.symbol.tool.stagenow
11-20-18.00-RG-U00 or 11-20-18.00-RG-U02	com.zebra.devicemanager
Any build of Android 11 that is later than 11-20-18.00-RG-U02	(None required)

Instructions for Zebra OEMConfig powered by MX

Zebra OEMConfig Powered by MX is a new version of the OEMConfig app released in May 2023.

> ⓘ Note
>
> On Android 11, the new OEM Config schema (Zebra OEMConfig powered by MX) doesn't work if the BSP version is HE_FULL_UPDATE_11-20-18.00-RG-U00-STD-HEL-04. You must upgrade to a later BSP to use the new OEMConfig app. For instructions on updating supported Zebra devices with Intune, see **Zebra LifeGuard Over-the-Air Integration with Microsoft Intune**

Use OEMConfig to deploy the following settings on devices that you want to use Remote Help with:

1. Under **Permission Access Configuration**, configure the following details:

Expand table

Key	Value
Package Name	com.microsoft.intune.remotehelp
Package Signing Certificate	`MIIGDjCCA/agAwIBAgIEUiDePDANBgkqhkiG9w0BAQsFADCByDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBD`

2.For the package you created, under **Package** > **Permissions**, add a new permission as follows:

Expand table

Key	Value
Name	System Alert Window
State	Grant

3.For the package created in step 1, under **Package** > **Allowed Services**, add two allowed services:

- One allowed service with a Service Identifier of `com.zebra.eventinjectionservice`
- Another allowed service with a Service Identifier of `com.zebra.remotedisplayservice`

Instructions for Legacy Zebra OEMConfig

When you use Legacy Zebra OEMConfig the OEMConfig profiles are applied as one-off actions, not persistent policy states. Make sure to deploy the OEMConfig profile after the Remote Help app is installed on the device. Also, if you uninstall and reinstall the Remote Help app on the device, you'll need to re-apply these OEMConfig settings after the app is reinstalled. You can create a new OEMConfig profile and assign it to the device, or edit the previously created OEMConfig profile.

Use OEMConfig to deploy the following settings on devices that you want to use Remote Help:

1. Under Permission Access Configuration, configure the following details:

Expand table

Name	Description
Permission Access Action	Grant
Grant Permission Access Action	System Alert Window
Grant Application Package	com.microsoft.intune.remotehelp
Grant Application Signature	`MIIGDjCCA/agAwIBAgIEUiDePDANBgkqhkiG9w0BAQsFADCByDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCB`

> **Note**
>
> The OEMConfig setting requires version MX 10.4 and higher on the device. For devices running a lower MX version, the display overlay permission must be manually granted to the Remote Help app. Contact Zebra for specific steps on your device or refer to the setup instructions for this permission on Samsung devices.

2.In a separate transaction step, under Service Access Configuration, create the following details:

Expand table

Name	Description
Service Binding Action	Allow
Allow Service Identifier	com.zebra.eventinjectionservice
Service Caller Action	Allow
Allow Service Identifier	com.zebra.eventinjectionservice
Allow Caller Package	com.microsoft.intune.remotehelp
Allow Caller Signature	`MIIGDjCCA/agAwIBAgIEUiDePDANBgkqhkiG9w0BAQsFADCByDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBD`

3.In another transaction step, under Service Access Configuration, configure the following details:

Expand table

Name	Description
Service Binding Action	Allow
Allow Service Identifier	com.zebra.remotedisplayservice

Name	Description
Service Caller Action	Allow
Allow Service Identifier	com.zebra.remotedisplayservice
Allow Caller Package	com.microsoft.intune.remotehelp
Allow Caller Signature	`MIIGDjCCA/agAwIBAgIEUiDePDANBgkqhkiG9w0BAQsFADCByDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBDb`

> ⓘ Note
>
> This setting enables unattended access and is only available on Zebra devices running MX 9.3 or later.

Permission setup for Samsung devices

In this section:

- Display overlay permission
- Knox KLMS Agent consent

Display overlay permission

> ⓘ Important
>
> If the device is in kiosk mode, designate the Settings app as a system app so it can launch. See Granting overlay permissions to Managed Home Screen for Android Enterprise dedicated devices for detailed instructions.

The Remote Help app needs the **Display over other apps** or **Appear on top** permission to display the Remote Help session UI. To grant this permission, create an OEMConfig profile that configures the permissions in the OEMConfig app.

Knox KLMS Agent consent

On some devices, the user also needs to agree to Samsung's KLMS Agent terms and conditions before the app can work.

1. After installing the Remote Help app, launch it. The prompt is automatically displayed when the app is launched.
2. Agree to the terms and conditions and tap **Confirm**.

> ⓘ Note
>
> - On Knox 2.8-3.7 (inclusive) this consent is revoked if the Remote Help app is uninstalled.
> - If the user agreed to KLMS license terms through another app, the prompt might not appear.

How to use Remote Help for Android

The use of Remote Help depends on whether you're requesting help or providing help. In this section, both scenarios are covered.

Request Help

To request help, you must reach out to your support staff to request assistance.

When you as the sharer and your helper are ready to begin the session:

1. On your device, you will see a prompt displaying a request to grant screen share or control of the device with the helpers information including their full name and company.

   a. If starting an attended screen sharing or full control session, you must select **Accept** to allow the session to begin. If you do not accept within 5 minutes, the session times out.

   b. If starting an unattended control session, the session will begin automatically after **30 seconds** if there is no response.

2. When the session is ongoing

   a. During an attended screen sharing or full control session, the device displays a floating **End Session** button. This button can be repositioned on the screen. Tap the button to end the session from your device.

   b. During an unattended control session, the screen of the device will blocked due to security and privacy reasons, and you will be notified if you interact with it. If you interact with the blocked screen, you will receive a notification that a helper is currently remotely accessing it for maintence. When the notification is shown, you and the helper will not be able to taken any action for 30 seconds when this screen will close. You will not be able to end the session from your device until the helper ends the session.

Provide Help

1. Navigate to the device you're trying to help from the Microsoft Intune admin center:

   a. Sign into Microsoft Intune admin center and go to **Devices** > **All devices** and select the Android device on which assistance is needed.

   b. From the remote action bar across the top of the device view, select **New remote assistance session** and select **Remote Help**, and then **Continue**.

   c. Select the session type from the options for which you have permission - screen sharing, full control, unattended control, and then **Launch Remote Help**.

2. On the device, the user sees a prompt displaying a request to grant screen share or control of the device.

   a. If starting an attended screen sharing or full control session, the user must select **Accept** to allow the session to begin. If the user doesn't accept within 5 minutes, the session times out.

   b. If starting an unattended control session, the session will begin automatically after **30 seconds** if there is no response from the user.

3. When the session is ongoing

   a. During an attended screen sharing or full control session, the sharer device displays a floating **End Session** button. This button can be repositioned on the screen. Tap the button to end the session from the sharer device.

   b. During an attended full control session, use the buttons on the menu bar, keyboard, or mouse input to interact with the sharer device. You can also long-press on the Power button in the menu bar to simulate a long press. For example, to open the power options menu on some devices.

   c. During an unattended control session, the screen of the device you are connected to will blocked due to security and privacy reasons, and the user will be notified if they interact with it. If the user interacts with the blocked screen, they will receive a notification letting them know that you are currently remotely accessing it for maintence. When the notification is shown, you and the end user will not be able to taken any action for 30 seconds when this screen will close.

> ⓘ Note
>
> During an unattended control session, even with the screen of the device you are connected blocked to the end user, we recommend to limit your activities to non-sensitive operations.

4. At the end of the session, select **Leave** to end the session from the admin console.

> ⓘ Note
>
> On Android 13 devices, the device unlock UI (the PIN entry pad, or the pattern dot grid) can't be displayed remotely. To unlock the device, you can still use keyboard input to enter a passcode. Android added this feature as a security measure to protect the end user from a passcode or unlock pattern being captured if the device is unlocked while screen sharing.

Next steps

Get support in Microsoft Intune admin center

Troubleshooting Remote Help on Android

Article • 03/03/2025

If a Remote Help session for Android is unable to connect, check for the following possibilities:

⛶ Expand table

Check if	Solution
The device has been newly enrolled with Intune.	On newly enrolled devices, push notifications (needed for Remote Help to receive session initiation requests) may take a while to start working. Wait for 15 minutes and try again later.
The Remote Help app isn't installed.	Install the app, see Remote Help on Android for details.
All the required permissions have been granted to the Remote Help app.	Review and ensure that all required permissions are granted. See Remote Help on Android for details.
The Intune app version isn't updated.	Update the Intune app to the latest version.
The device doesn't have access to Google services.	Remote Help requires access to Google Mobile Services to function, so make sure the device has Google services. You can do this by verifying that the Play Store is present on the device. See Android: Google Mobile Services.
There's no response from the end user.	Screen Sharing and Full Control Sessions time out automatically after 5 minutes if there's no response from Android: Google Mobile Services on the end user device. Make sure the user accepts the prompt to start the session.
The device manufacturer or OS/Zebra MX/Samsung Knox version isn't supported	Make sure the device is supported. See Remote Help on Android
(On Samsung devices only) The Knox license on the device is expired/invalid or has network issues.	Make sure that all Knox permissions have been granted, and that the device has an active Knox license; see License activation errors for troubleshooting Knox activation errors.
(On Samsung devices only) Other apps are actively using the Samsung Knox	Close or uninstall any other apps that may be using remote viewing/control capabilities on the device.

Check if	Solution
remote desktop APIs (you're using another remote assistance app on the device).	

Next steps

Get support in Microsoft Intune admin center

Feedback

Was this page helpful? 👍 Yes 👎 No

Remediations

Article • 05/28/2025

> ⓘ Important
>
> **Proactive Remediations** is renamed to **Remediations** and is now available from **Devices** > **Manage devices** > **Scripts and remediations**. All references to Proactive Remediations in this documentation are replaced with **Remediations**. However, the term Proactive Remediations might still appear in some blogs and other articles.

Remediations helps you fix common support issues before end-users notice issues.

In this article, you learn how to:

- ✓ Review prerequisites for Remediations
- ✓ Deploy a built-in script package
- ✓ Deploy a custom script package
- ✓ Run a Remediation script on-demand (preview)
- ✓ Client policy retrieval and client reporting
- ✓ Monitor the script packages
- ✓ Export script output
- ✓ Monitor remediation status for a device

About Remediations

Remediations are script packages that can detect and fix common support issues on a user's device before they even realize there's a problem. Remediations can help reduce support calls. You can create your own script package, or deploy one of the script packages we've written and used in our environment for reducing support tickets.

Each script package consists of a detection script, a remediation script, and metadata. Through Intune, you can deploy these script packages and see reports on their effectiveness.

Prerequisites

Whether enrolling devices via Intune or Configuration Manager, Remediation scripting has the following requirements:

- Devices must be Microsoft Entra joined or Microsoft Entra hybrid joined and meet one of the following conditions:

- Is managed by Intune and runs an Enterprise, Professional, or Education edition of Windows 10 or later.
- A co-managed device running Windows 10, version 1903 or later. Co-managed devices on preceding versions of Windows 10 will need the Client apps workload pointed to Intune (only applicable up to version 1607).

Licensing

Remediations requires users of the devices to have one of the following licenses:

- Windows 10/11 Enterprise E3 or E5 (included in Microsoft 365 F3, E3, or E5)
- Windows 10/11 Education A3 or A5 (included in Microsoft 365 A3 or A5)
- Windows 10/11 Virtual Desktop Access (VDA) per user

Permissions

- For Remediations, the user needs permissions appropriate to their role under the **Device configurations** category. For more information, see Role-based access control for Microsoft Intune.
- An Intune Service Administrator is required to confirm licensing requirements before using Remediations for the first time.

Script requirements

- You can have up to 200 script packages.
- A script package can contain a detection script only or both a detection script and a remediation script.
  - A remediation script only runs if the detection script uses exit code `exit 1`, meaning the issue was detected.
- Ensure the scripts are encoded in UTF-8.
  - If the option **Enforce script signature check** is enabled in the Settings page of creating a script package, then make sure that the scripts are encoded in UTF-8 not UTF-8 BOM.
- The maximum allowed output size limit is 2048 characters.
- If the option **Enforce script signature check** is enabled in the Settings page of creating a script package, the script runs using the device's PowerShell execution policy. The default execution policy for Windows client computers is **Restricted**. The default execution for Windows Server devices is **RemoteSigned**. For more information, see PowerShell execution policies.

