Third Party Application Approval Process
in the Enterprise Shared Tenant

Overview

There are multiple ways that a third-party application can be added to a workspace in the EST. For the purposes of this document, **Third-Party application** is any application that is not part of the Microsoft 0365/AAD ecosystem. This includes applications from the Microsoft Store, the Azure Marketplace, agency purchased or developed applications either on premise or in the Cloud.

This document specifies how an agency can request a third-party application be added, by whom, and the process. It also includes the methods and criteria that should be considered before requesting that an application be added to the EST.

Before deploying applications to the AAD environment, administrators should review the following documentation that meets their use case:

Application management documentation | Microsoft Docs

Methods for Publishing third party Applications

- Purchase from the Microsoft Store:
- Purchase from the Azure Marketplace:
- Publish on-premise applications to AAD
- Direct Federation through ADFS

Evaluating Third-Party Applications

Things to consider while evaluating Applications

1. Is there a Microsoft Application that meets the same needs?
2. What is the Category of Data that will be used/generated with the application?
3. Does it support Single Sign-On?
4. Is data stored in O365 applications or outside of the tenant in the application environment?
5. If data is stored outside of Azure, is the data encrypted during transport and at rest?
6. Who will have access to this application? Are there any external users included?
7. Can access to the application be restricted to your agency?
8. What are the licensing requirements/restrictions for the application?
9. Is the application free or is there a cost? How will that cost be3 managed? Does it require that the entire tenant must be licensed, or can it be restricted to users within your agency?

Conditional Access and Third-party Applications:

Unlike Microsoft Applications, Conditional Access Policies cannot prevent the download of data to a personal device. Therefore, if agencies should limit access to applications with sensitive data to domain joined devices or SGN access only.

Any application that will be accessed by B2B accounts (External Users) requires a Design Review. In addition, it is required that all B2B accounts accessing state applications require from the Internet require that MFA be configured for that access even if the data is considered Category 1 or 2. In most cases, this is already configured in the EST by default, but no agency should exempt B2B accounts from MFA when accessing resources within the EST.

Records Retention in Third Party Applications

Unless the application you are considering stores data on SharePoint, Exchange or OneDrive, be aware that Records Retention Policies and eDiscovery searches will not be able to access this data. Therefore, agencies need to consider if data stored or created by these applications will need to be retained for Public Disclosure and Records Retention. This is the responsibility of the agency that is using the third-party application and not the responsibility of WaTech. Agencies planning on implementing third-party application within the EST should make sure that they consult with their internal records retention and public disclosure personnel about the ramifications of storing data outside of the EST.

Applications that would not Comply

The following list of items are "red flags" and should be an indication that this application will not be allowed in the Shared Tenant or pass OCS Design Review.

- Applications that store or transport sensitive data unencrypted.
- Applications that do not support single sign-on.
- Applications that do not guarantee data will not be used for personal purposes.
- Applications that require write access to the AAD.
- Applications that require Global Administrator rights in AAD or in O365.
- Applications that cannot be scoped to agency data only.

When will an Application be Required to complete an OCS Design Review?

- Applications that will be used and/or store sensitive data
- External users (B2B) will access the application
- Data can be downloaded from the application

Application Delegation

Configuration for applications federated with AAD and provisioned using the Application Proxy will be managed by the agency. This is a new feature that is not able to be delegated via ADFS. WaTech will maintain control over the security of the application (conditional access policies, MFA, etc.) in order to comply with State Security Standards.

Store applications can be provisioned to agencies that request or purchase them via policy. WaTech will create and maintain those policies for the agency.

Approval Process for Microsoft Store Applications

1. Review the OCS approved application list (https://watech.sp.wa.gov/ocs/SPC/SitePages/AgencyResources.aspx/) and available Microsoft products to see if they will meet your business requirements.
2. If not, use the Pre-production tenant to identify a third-party application that meets your business need.
3. Submit a Ticket through the Support Center to request the application. Review the applications permissions and implementation restrictions with the Cloud Enablement Team. The Cloud Enablement Team will determine if this application needs a Design Review.
4. If required, fill out the Design Review Checklist A and the Appendix A for the application and submit it to the Office of Cyber Security. This form is available on the Design Review SharePoint site listed above.
   Please note: If you have any questions about the OCS Design Review process, please contact the OCS Security Design Review (SDR) team at SDR@ocs.wa.gov
5. If the application is approved by OCS, submit a ticket to Cloud Enablement to add the application to your agency policy.
6. Present the application to CEAC with its use, description, cost and the business need it addresses for your agency. CEAC may determine that this will be the standard application for that purpose and/or that it be added to the Global Application Policy.

Approval Process for Azure Marketplace Applications

Azure Marketplace Applications are SaaS applications just like those currently federated directly through ADFS. These applications are accessed using single sign-on from AAD rather than AD, but the process for approval is the same as for any other federated application. If that application has already been approved for use for ADFS, it can be approved without Design Review for AAD. However, there may be additional limitations federating with AAD at this time and you still may be required to access the application through ADFS.

1. Review the OCS approved application list (https://watech.sp.wa.gov/ocs/SPC/SitePages/AgencyResources.aspx/) and available Microsoft products to see if they will meet your business requirements.
2. Submit a Ticket through the Support Center to Cloud Enablement to request the application.
3. A Federation Specialist will send you a checklist to fill out for the requested app.
4. Review the applications permissions and implementation restrictions with the Cloud Enablement Team. The Cloud Enablement Team will determine if this application needs a Design Review.
5. If required, fill out the Design Review Checklist A and the Appendix A for the application and submit it to the Office of Cyber Security. This form is available on the Design Review SharePoint site listed above.

6. If the application is approved by OCS, submit a ticket to Cloud Enablement to complete the federation with the application and give agency personnel access and configure conditional access policies that may be required.

Publishing On-Premise Applications to AAD Using the AAD Application Proxy Service

Using the App Proxy Service, on-premises applications can now be published to AAD and displayed on the "All Apps" page in AAD. Unlike the other applications listed above, these are applications that are owned by the agency; therefore, the agency should understand the data and risks of publication outside of the SGN.

1. Submit a Ticket through the Support Center to Cloud Enablement to request the application.
2. A Federation Specialist will discuss your application with you and determine if publication will require a design review and other requirements.
3. If required, fill out the Design Review Checklist A and the Appendix A for the application and submit it to the Office of Cyber Security. This form is available on the Design Review SharePoint site listed above.
4. If the application is approved by OCS, submit a ticket to Cloud Enablement to complete the publication of the application, give agency personnel access and configure conditional access policies that may be required.
   Please note: For any Design Review that is approved, OCS will provide an email message (this could contain a "green light" statement or a general approval note with outlined provisions) to indicate the request can move forward. Please include this email message from OCS within the ticket request.

For more information on the Application Proxy, please see:

Azure AD secure hybrid access | Microsoft Docs