APP GOVERNANCE GUIDE

For Microsoft Teams Administrators in Government Community Cloud

Summary

This guide is designed to help administrators set up Microsoft Teams to maximize user productivity while mitigating risk. The main tools we'll be using to govern apps in Teams are app policies – a control given to tenant admins. These policies are really powerful because they give granular control over which apps are accessible to individual users. As a result, admins never have to worry about their users sharing data with app developers that haven't been approved internally. To get familiar with app policies, watch this short video.

Follow these steps to successfully adopt app policies and maximize the number of apps available to end-users. In the end you should walk away with more productive, collaborative, and happy colleagues!

Checklist

Item	Task	Expected Result
1	Leverage Teams apps for your own team - e.g. Jira, ServiceNow for tickets	Build familiarity with apps in Teams so that you can speak to them confidently and see first-hand how they can boost collaboration and productivity
2	Review the security and compliance catalog for third-party apps	Understand the security and compliance attributes of third-party applications
3	Adjust org-wide app settings to allow third-party apps	If you want to block any apps, we recommend using permission policies. Org-wide settings is not the best place for blocking (see why on page 3)
4	Create a custom app permission policy just for a small group of trusted people from IT	Creates a safe place to test apps that the rest of the org can't access
5	Enable apps in the global (org-wide default) permission policy	Make sure as many apps are enabled as you're comfortable allowing (see page 3 for criteria you might use to determine which apps to enable)
6	If you are struggling to identify apps to enable in Teams, find out which apps are enabled for Azure Active Directory single-sign-on	If a cloud application is using AAD for sign-on, it has already passed an internal review and should be enabled in Teams
7	Create a feedback loop from end-users to learn what is working. Try a specific channel or anonymous form pinned as a tab in Teams	Learn where end-users are running into roadblocks with apps or find out if there is significant demand for a specific application
8	Use app setup policies to pin apps to the left rail. Start with a productivity app or HR app which is universally relevant to all employees	Increases discoverability and engagement by up to 5-10X by making the most-used apps easier for users to find

Introduction

For Microsoft Teams customers to successfully take advantage of Teams' platform capabilities, administrators must set up an app governance process that finds harmony between enabling the wide-ranging scenarios for app integrations in Teams and accepting the limitations of internal IT policies, standards, and risk-profiles.

KEY RECOMMENDATION

Administrators should first find ways to benefit from apps themselves! Are there apps to capture end-user feedback? (Forms) Can you bring your tasks and tickets into Teams? (Jira, ServiceNow)

Step 1: Identify Internal Constraints

As you begin the process of identifying your governance criteria, ask the following questions:

What software tools are already approved for use *outside* Teams today?

- Piggy-back on work that's already been done! What standards did these applications have to meet?

What situations does your IT department most want to avoid? (e.g. customer data leak, confidential information stored in non-compliant way, shadow IT, overload of licensing requests, etc)

- Explore the security and compliance catalog for third-party apps. The information in this catalog will help you make educated decisions about third-party apps and whether they meet internal standards. The data listed for each app could inspire you to set certain criteria for your app policies. For example: "We allow apps that meet FINRA compliance standards" or "We allow apps that have a data audit trail."
- Read this list of considerations on app permissions and capabilities. This article will answer questions about when data leaves your network through specific app capabilities like bots, tabs, and connectors.

What apps might IT block that would significantly reduce employee productivity?

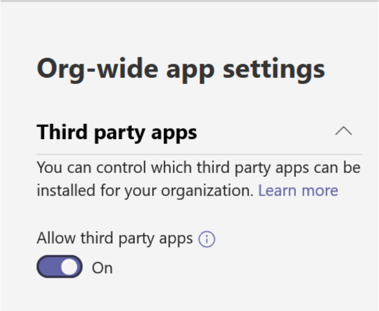
- Sometimes there are apps like Salesforce, ServiceNow, or Trello that should be enabled from day one because they are such an important part of the organization's workflows. Try to push these through even if they require special reviews or exceptions.

KEY RECOMMENDATION

Review the security and compliance catalog for third party apps. Most third-party apps in the app store have a listing with details about the developer, how they handle data, and which compliance standards they meet. View the ADP Virtual Assistant app profile as an example.