  - Scripts built into Remediations are signed and the certificate is added to the **Trusted Publishers** certificate store of the device.
  - When using third-party scripts that are signed, make sure the certificate is in the **Trusted Publishers** certificate store. As with any certificate, the certificate authority must be trusted by the device.
  - Scripts without **Enforce script signature check** use the **Bypass** execution policy.
- Don't put reboot commands in detection or remediations scripts.
- Do not include any type of sensitive information in scripts (such as passwords)
- Do not include Personally Identifiable Information (PII) in scripts
- Do not use scripts to collect PII from devices
- Always follow privacy best practices

Deploy built-in script packages

There are built-in script packages you can use to get started with Remediations. The **Microsoft Intune Management Extension** service gets the scripts from Intune and runs them. The following built-in script packages just need to be assigned:

- **Update stale Group Policies** – Stale Group Policies can lead to helpdesk tickets related to connectivity and internal resource access.
- **Restart Office Click-to-run service** – When the Click-to-run service is stopped, Office apps fail to start leading to helpdesk calls.

To assign the script package:

1. From the **Devices** > **Manage devices** > **Scripts and remediations** node, select one of the built-in script packages.
2. Select **Properties**, then next the **Assignments** heading, select **Edit**.
3. Choose the groups you want to **Assign to** and any **Excluded groups** for the script package.
4. To change the **Scope tags**, select **Edit** then **Select scope tags**.
5. If you would like to change the schedule, select the ellipses and choose **Edit** to specify your settings then **Apply** to save them.
6. When you're done, select **Review + save**.

Create and deploy custom script packages

The **Microsoft Intune Management Extension** service gets the scripts from Intune and runs them. The scripts are rerun every 24 hours. You can copy the provided scripts and deploy them, or you can create your own script packages. To deploy script packages, follow the instructions in the next section.

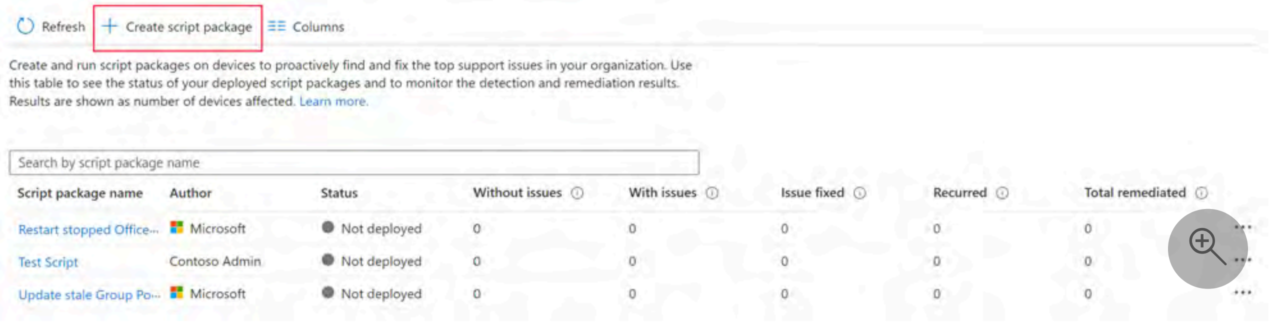
Copy the provided detection and remediation scripts

1. Copy the scripts from the PowerShell scripts article.
   - Script files whose names start with `Detect` are detection scripts. Remediation scripts start with `Remediate`.
   - For a description of the scripts, see the Script descriptions.
2. Save each script using the provided name. The name is also in the comments at the top of each script. Ensure the saved scripts are encoded in UTF-8.
   - You can use a different script name, but it won't match the name listed in the Script descriptions.

Deploy the script packages

Remediation scripts need to be encoded in UTF-8. Uploading these scripts rather than editing them directly in your browser helps ensure that the script encoding is correct so your devices can execute them.

1. In the Intune admin center, go to **Devices** > **Manage devices** > **Scripts and remediations**.
2. Choose **Create script package** button to create a script package.



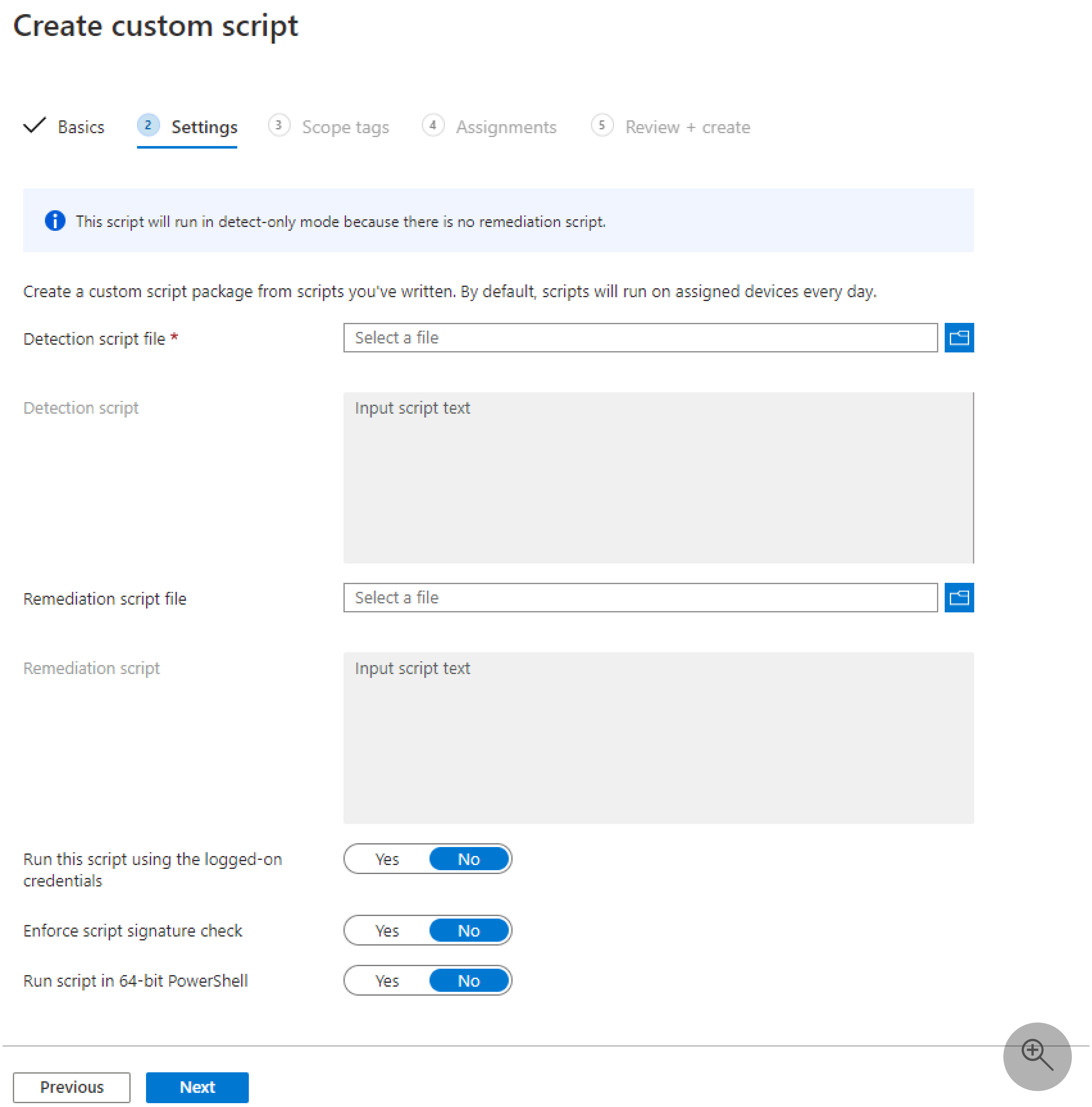
Create and run script packages on devices to proactively find and fix the top support issues in your organization. Use this table to see the status of your deployed script packages and to monitor the detection and remediation results. Results are shown as number of devices affected. Learn more.

Script package name	Author	Status	Without issues	With issues	Issue fixed	Recurred	Total remediated
Restart stopped Office...	Microsoft	● Not deployed	0	0	0	0	0
Test Script	Contoso Admin	● Not deployed	0	0	0	0	0
Update stale Group Po...	Microsoft	● Not deployed	0	0	0	0	0

3. In the **Basics** step, give the script package a **Name** and optionally, a **Description**. The **Publisher** field can be edited, but defaults to your name. **Version** can't be edited.
4. On the **Settings** step, upload both the **Detection script file** and the **Remediation script file** by doing the following steps:
   a. Select the folder icon.
   b. Browse to the `.ps1` file.
   c. Choose the file and select **Open** to upload it.

   The detection script must use exit code `exit 1` if the target issue is detected. If there's any other exit code, the remediation script won't run. Including an empty output, since it results in an *issue is not found* state. Review the Sample detection script for an example of exit code usage.

You need the corresponding detection and remediation script to be in the same package. For example, the `Detect_Expired_User_Certificates.ps1` detection script corresponds with the `Remediate_Expired_User_Certificates.ps1` remediation script.



This script will run in detect-only mode because there is no remediation script.

Create a custom script package from scripts you've written. By default, scripts will run on assigned devices every day.

Detection script file *: Select a file

Detection script: Input script text

Remediation script file: Select a file

Remediation script: Input script text

Run this script using the logged-on credentials: Yes [✓ No]

Enforce script signature check: Yes [✓ No]

Run script in 64-bit PowerShell: Yes [✓ No]

5. Finish the options on the **Settings** page with the following recommended configurations:

    - **Run this script using the logged-on credentials**: This setting is dependent on the script. For more information, see the Script descriptions.
    - **Enforce script signature check**: No
    - **Run script in 64-bit PowerShell**: No

    For information about enforcing script signature checks, see Script requirements.

6. Select **Next** then assign any **Scope tags** you need.

7. In the **Assignments** step, select the device groups to which you want to deploy the script package. When you're ready to deploy the packages to your users or devices, you can

also use filters. For more information, see Create filters in Microsoft Intune.

> ⓘ **Note**
>
> Don't mix user and device groups across include and exclude assignments.

8. Complete the **Review + Create** step for your deployment.

Run a remediation script on-demand (preview)

You can use the **Run remediation** device action to run a remediation script on-demand to a single Windows device.

Prerequisites for running a remediation script on-demand

- Remediations must already be configured before a remediation script can be used on-demand.
- The built-in or custom script packages must be available for users to run a remediation on-demand, however they don't need to be assigned to a user or device. You can use **Scope tags** to limit which remediation script packages a user can see.
- Users must be Global Admins, Intune Admins, or have a role with the **Run remediation** permission (available under **Remote tasks**). During the public preview, the user must also have Organization: Read.
- Devices are online and able to communicate with Intune and Windows Push Notification Service (WNS) during the remote action.
- The Intune Management Extension must be installed on devices. The installation is done automatically when a Win32 app, PowerShell script, or Remediation is assigned to a user or device.

How to run a Remediation script on-demand

1. Sign in to the Microsoft Intune admin center .
2. Navigate to **Devices** > **By platform** > **Windows** > select a supported device.
3. On the device's **Overview** page, select **...** > **Run remediation (preview).**
4. In the **Run remediation (preview)** pane, select the **Script package** you want to run from the list. Select **View details** to see properties of the script package like detection and remediation script contents, description, and configured settings.

5. To run the remediation on-demand, select **Run remediation**.

> ⓘ Note
>
> Only a single **Run remediation** device action can be issued at a time for the same device. If you run multiple **Run remediation** device actions in a short period of time to a device, they may overwrite each other.

> ⓘ Note
>
> The device might not receive the **Run remediation** device action if it is not online or able to successfully communicate with Intune or Windows Push Notification Service (WNS) when the device action is sent.

