# Office AMS: SIDELOADING

|  |  |
| --- | --- |
| Summary: | Applies to: |
| This sample shows how to use search to enumerate site collections | * Office 365 Multi Tenant (MT) * Office 365 Dedicated (D) * SharePoint 2013 on-premises |
| Solution: | Core.SideLoading, version 1.0 |
| Author: | Frank Marasco (Microsoft) |
| //\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  // THIS CODE IS PROVIDED \*AS IS\* WITHOUT WARRANTY OF  // ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING ANY  // IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR  // PURPOSE, MERCHANTABILITY, OR NON-INFRINGEMENT.  //\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* | |

# Scenario need

This scenario shows how one can use sideLoading of a Provider Hosted Application to install a SharePoint Provider Hosted Application to a site collection.

SharePoint Administrators can deploy apps to their tenancy basically two different ways. Deploy from the app catalog (“app stapling”) or via sideloading.

What is sideloading? App sideloading, from a SharePoint context, is the ability to install a SharePoint app directly into a site to explicitly bypass the regular governance controls of SharePoint. Sideloading apps is insecure. The main reason for blocking sideloading by default on non-developer sites is the risk that faulty apps pose to their host web/host site collection. Apps have the potential to destroy data and make sites or, given enough permissions, can even make site collections unusable. Therefore, apps should only be sideloaded in dev/test environments and in production only when deploying from the AppCatalog does not meet your needs. It is not recommended to sideload SharePoint Hosted-Applications, because of the risk of data loss.

Note:

* Enabling the app sideloading features requires tenant admin permissions (in a multi-tenant environment) or farm admin permissions (in a single tenant environment).
* You must have a user context when sideloading the application. App-only permission is not available.
* Sideloading does not suppress the security check or compensate existing security requirements. It does however enable the programmatic installation of an app
* You must still register and app principal for SharePoint Provider hosted appliations
* You should deactivate the sideloading feature immediately once the app is in installed. Site Collections admnistrators can install apps using CSOM which could circumvent your goverance practices.

## Centrally deployed apps vs side loading comparison

|  |  |
| --- | --- |
| App Stapling (Deploy from App Catalog) | Sideloading |
| Custom actions and app parts are not supported | Custom actions and app parts are supported |
| App Install, Uninstall and upgrade event receivers cannot be handled | App Install, Uninstall and upgrade event receivers do fire and can be handled |
| Site Collection Administrators cannot uninstall the application | Site Collection Administrators can uninstall the application |
| Applied to new and existing site collections | Custom code must be used to install the application |
| There is metadata about the app and updates are applied | Tenant Administrators must enable the sideloading feature prior to install the application and should be disabled after the application is installed |
|  | There is no metadata about the app and updates have to be managed manually |

# How to use against Office 365 Multi-tenant

Since this solution is based on the using a provider hosted application, the following should be taken in account:

* The user must be a tenant administrator in order to enable the SideLoading Feature
* The Provider hosted application has already been registered by the tenant administrator
* The Provider hosted application has been deployed to your hosting platform

Guid \_sideloadingFeature = new Guid("AE3A1339-61F5-4f8f-81A7-ABD2DA956A7D");

string \_url = GetUserInput("Please Supply the SharePoint Online Site Collection URL: ");

/\* Prompt for Credentials \*/

Console.WriteLine("Enter Credentials for {0}", \_url);

string \_userName = GetUserInput("SharePoint Username: ");

SecureString \_pwd = GetPassword();

ClientContext \_ctx = new ClientContext(\_url);

\_ctx.ApplicationName = "AMS SIDELOADING SAMPLE";

\_ctx.AuthenticationMode = ClientAuthenticationMode.Default;

//For SharePoint Online

\_ctx.Credentials = new SharePointOnlineCredentials(\_userName, \_pwd);

string \_path = GetUserInput("Please supply path to your app package:");

Site \_site = \_ctx.Site;

Web \_web = \_ctx.Web;

try

{

\_ctx.Load(\_web);

\_ctx.ExecuteQuery();

//Make sure we have side loading enabled. You must be a tenant admin to activate or you will get //an exception! The ProcessFeature is an extension method,

//see OfficeAMS (https://officeams.codeplex.com/) OfficeAMS.Core sample

\_site.ProcessFeature(\_sideloadingFeature, true);

try

{

var \_appstream = System.IO.File.OpenRead(\_path);

AppInstance \_app = \_web.LoadAndInstallApp(\_appstream);

\_ctx.Load(\_app);

\_ctx.ExecuteQuery();

}

catch

{

throw;

}

//we should ensure that the side loading feature is disable when we are done or if an //exception occurs

\_site.ProcessFeature(\_sideloadingFeature, false);

}

catch (Exception \_ex)

{

Console.ForegroundColor = ConsoleColor.Red;

Console.WriteLine(string.Format("Exception!"), \_ex.ToString());

Console.WriteLine("Press any key to continue.");

Console.Read();

}