Client policy retrieval and client reporting

The client retrieves policy for Remediation scripts at the following times:

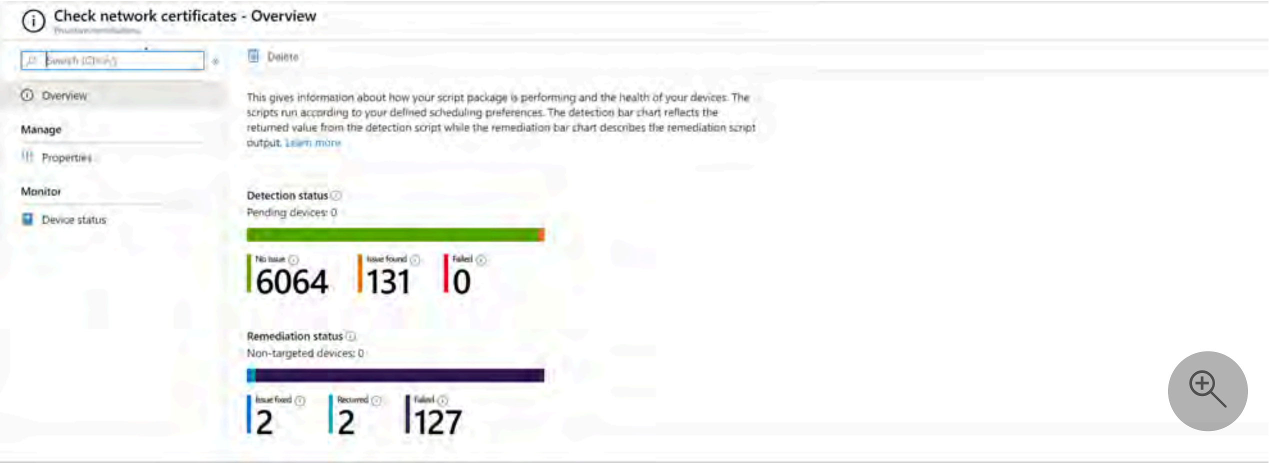
- After a restart of the device or Intune management extension service
- After a user signs into the client
- Once every 8 hours
    - The 8 hour script retrieval schedule is fixed based on when the Intune management extension service starts. User sign ins do not alter the schedule.

The client reports Remediation information at the following times:

- When a script is set to run once, the results are reported after the script runs.
- Recurring scripts follow a seven day reporting cycle:
    - Within the first six days, the client reports only if a change occurs. The first time the script runs would be considered a change.
    - Every seven days the client sends a report even if there wasn't a change.

Monitor your script packages

1. In the Intune admin center, go to **Devices** > **Manage devices** > **Scripts and remediations**, you can see an overview of your detection and remediation status.



Check network certificates - Overview

Delete

This gives information about how your script package is performing and the health of your devices. The scripts run according to your defined scheduling preferences. The detection bar chart reflects the returned value from the detection script while the remediation bar chart describes the remediation script output. Learn more

Detection status

Pending devices: 0

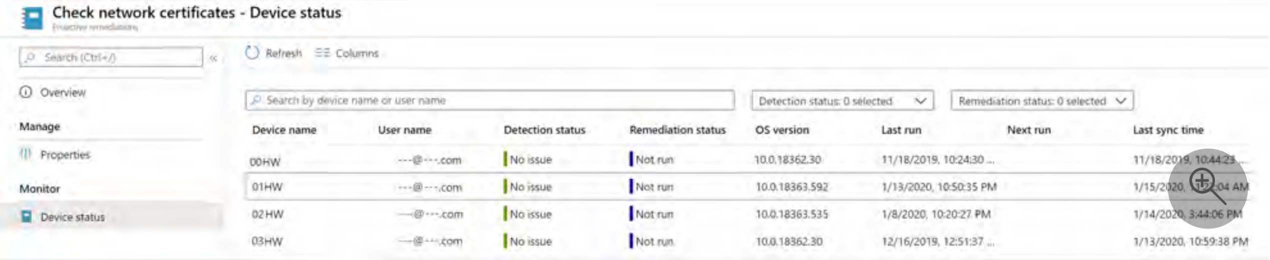
No issue 6064 · Issue found 131 · Failed 0

Remediation status

Non-targeted devices: 0

Issue fixed 2 · Recurred 2 · Failed 127

2. Select **Device status** to get status details for each device in your deployment.



Check network certificates - Device status

Search by device name or user name

Detection status: 0 selected

Remediation status: 0 selected

Device name	User name	Detection status	Remediation status	OS version	Last run	Next run	Last sync time
00HW	---@---.com	No issue	Not run	10.0.18362.30	11/18/2019, 10:24:30 ...		11/18/2019, 10:44:23 ...
01HW	---@---.com	No issue	Not run	10.0.18363.592	1/13/2020, 10:50:35 PM		1/15/2020, [illegible]:04 AM
02 HW	---@---.com	No issue	Not run	10.0.18363.535	1/8/2020, 10:20:27 PM		1/14/2020, 3:44:06 PM
03HW	---@---.com	No issue	Not run	10.0.18362.30	12/16/2019, 12:51:37 ...		1/13/2020, 10:59:38 PM

Export script output

To help you easily analyze returned outputs, use the **Export** option to save the output as a `.csv` file. Exporting the output to a `.csv` file allows you to analyze the returned outputs when Remediations run on devices with issues. Exporting also allows you to share the results with others for more analysis.

Monitor remediation status for a device

You can view the status of Remediations that are assigned or run on-demand to a device.

1. Sign in to the Microsoft Intune admin center.
2. Navigate to **Devices** > **By platform** > **Windows** > select a supported device.
3. Select **Remediations** in the **Monitor** section.

Known Issues

When applying filters such as "Author" or "Status," or using the **Export** option on the **Remediations** page of **Scripts and remediations**, only the currently loaded script packages are included. To include all scripts, scroll until the full list is loaded.

Next steps

- Get the PowerShell scripts for Remediations.
- Learn more about PowerShell script security.

PowerShell scripts for Remediations

Article • 03/03/2025

This article includes sample scripts that customers can implement or use as templates to learn how to create their own. Use the information provided here to create script packages for Remediations.

Script descriptions

This table shows the script names, descriptions, detections, remediations, and configurable items. Script files whose names start with `Detect` are detection scripts. Remediation scripts start with `Remediate`. These scripts can be copied from the next section in this article.

Expand table

Script name	Description

Check network certificates
`Detect_Expired_Issuer_Certificates.ps1`
`Remediate_Expired_Issuer_Certificates.ps1`
	Detects certificates issued by a CA in either the Machine's or User's personal store that are expired, or near expiry.
	Specify the CA by changing the value for `$strMatch` in the detection script. Specify 0 for `$expiringDays` to find expired certificates, or specify another number of days to find certificates near expiry.
	
	Remediates by raising a toast notification to the user.
	Specify the `$Title` and `$msgText` values with the message title and text you want users to see.
	
	Notifies users of expired certificates that might need to be renewed.
	
	Run the script using the logged-on credentials: Yes

Clear stale certificates
`Detect_Expired_User_Certificates.ps1`
`Remediate_Expired_User_Certificates.ps1`
	Detects expired certificates issued by a CA in the current user's personal store.
	Specify the CA by changing the value for `$certCN` in the detection script.
	
	Remediates by deleting expired certificates issued by a CA from the current user's personal store.

Script name	Description
	Specify the CA by changing the value for `$certCN` in the remediation script. Finds and deletes expired certificates issued by a CA from the current user's personal store. **Run the script using the logged-on credentials**: Yes

Update stale Group Policies (built-in)
`Detect_stale_Group_Policies.ps1`
`Remediate_stale_GroupPolicies.ps1`
	Detects if last Group Policy refresh is greater than `7 days` ago.
	This script package is included with Remediations, but a copy is provided if you want to change the threshold. Customize the seven day threshold by changing the value for `$numDays` in the detection script.
	
	Remediates by running `gpupdate /target:computer /force` and `gpupdate /target:user /force`
	
	Can help reduce network connectivity-related support calls when certificates and configurations are delivered via Group Policy.
	
	Run the script using the logged-on credentials: Yes

Check network certificates script package

This script package detects certificates issued by a CA in either the Machine's or User's personal store that are expired, or near expiry. The script remediates by raising a toast notification to the user.

Detect_Expired_Issuer_Certificates.ps1

PowerShell

```
#=============================================================================
==================================================
#
# Script Name:     Detect_Expired_Issuer_Certificates.ps1
# Description:     Detect expired certificates issued by "CN=<your CA here>"
in either Machine
#                  or User certificate store
# Notes:           Change the value of the variable $strMatch from "CN=<your
```

```
CA here>" to "CN=..."
#                   For testing purposes the value of the variable
$expiringDays can be changed to a positive integer
#                   Don't change the $results variable
#
#============================================================================
==================================================

# Define Variables
$results = @()
$expiringDays = 0
$strMatch = "CN=<your CA here>"

try
{
    $results = @(Get-ChildItem -Path Cert:\LocalMachine\My -Recurse -
ExpiringInDays $expiringDays | where {$_.Issuer -match $strMatch})
    $results += @(Get-ChildItem -Path Cert:\CurrentUser\My -Recurse -
ExpiringInDays $expiringDays | where {$_.Issuer -match $strMatch})
    if (($results -ne $null)){
        #Below necessary for Intune as of 10/2019 will only remediate Exit
Code 1
        Write-Host "Match"
        Return $results.count
        exit 1
    }
    else{
        #No matching certificates, do not remediate
        Write-Host "No_Match"
        exit 0
    }
}
catch{
    $errMsg = $_.Exception.Message
    Write-Error $errMsg
    exit 1
}
```

Remediate_Expired_Issuer_Certificates.ps1

PowerShell

```
#============================================================================
==================================================
#
# Script Name:     Remediate_Expired_Issuer_Certificates.ps1
# Description:     Raise a Toast Notification if expired certificates issued
by "CN=..."
#                   to user or machine on the machine where detection script
found them. No remediation action besides
#                   the Toast is taken.
# Notes:           Change the values of the variables $Title and $msgText
```

```
#
#===========================================================================
==================================================

## Raise toast to have user contact whoever is specified in the $msgText

# Define Variables
$delExpCert = 0
$Title = "Title"
$msgText = "message"

# Main script
[Windows.UI.Notifications.ToastNotificationManager,
Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications,
ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument,
ContentType = WindowsRuntime] | Out-Null

$APP_ID = '{1AC14E77-02E7-4E5D-B744-
2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe'

$template = @"
<toast>
    <visual>
        <binding template="ToastText02">
            <text id="1">$Title</text>
            <text id="2">$msgText</text>
        </binding>
    </visual>
</toast>
"@

$xml = New-Object Windows.Data.Xml.Dom.XmlDocument
$xml.LoadXml($template)
$toast = New-Object Windows.UI.Notifications.ToastNotification $xml
[Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier($AP
P_ID).Show($toast)
```

Clear stale certificates script package

This script package detects expired certificates issued by a CA in the current user's personal store. The script remediates by deleting expired certificates issued by a CA from the current user's personal store.

Detect_Expired_User_Certificates.ps1

PowerShell

```powershell
#============================================================================
==================================================
#
# Script Name:     Detect_Expired_User_Certificates.ps1
# Description:     Detect expired certificates issued by "CN=<your CA here>"
to User
# Notes:           Change the value of the variable $certCN from "CN=<your
CA here>" to "CN=...".
#                  Don't change $results
#
#============================================================================
==================================================

# Define Variables
$results = 0
$certCN = "CN=<your CA here>"

try
{
    $results = Get-ChildItem -Path Cert:\CurrentUser\My -Recurse -
ExpiringInDays 0 | where {$_.Issuer -eq($certCN)}
    if (($results -ne $null)){
        #Below necessary for Intune as of 10/2019 will only remediate Exit
Code 1
        Write-Host "Match"
        Return $results.count
        exit 1
    }
    else{
        Write-Host "No_Match"
        exit 0
    }
}
catch{
    $errMsg = $_.Exception.Message
    Write-Error $errMsg
    exit 1
}
```

Remediate_Expired_User_Certificates.ps1

PowerShell

```powershell
#============================================================================
==================================================
#
# Script Name:     Remediate_Expired_User_Certificates.ps1
# Description:     Remove expired certificates issued by "CN=<your CA here>"
to User
# Notes:           Change the value of the variable $certCN from "CN=<your
CA here>" to "CN=..."
```

```
#
#=============================================================================
==================================================

# Define Variables
$certCN = "CN=<your CA here>"

try
{
    Get-ChildItem -Path cert:\CurrentUser -Recurse -ExpiringInDays 0 | where
{$_.Issuer -eq($certCN)} | Remove-Item
    exit 0
}
catch{
    $errMsg = $_.Exception.Message
    Write-Error $errMsg
    exit 1
}
```

Update stale Group Policies script package

This script package is included with Remediations, but a copy is provided if you want to change the threshold.

This script package detects if last Group Policy refresh is greater than `7 days` ago. The script remediates by running `gpupdate /target:computer /force` and `gpupdate /target:user /force`.

Detect_stale_Group_Policies.ps1

PowerShell

```
#=============================================================================
==================================================
#
# Script Name:     Detect_stale_Group_Policies.ps1
# Description:     Detect if Group Policy has been updated within number of
days
# Notes:           Remediate if "Match", $lastGPUpdateDays default value of
7, change as appropriate
#
#=============================================================================
==================================================

# Define Variables

try {
    $gpResult = [datetime]::FromFileTime(([Int64] ((Get-ItemProperty -Path
"Registry::HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-
000000000000}").startTimeHi) -shl 32) -bor ((Get-ItemProperty -Path
"Registry::HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-
000000000000}").startTimeLo))
    $lastGPUpdateDate = Get-Date ($gpResult[0])
    [int]$lastGPUpdateDays = (New-TimeSpan -Start $lastGPUpdateDate -End
(Get-Date)).Days

    if ($lastGPUpdateDays -gt 7){
        #Exit 1 for Intune. We want it to be within the last 7 days "Match"
to remediate in SCCM
        Write-Host "Match"
        exit 1
    }
    else {
        #Exit 0 for Intune and "No_Match" for SCCM, only remediate "Match"
        Write-Host "No_Match"
        exit 0
    }
}
catch {
    $errMsg = $_.Exception.Message
    return $errMsg
    exit 1
}
```

Remediate_stale_GroupPolicies.ps1

PowerShell

```
#============================================================================
==================================================
#
# Script Name:     Remediate_stale_GroupPolicies.ps1
# Description:     This script triggers Group Policy update
# Notes:           No variable substitution needed
#
#============================================================================
==================================================

try {
    $compGPUpd = gpupdate /force
    $gpResult = [datetime]::FromFileTime(([Int64] ((Get-ItemProperty -Path
"Registry::HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-
000000000000}").startTimeHi) -shl 32) -bor ((Get-ItemProperty -Path
"Registry::HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-
000000000000}").startTimeLo))
    $lastGPUpdateDate = Get-Date ($gpResult[0])
    [int]$lastGPUpdateDays = (New-TimeSpan -Start $lastGPUpdateDate -End
(Get-Date)).Days

    if ($lastGPUpdateDays -eq 0){
        Write-Host "gpupdate completed successfully"
        exit 0
    }
    else{
        Write-Host "gpupdate failed"
        }
}
catch{
    $errMsg = $_.Exception.Message
    return $errMsg
    exit 1
}
```

Next steps

For information about deploying script packages, see Remediations.

Feedback

Was this page helpful? Yes No

How to use Microsoft Intune documentation

Article • 09/27/2022

This article provides resources and tips for using the Microsoft Intune product family documentation library. It applies to Configuration Manager, Microsoft Intune, Endpoint analytics, and Autopilot, and covers the following areas:

- How to search
- Submitting doc bugs, enhancements, questions, and new ideas
- How to get notified of changes
- How to contribute to documentation on Microsoft Learn

For general help and support, see:

- Find help for Configuration Manager
- Get support in Microsoft Intune

> **Tip**
>
> Also visit the **Documentation** node in the **Community** workspace of the Configuration Manager console. This node includes up-to-date information about Configuration Manager documentation and support articles. For more information, see Using the Configuration Manager console.

Information in this article also applies to the Configuration Manager PowerShell documentation in the sccm-docs-powershell-ref repository.

Search

Use the following search tips to help you find the information that you need:

- When using your preferred search engine to locate content, include a keyword along with your search keywords. For example, `ConfigMgr` for Configuration Manager and `Intune` for Intune.
    - Look for results from `learn.microsoft.com/mem`. Results from `learn.microsoft.com/previous-versions`, `technet.microsoft.com`, or `msdn.microsoft.com` are for older product versions.

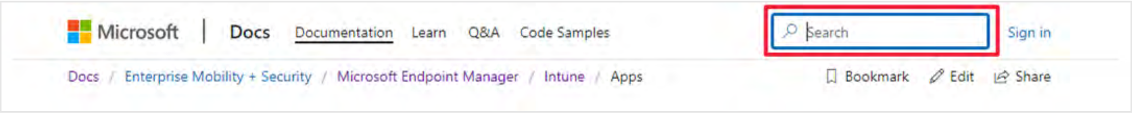
  - To further focus the search results to the current content library, include `site:learn.microsoft.com` in your query to scope the search engine.

- Use search terms that match terminology in the user interface and online documentation. Avoid unofficial terms or abbreviations that you might see in community content. For example, search for:
  - "management point" rather than "MP"
  - "deployment type" rather than "DT"
  - "Intune management extension" rather than "IME"

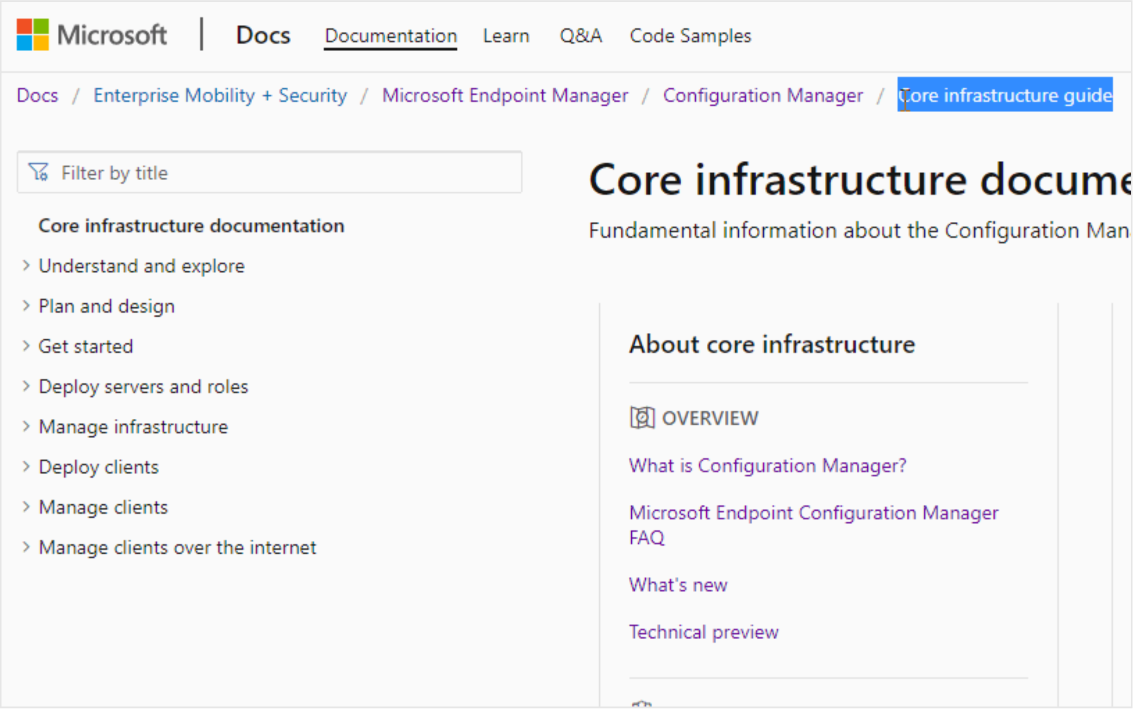
- To search within the current article, use your browser's **Find** feature. With most modern web browsers, press **Ctrl**+**F** and then enter your search terms.

- Each article on `learn.microsoft.com` includes the following fields to assist with searching the content:

  - **Search** in the upper right corner. To search all articles, enter terms in this field. Articles in this content library automatically include one of the following search scopes: `ConfigMgr`, `Intune`, or `Autopilot`.

    
    Microsoft
    Docs
    Documentation
    Learn
    Q&A
    Code Samples
    Search
    Sign in
    Docs / Enterprise Mobility + Security / Microsoft Endpoint Manager / Intune / Apps
    Bookmark
    Edit
    Share

  - **Filter by title** above the left table of contents. To search the current table of contents, enter terms in this field. This field only matches terms that appear in the article titles for the current node. For example, **Configuration Manager Core Infrastructure** (`learn.microsoft.com/mem/configmgr/core`) or **Intune Apps** (`https://learn.microsoft.com/mem/intune/apps/`). The last item in the search results gives you the option to search for the terms in the entire content library.


Microsoft
Docs
Documentation
Learn
Q&A
Code Samples
Docs / Enterprise Mobility + Security / Microsoft Endpoint Manager / Configuration Manager / Core infrastructure guide
Filter by title

Core infrastructure documentation

- Understand and explore
- Plan and design
- Get started
- Deploy servers and roles
- Manage infrastructure
- Deploy clients
- Manage clients
- Manage clients over the internet

Core infrastructure docume

Fundamental information about the Configuration Man

About core infrastructure

OVERVIEW

What is Configuration Manager?

Microsoft Endpoint Configuration Manager FAQ

What's new

Technical preview

Having problems finding something? File feedback! When you file an issue about search results, provide the search engine you're using, the keywords you tried, and the target article. This feedback helps Microsoft optimize the content for better search.

Add a custom search engine

With many modern web browsers, you can create a custom search engine. Use this feature to quickly and easily search `learn.microsoft.com`. For example, with Microsoft Edge, version 77 and later, use the following process:

1. In Microsoft Edge, version 77 and later, open **Settings**.

2. In the left menu, select **Privacy, search, and services**.

3. Scroll to the bottom of the **Services** group and select **Address bar and search**.

4. Select **Manage search engines**.

5. Select **Add** and specify the following information:

    - **Search engine**: Enter a friendly name to identify it in the list of search engines. For example, `Microsoft Learn`.

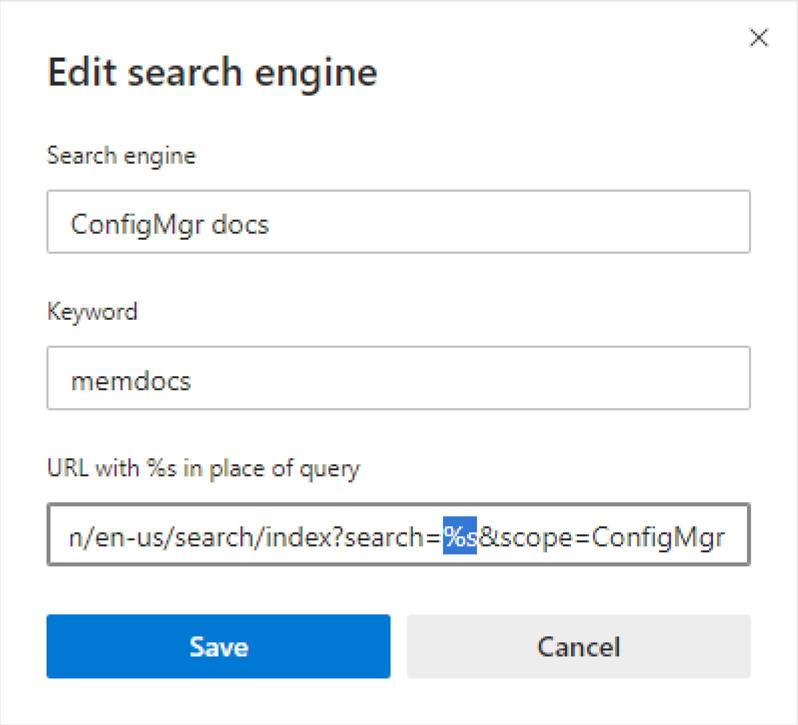
    - **Keyword**: Specify a short term to use in the address bar to activate this search engine. For example, `memdocs`.

    - **URL with `%s` in place of query**: For example,

    ```
    https
    ```

```
https://learn.microsoft.com/search/index?search=%s&scope=ConfigMgr
```

> ⓘ **Note**
>
> This example is specific to the `ConfigMgr` scope. You can remove the scope variable to search all `learn.microsoft.com` or use a different scope.
>
> The Microsoft technical documentation search engine requires a locale in the address. For example, `en-us`. You can change your entry to use a different locale.



Edit search engine

Search engine: ConfigMgr docs

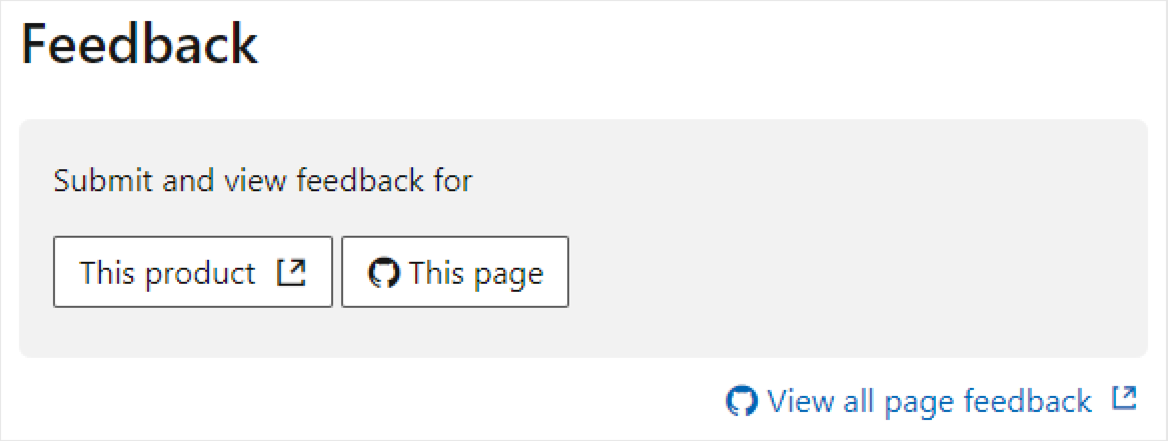
Keyword: memdocs

URL with %s in place of query: n/en-us/search/index?search=%s&scope=ConfigMgr

After you add this search engine, type your keyword in the browser address bar, press `Tab`, then type your search terms, and press `Enter`. It will automatically search Microsoft technical documentation for your specified terms using the defined scope.

About feedback

Select the **Feedback** link in the upper right of any article to go to the Feedback section at the bottom. Feedback is integrated with GitHub Issues. For more information about this integration with GitHub Issues, see the docs platform blog post.



To share feedback about the current article, select **This page**. A GitHub account is a prerequisite for providing documentation feedback. Once you sign in, there's a one-time authorization for the MicrosoftDocs organization. It then opens the GitHub new issue form. Add a descriptive title and detailed feedback in the body, but don't modify the document details section. Then select **Submit new issue** to file a new issue for the target article in the MEMDocs GitHub repository.

To see whether there's already feedback for this article, select **View all page feedback**. This action opens a GitHub issue query for this article. By default it displays both open and closed issues. Review any existing feedback before you submit a new issue. If you find a related issue, select the face icon to add a reaction, add a comment to the thread, or **Subscribe** to receive notifications.

Types of feedback

Use GitHub Issues to submit the following types of feedback:

- Doc bug: The content is out of date, unclear, confusing, or broken.
- Doc enhancement: A suggestion to improve the article.
- Doc question: You need help with finding existing documentation.
- Doc idea: A suggestion for a new article.
- Kudos: Positive feedback about a helpful or informative article!
- Localization: Feedback about content translation.
- Search engine optimization (SEO): Feedback about problems searching for content. Include the search engine, keywords, and target article in the comments.

If you create an issue for something not related to an article, Microsoft will close the issue and redirect you to a better feedback channel. For example:

- Product feedback for Configuration Manager or Intune
- Product questions
- Support requests for Configuration Manager or Microsoft Intune

To share feedback on the Microsoft Learn platform itself, see Docs feedback. The platform includes all of the wrapper components such as the header, table of contents, and right menu. Also how the articles render in the browser, such as the font, alert boxes, and page anchors.

Notifications

To receive notifications when content changes in the documentation library, use the following steps:

1. Use the docs search to find an article or set of articles.

   - Search for a single article by title, such as What's new in Microsoft Intune.

     > **Tip**
     >
     > To refine the search to a single article, use the full title that displays in the Microsoft technical documentation search results. You can also use a string from the first paragraph, as shown in this example.

     This example results in the following RSS link:

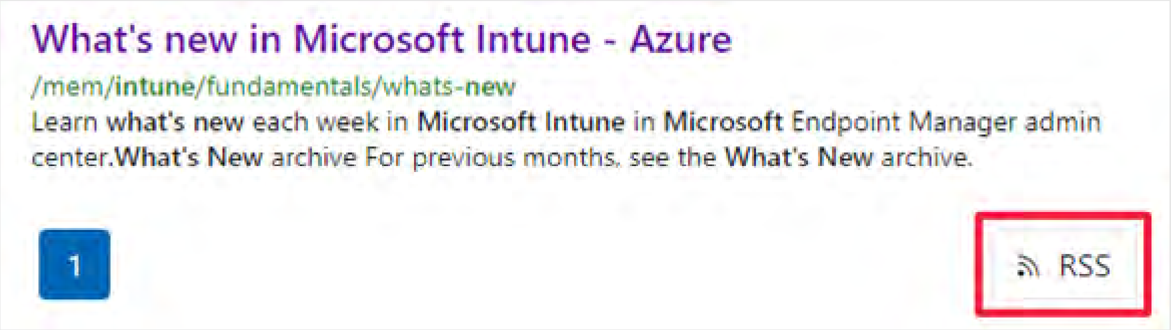
     ```https
     https://learn.microsoft.com/api/search/rss?
     search=%22What%27s+new+in+microsoft+intune%22%2B%22learn+what%27s+
     new%22&locale=en-
     us&facet=&%24filter=scopes%2Fany%28t%3A+t+eq+%27Intune%27%29
     ```

     > **Note**
     >
     > The above RSS feed URL example includes the `&locale=en-us` variable. The `locale` variable is required, but you can change it to another supported locale. For example, `&locale=ja-jp`.

   - Search for any Configuration Manager article about BitLocker

   > **Note**
   >
   > Use other keywords or the Microsoft Learn search filters to further refine your search query.

2. At the bottom of the list of results, select the **RSS** link.



What's new in Microsoft Intune - Azure

/mem/intune/fundamentals/whats-new

Learn what's new each week in Microsoft Intune in Microsoft Endpoint Manager admin center.What's New archive For previous months, see the What's New archive.

3. Use this feed in an RSS application to receive notifications when there's a change to any of the search results. Refer to the RSS application's documentation on how to configure and tune it.

> **Tip**
>
> You can also **Watch** the MEMDocs repository on GitHub. This method can generate *many* notifications. It also doesn't include changes from the private repository that Microsoft uses.

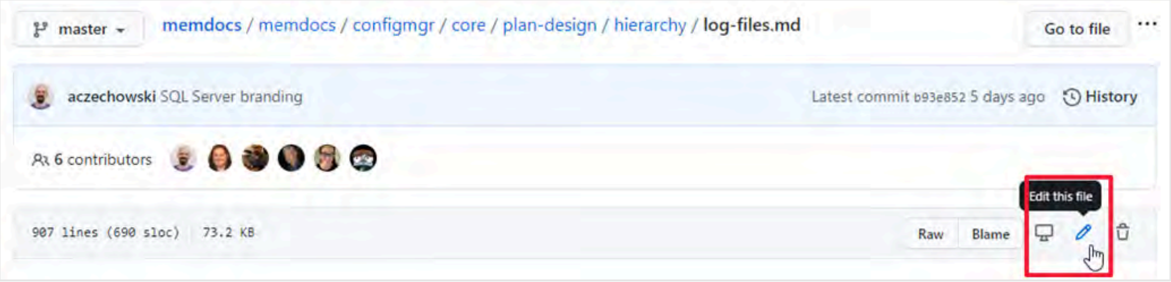
Contribute

The Microsoft Intune product family documentation library, like most Microsoft technical documentation, is open-sourced on GitHub. This library accepts and encourages community contributions. For more information on how to get started, see our contributor guide. The only prerequisite is to create a GitHub account.

Basic steps to contribute

1. From the target article, select **Edit** in the upper right corner. This action opens the source file in GitHub.

2. To edit the source file, select the pencil icon.



master
memdocs / memdocs / configmgr / core / plan-design / hierarchy / log-files.md
Go to file
aczechowski SQL Server branding
Latest commit b93e852 5 days ago
History
6 contributors
907 lines (690 sloc) 73.2 KB
Raw
Blame
Edit this file

3. Make changes in the markdown source. For more information, see How to use Markdown in Microsoft Learn articles.

4. In the Propose file change section, enter the public commit comment describing *what* you changed. Then select **Propose file change**.

5. Scroll down and verify the changes you made. Select **Create pull request** to open the form. Describe *why* you made this change. Select **Create pull request**.

The writing team receives your pull request, and assigns it to the appropriate writer. The author reviews the text, and does a quick edit pass on it. They'll either approve and merge the changes, or contact you for more information about the update.

What to contribute

If you want to contribute, but don't know where to start, see the following suggestions:

- Review an article for accuracy. Then update the **ms.date** metadata using `mm/dd/yyyy` format. This contribution helps keep the content fresh.

- Add clarifications, examples, or guidance based on your experience. This contribution uses the power of the community to share knowledge.

> ⓘ Note
>
> Large contributions require signing a Contribution License Agreement (CLA) if you aren't a Microsoft employee. GitHub automatically requires you to sign this agreement when a contribution meets the threshold. You only need to sign this agreement once.

Contribution tips

Follow these general guidelines when you contribute:

- Don't surprise us with large pull requests. Instead, file an issue and start a discussion. Then we can agree on a direction before you invest a large amount of time.

- Read the Microsoft style guide. Know the Top 10 tips for Microsoft style and voice.

- Follow the GitHub Flow workflow .

- Blog and tweet (or whatever) about your contributions, frequently!

(This list was borrowed from the .NET contributing guide.)

Feedback

Was this page helpful? Yes No

How to get support in the Microsoft Intune admin center

Article • 02/28/2025

Microsoft provides global technical, presales, billing, and subscription support for device management cloud-based services. These cloud-based services include Intune, Configuration Manager, Windows 365, and Microsoft Managed Desktop. You can access support for all of these options from **Help and support** in the Microsoft Intune admin center. In this article, we explain how to get to Help and support and review your different support options from within the admin center.

To access support resources in the Intune admin center, including creating and managing a support incident, your account must have an Azure Active Directory (Azure AD) role that includes the *action* **microsoft.office365.supportTickets**. Guest users are an exception: they can't file support tickets, even when granted the correct action. For information about Azure AD roles and permissions that are required to create a support ticket, see administrator roles in Azure Active Directory.

Support is available both online and by phone for paid and trial subscriptions. Online technical support is available in English and Japanese. Phone support and online billing support are available in other languages.

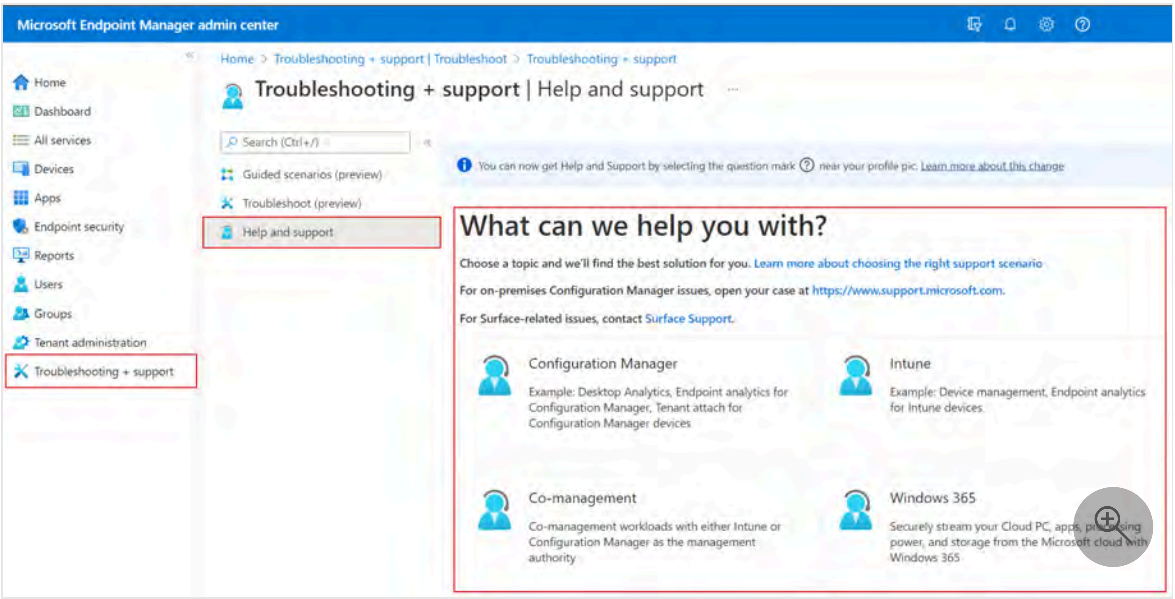
Access Help and support

Use one of the following links to open the Microsoft Intune admin center. The link you use depends on how your tenant is hosted:

- **Public cloud**: Use https://intune.microsoft.com
- **Private cloud** for government, which is also known as a sovereign cloud like Azure Government: Use https://intune.microsoft.us

To access help and support in the admin center, you have some options:

- Go to **Troubleshooting + support** or another node in the admin center and select **Help and support** to open a full screen experience of Help and support.



Microsoft Endpoint Manager admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Troubleshooting + support | Troubleshoot > Troubleshooting + support
Search (Ctrl+/)
Guided scenarios (preview)
Troubleshoot (preview)
Help and support

Troubleshooting + support | Help and support

You can now get Help and Support by selecting the question mark near your profile pic. Learn more about this change

What can we help you with?

Choose a topic and we'll find the best solution for you. Learn more about choosing the right support scenario

For on-premises Configuration Manager issues, open your case at https://www.support.microsoft.com.

For Surface-related issues, contact Surface Support.

Configuration Manager

Example: Desktop Analytics, Endpoint analytics for Configuration Manager, Tenant attach for Configuration Manager devices

Intune

Example: Device management, Endpoint analytics for Intune devices

Co-management

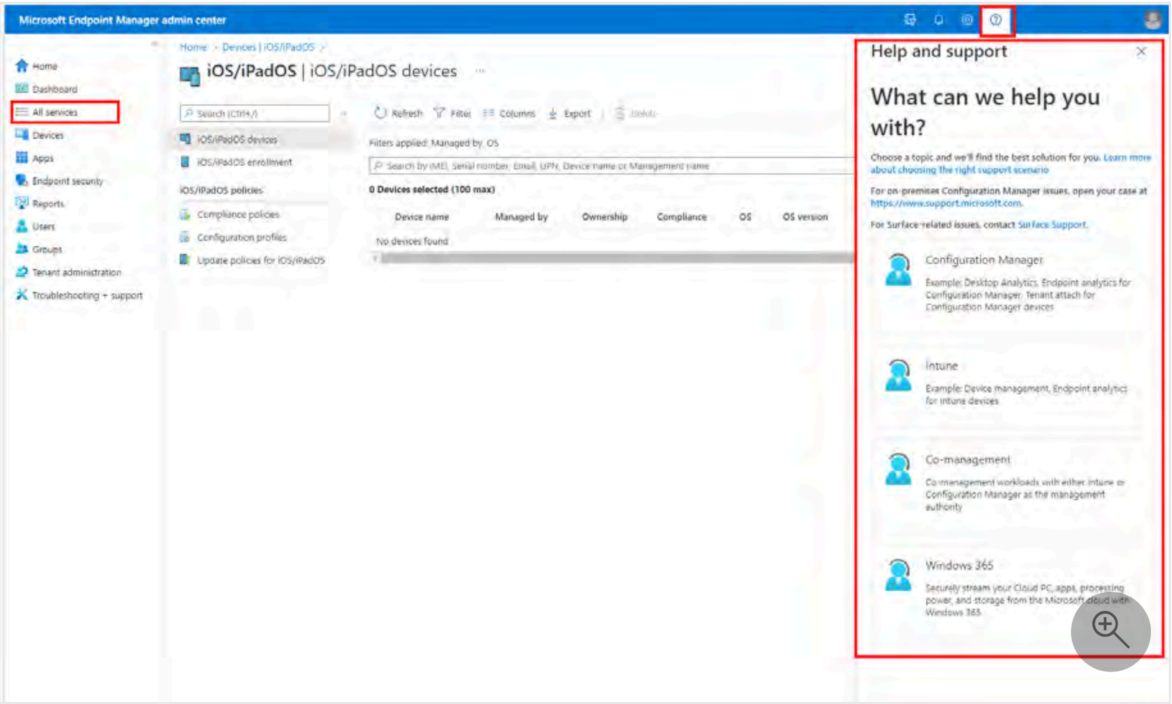
Co-management workloads with either Intune or Configuration Manager as the management authority

Windows 365

Securely stream your Cloud PC, apps, processing power, and storage from the Microsoft cloud with Windows 365

- From any node in the admin center, or your current area of focus, select the question mark (?) near your profile pic to open the Help and Support pane.

  In the following example, select **All services** and then select the question mark (?). **Help and support** opens:

  iOS/iPadOS | iOS/iPadOS devices

  Help and support

  What can we help you with?

  Choose a topic and we'll find the best solution for you. Learn more about choosing the right support scenario

  For on-premises Configuration Manager issues, open your case at https://www.support.microsoft.com.

  For Surface-related issues, contact Surface Support.

  Configuration Manager

  Example: Desktop Analytics, Endpoint analytics for Configuration Manager, Tenant attach for Configuration Manager devices

  Intune

  Example: Device management, Endpoint analytics for Intune devices

  Co-management

  Co-management workloads with either Intune or Configuration Manager as the management authority

  Windows 365

  Securely stream your Cloud PC, apps, processing power, and storage from the Microsoft cloud with Windows 365

  When you open **Help and support** in this way, it's pinned at the side. You can select any other option and it stays pinned.

Use Support Assistant to resolve issues

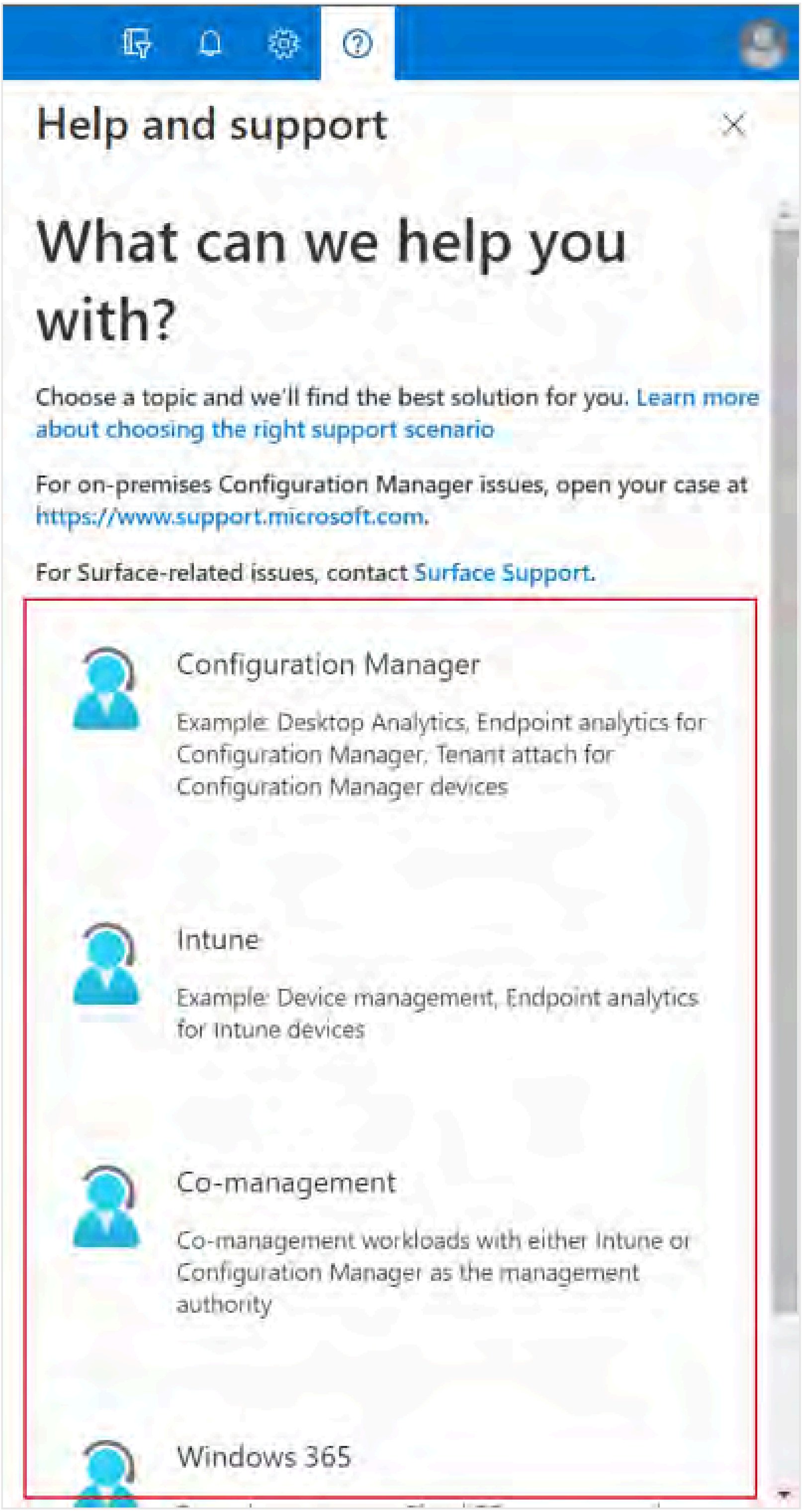
The Support Assistant uses AI to enhance your help and support experience, ensuring more efficient issue resolution. The Support Assistant is available in the Microsoft Intune admin center by selecting **Troubleshoot + support** > **Help and Support**, or by selecting the question mark near your profile pic.

> ⓘ **Note**
>
> You can enable and disable the Support Assistant by choosing to opt in and opt out at any time.

Choose the right support scenario

In **Help and support**, select any available option to focus support on your scenario. You can only see tiles for the services that you have subscriptions to use.

In the following example, you see the different services available in this subscription:



Help and support

What can we help you with?

Choose a topic and we'll find the best solution for you. Learn more about choosing the right support scenario

For on-premises Configuration Manager issues, open your case at https://www.support.microsoft.com.

For Surface-related issues, contact Surface Support.

Configuration Manager

Example: Desktop Analytics, Endpoint analytics for Configuration Manager, Tenant attach for Configuration Manager devices

Intune

Example: Device management, Endpoint analytics for Intune devices

Co-management

Co-management workloads with either Intune or Configuration Manager as the management authority

Windows 365

The following information can help you choose the correct focus:

- **Intune**:
  - Managing devices with Intune
  - Endpoint analytics for Intune devices

- **Configuration Manager**:
  - Endpoint analytics for Configuration Manager devices
  - Tenant attach for Configuration Manager devices

For issues with **on-premises Configuration Manager**, open your case at www.support.microsoft.com .

- **Co-management**:
  - Co-management workloads with Intune or Configuration Manager as the management authority

- **Microsoft Managed Desktop**:

  This tile is available only to Microsoft Managed Desktop customers.
  - Information requests for the Microsoft Managed Desktop tenant or configuration
  - Change requests to the configuration of Microsoft Managed Desktop devices
  - Reporting an incident or outage

  If you're a Microsoft Managed Desktop customer, then select the tile for Microsoft Managed Desktop related issues and the Service Requests page is displayed. For more information on Service Requests, see Admin support for Microsoft Managed Desktop.

- **Windows 365**:
  - When you have a subscription for Windows 365, this tile opens Help and support for Windows 365.

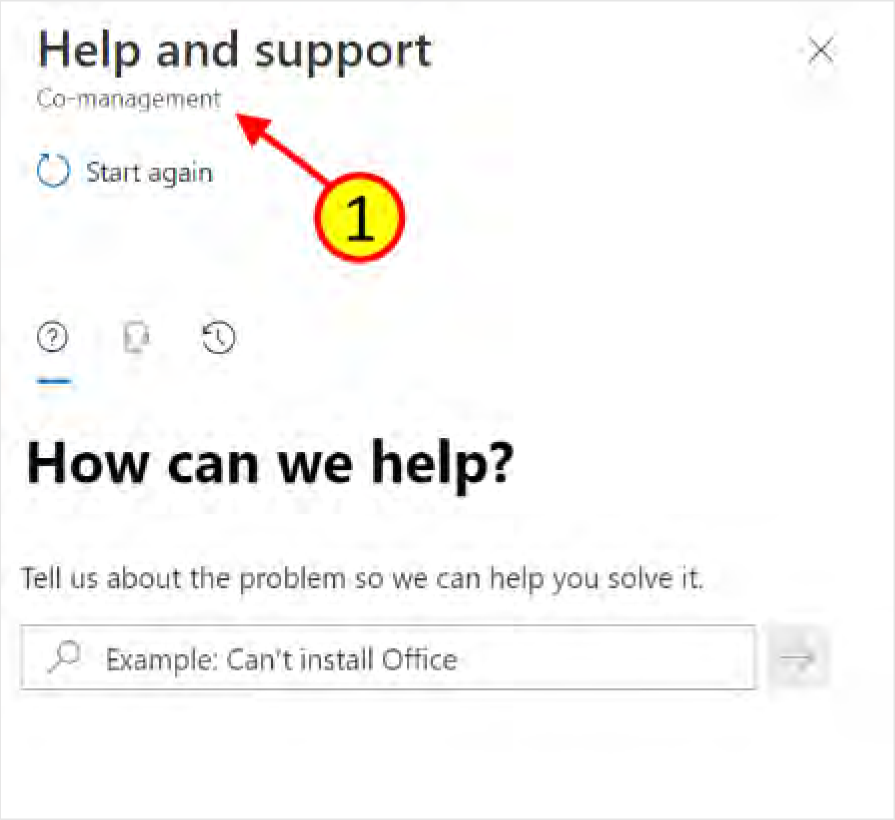
> **Tip**
>
> Help and Support might fail to open for newly created tenants, and the following message is presented:
>
> - *We encountered an unknown problem. Refresh the page but if the problem persists, create a case through M365 Admin Center and reference the session ID provided.*
>
> The error details include a *Session ID*, *Extension* details, and more.
>
> This problem occurs when you haven't authenticated and accessed the *How can we help?* page from your new tenant account through either the **Microsoft 365 Admin Center** at https://admin.microsoft.com , or the **Office 365 portal** at https://portal.office.com . To resolve this problem, select the link for *Microsoft 365 Admin Center* in the message, or visit https://portal.office.com , and sign in. Following authentication at either site, go to the Admin area and select the Need Help icon in the lower right. After completing these steps, the *Help and Support* page for Intune becomes accessible.

Review your support options

When you select a support scenario, the admin center displays the Help and Support page with the support scenario that you selected displayed at the top **(1)**. If the wrong support scenario is selected, you need to go back to make a different selection.

ⓘ Note

To access support scenarios in the Intune admin center, your account must have an Azure Active Directory (Azure AD) role that includes the *action* **microsoft.office365.supportTickets**.

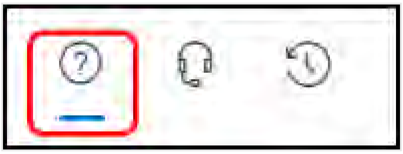

Help and support
Co-management
1
Start again
How can we help?
Tell us about the problem so we can help you solve it.
Example: Can't install Office

Above the *How can we help?* title, there are three icons that you can select to open different panes: *Find solutions*, *Contact support*, and *Service requests*. An underlined icon indicates the active pane you're viewing. By default, the Help and support page opens to the *Find solutions* pane.

Tip

Customers with a **Premier** or **Unified** support contract have other options for support. If you've a Premier or Unified support contract, you'll see a banner similar to the following image:

Search for solutions



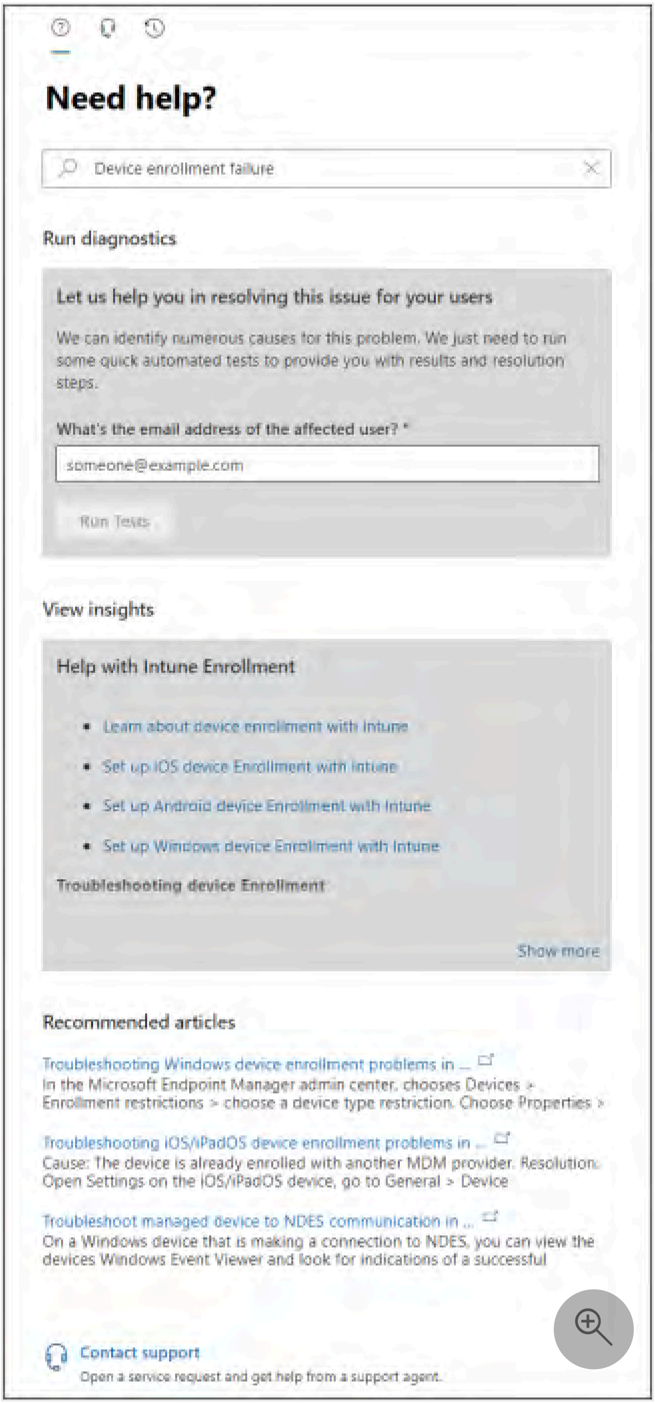
On the *Search for solutions* pane, specify a few details about an issue in the provided text box. The console might offer suggestions based on the details that you enter. Depending on the presence of specific keywords, the console offers one of two support experiences depending on what is available for the product you selected: the traditional support experience and the updated support experience.

Traditional experience

For products that use traditional support, when you enter keywords, the *Search for solutions* pane returns one or more of the following options. These options are based on the details you provide:

- **Run diagnostics**: From the console you can start automated tests and investigations of your tenant that can reveal known issues. When you run a diagnostic, you might receive mitigation steps you can take to help resolve the issue.
- **View insights**: Find links to documentation that provide context and background specific to the product area or actions you've described.
- **Recommended articles**: Browse suggested to troubleshooting articles and other content related to the issue you've described.

For example, for Microsoft Intune you might enter **device enrollment failure**. With these criteria, your results include the option to run diagnostics for a user account:



Need help?

Device enrollment failure

Run diagnostics

Let us help you in resolving this issue for your users

We can identify numerous causes for this problem. We just need to run some quick automated tests to provide you with results and resolution steps.

What's the email address of the affected user? *

someone@example.com

Run Tests

View insights

Help with Intune Enrollment

- Learn about device enrollment with Intune
- Set up iOS device Enrollment with Intune
- Set up Android device Enrollment with Intune
- Set up Windows device Enrollment with Intune

Troubleshooting device Enrollment

Show more

Recommended articles

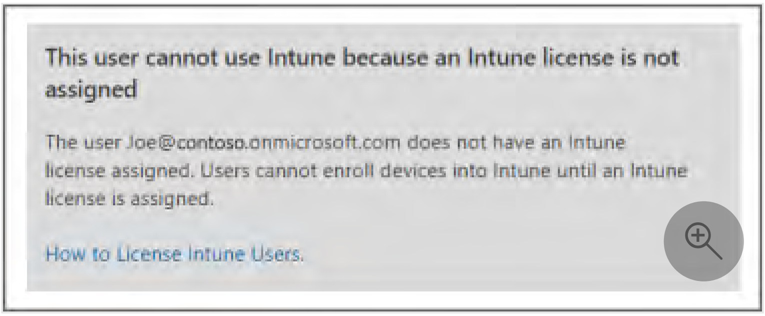
Troubleshooting Windows device enrollment problems in ...
In the Microsoft Endpoint Manager admin center, chooses Devices > Enrollment restrictions > choose a device type restriction. Choose Properties >

Troubleshooting iOS/iPadOS device enrollment problems in ...
Cause: The device is already enrolled with another MDM provider. Resolution: Open Settings on the iOS/iPadOS device, go to General > Device

Troubleshoot managed device to NDES communication in ...
On a Windows device that is making a connection to NDES, you can view the devices Windows Event Viewer and look for indications of a successful

Contact support
Open a service request and get help from a support agent.

Running the diagnostics can identify issues for that account in Azure AD. In this example, the user wasn't assigned a license for Intune, preventing the device enrollment, and we see a link to relevant content:



This user cannot use Intune because an Intune license is not assigned

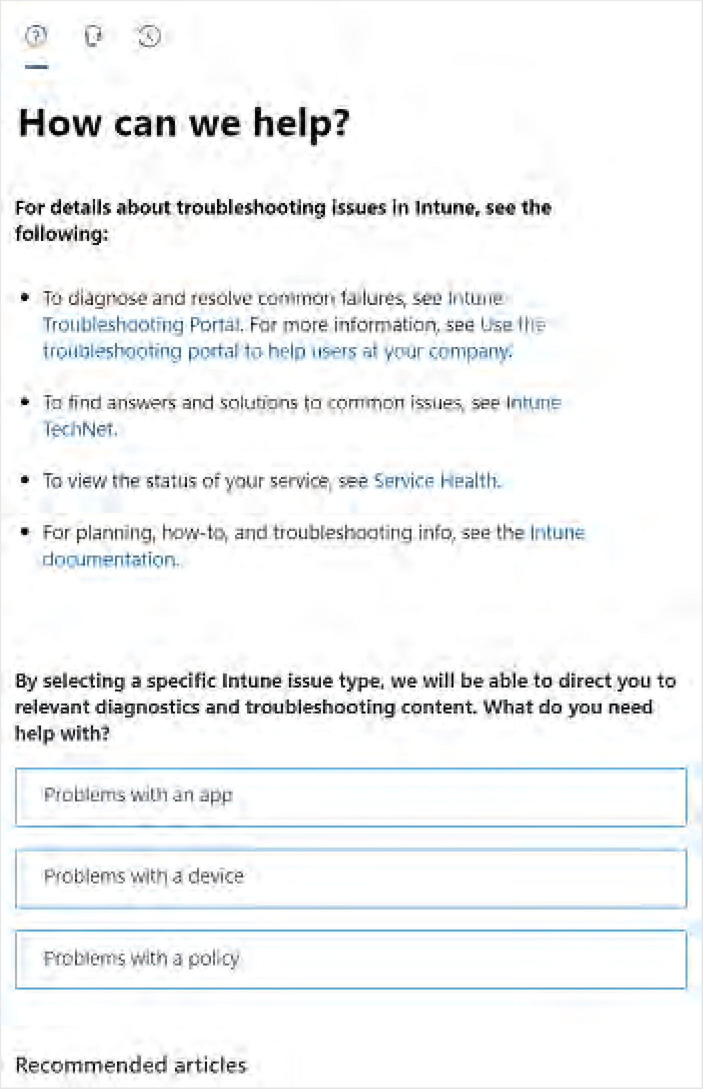
The user Joe@contoso.onmicrosoft.com does not have an Intune license assigned. Users cannot enroll devices into Intune until an Intune license is assigned.

How to License Intune Users.

Updated support experience

This support experience is currently available for Intune and Co-management.

Some keywords lead to an enhanced experience that helps you drill down to more scenario-specific support. For example, you're using Microsoft Intune and enter a generic search for *Need help with Intune*. You can see several more focused scenarios and you can select to clarify the problem and find more focused results.



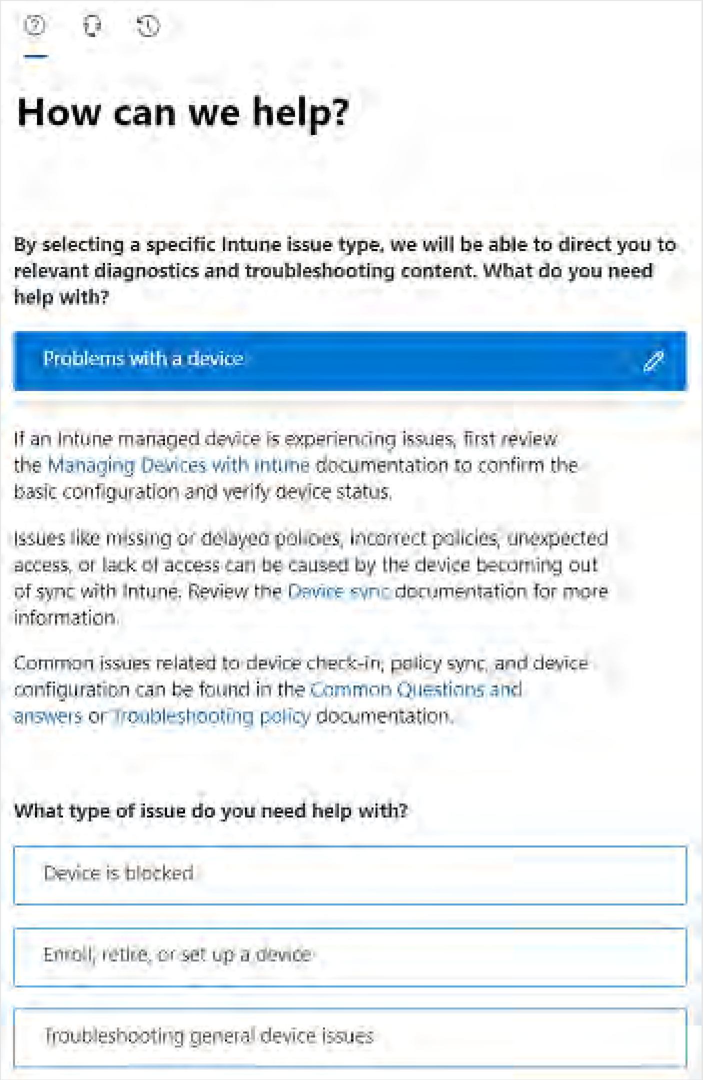
How can we help?

For details about troubleshooting issues in Intune, see the following:

- To diagnose and resolve common failures, see Intune Troubleshooting Portal. For more information, see Use the troubleshooting portal to help users at your company.
- To find answers and solutions to common issues, see Intune TechNet.
- To view the status of your service, see Service Health.
- For planning, how-to, and troubleshooting info, see the Intune documentation.

By selecting a specific Intune issue type, we will be able to direct you to relevant diagnostics and troubleshooting content. What do you need help with?

When you select a scenario, new options are offered to help narrow down the issue.



How can we help?

By selecting a specific Intune issue type, we will be able to direct you to relevant diagnostics and troubleshooting content. What do you need help with?

Problems with a device

If an Intune managed device is experiencing issues, first review the Managing Devices with Intune documentation to confirm the basic configuration and verify device status.

Issues like missing or delayed policies, incorrect policies, unexpected access, or lack of access can be caused by the device becoming out of sync with Intune. Review the Device sync documentation for more information.

Common issues related to device check-in, policy sync, and device configuration can be found in the Common Questions and answers or Troubleshooting policy documentation.

What type of issue do you need help with?

Device is blocked

Enroll, retire, or set up a device

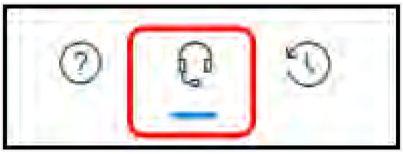
Troubleshooting general device issues

When presented, you can run automated tests or diagnostics where applicable, and view insightful information to help troubleshoot the problem. You might also see remediation steps to help you fix the issue.

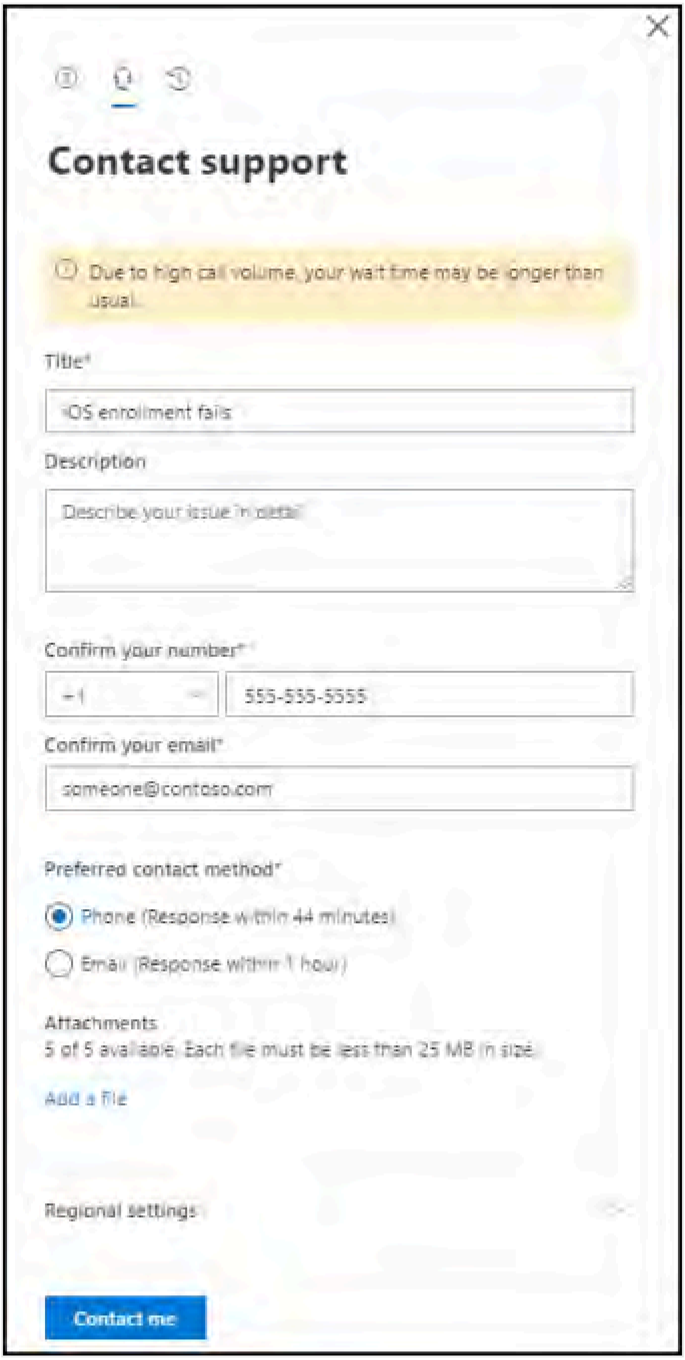
Contact support

The **Contact Support** option is available after you provide some basic keywords on the *Search for solutions* pane. You can use this pane to file an online support ticket for a supported service.

> ⓘ **Important**
>
> For technical support with third-party products that work with Intune (like Cisco or Lookout), contact the supplier of that product first. Before you open a request with Intune support, make sure you configured the other product correctly.



When requesting assistance, provide a description of the problem with as much detail as needed. After confirming your phone and email contact information, select the method of contact you prefer. The window displays a response time for each contact method, which gives you an expectation of when you'll be contacted. Before submitting your request, attach files like logs or screenshots that can help fill in details about the issue.



Contact support

ⓘ Due to high call volume, your wait time may be longer than usual.

Title*

iOS enrollment fails

Description

Describe your issue in detail

Confirm your number*

+1 | 555-555-5555

Confirm your email*

someone@contoso.com

Preferred contact method*

● Phone (Response within 44 minutes)

○ Email (Response within 1 hour)

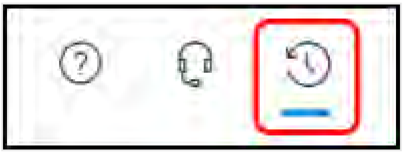
Attachments

5 of 5 available. Each file must be less than 25 MB in size.

After you fill in the required information, select **Contact me** to submit the request.

Service requests

The *Service requests* pane displays your case history. Active cases are at the top of the list, with closed issues also available for review.



If you have an active support case number, you can enter it here to go to that issue. Or, you can select any incident from the list of active and closed incidents to view more information about it.

When you're done viewing details for an incident, select the left arrow that appears at the top of the service request window just above the icons for the **How can we help?** pane icons. The back arrow returns the display to the list of opened support incidents.

Premier and Unified support options

As a customer with a **Premier** or **Unified** support contract, you can specify a severity for your issue, and schedule a support callback for a specific time and day. These options are available when you open or submit a new issue and when you edit an active support case.

Severity - The options to specify the severity of an issue depend on your support contract:

- *Premier*: Severity of A, B, or C
- *Unified*: Critical, or noncritical

Selecting either a severity **A** or **Critical** issue limits you to a phone support case, which provides the fastest option to get support.

Callback schedule - You can request a callback on a specific day and time.

Next steps

- Billing and subscription management support
- Use the troubleshooting portal to help users at your company
- Microsoft Intune troubleshooting documentation
- Volume licensing

Feedback

Was this page helpful? 👍 Yes 👎 No

Microsoft Intune troubleshooting

This documentation gives troubleshooting guidance to help you diagnose and fix issues that you might encounter when you use Microsoft Intune. For a complete article list, browse the navigation pane on the left, or use the search box to help find specific issues and solutions.

App management

OVERVIEW

App management overview

App installation error reference

App protection policies (APP)

HOW-TO GUIDE

Troubleshooting APP deployment

Troubleshooting APP user issues

Certificates

HOW-TO GUIDE

Troubleshooting SCEP certificate profiles

Troubleshooting SCEP profile deployment

Troubleshooting the NDES policy module

REFERENCE

Certificate Connector events and diagnostic codes

Co-management with Configuration Manager

HOW-TO GUIDE

Troubleshoot co-management auto-enroll

Troubleshoot co-management bootstrap

Troubleshoot co-management workloads

Device configuration

HOW-TO GUIDE

Troubleshooting Wi-Fi device configuration profiles

Windows - Troubleshooting CSP custom settings

Android - Factory reset protection emails setting isn't enforced

Device enrollment

HOW-TO GUIDE

Troubleshooting device enrollment

Troubleshooting Android Enterprise device enrollment

Troubleshooting Windows device enrollment errors

Troubleshooting the Enrollment Status Page (ESP)

Device management

HOW-TO GUIDE

Troubleshooting device actions

Windows 10 devices can't sync with Intune

Device protection

HOW-TO GUIDE

Troubleshoot Conditional Access

Troubleshooting BitLocker from the client side

Troubleshooting BitLocker with the Intune encryption report