Step 2: Define Permission Criteria

There are several tools in the admin portal to control which apps are exposed to end users. These settings include Org-wide App Settings and App Permission Policies (see exhibits 1 and 2). Org-wide app settings (see right) should be used sparingly because they supersede permission policies and create unnecessary, binding constraints. For example, if an IT team wants two of its members to test a third-party app prior to making it available to others, they need their own permission policy that allows that app. If they block third-party apps entirely in org-wide settings, the custom permission policy is overridden, and they won't be able to conduct the necessary testing.



Org-wide app settings

Third party apps

You can control which third party apps can be installed for your organization. Learn more

Allow third party apps: On

KEY RECOMMENDATION

We suggest allowing third party apps in org-wide app settings. If administrators want to block apps (an entire category or specific apps) this should be done with permission policies.

The key criteria to consider in setting up app permissions are:

Which Microsoft apps will be allowed?

- There are very few reasons to not allow all Microsoft apps since they are integrating Office 365 applications which have the same data-handling, security, and compliance standards as Microsoft Teams.
- Two exceptions include the app called "*Who*", which is developed by Microsoft but appears in the third-party catalog because it is built using other services outside of Microsoft Office. The Yammer integration is also non-compliant today and will not appear in the list of Microsoft apps.

Which third party apps will be allowed?

- This will be mostly answered by the constraints identified in step 1 above (details about the app's security/compliance or the way data is transferred via specific app capabilities).
- Note that the "website" app (ability to add any website as a tab in a channel) is treated like a third-party app and will be blocked by default.

As administrators think about the criteria they will use to enable or block apps, they may prefer to expose apps only to specific business units. For example, the Salesforce app would only be made available to the sales team. This is possible by creating custom permission policies and applying them to groups of users with a powershell script.

KEY RECOMMENDATION

Once app policies are implemented, build in a feedback loop from end-users so that IT can learn what is working and what is not. This could be as easy as creating a specific Team and Channel for feedback or making an anonymous form available in Teams for users to share app-related requests.

Frequently Asked Questions

GENERAL

What about custom apps?

Custom, line-of-business applications are not available or supported in the Government Community Cloud as of today, January 17, 2020.

What are the default settings?

Org-wide settings: "Allow Third party apps" is turned off in org-wide settings. "Allow new third party apps published to the store by default" is also turned off. All third-party apps are included in the list of blocked apps.
Permission policies; Microsoft Apps are all allowed. Third party apps are all blocked.

How long does it take for a policy to propagate?

Up to 24-48 hours. This can be frustrating with setup policies when you expect to see the icons in the sidebar change or want to get access to an app. Try making the policy adjustment on Friday so users will see the change first thing on Monday.

How do app permission policies relate to pinned apps and app setup policies?

You can use app setup policies together with app permission policies. Pre-pinned apps are selected from the set of enabled apps for a user. Additionally, if a user has an app permission policy that blocks an app in their app setup policy, that app won't appear in Teams.

Can I apply policies to groups?

Currently you cannot apply policies to distribution groups or security groups. You must use powershell to apply policies in bulk.

PERMISSION POLICIES

What does a user experience when an app is blocked?

Users can't interact with a blocked app or its capabilities, such bots, tabs, and messaging extensions. (see more)

SETUP POLICIES

How many apps can be pinned with setup policies?

A minimum of two apps must be pinned. An unlimited amount can be pinned, but the average screen can only show about 11-12. Any apps that can't fit in the screen move to the overflow (ellipsis on desktop, overflow tray on mobile).

Are there any issues or best practices with app setup policies on mobile?

Setup policies (pinning) are the best way to distribute line-of-business apps on mobile because as of January 2020 there is no app store to search for apps on mobile.

Why isn't a pinned app appearing on mobile?

There are only 3-5 icons displayed because of the smaller screen size. It might be in the "more" overflow.

Common Concerns

Third party applications might have access to all my Teams information (conversations and user data)
This is a common fear, but that’s now how the Teams platform works. See these details on what information bots, tabs, messaging extensions, and connectors can access. A few highlights:

Bots & Messaging Extensions

- Bots only have access to teams to which they've been added or to users who have installed them.
- Bots can only receive information when they’re explicitly mentioned by users. This data leaves the corporate network.
- Bots can retrieve (and might store) very basic identity information for the team members the app has been added to, or for individual users in personal or group chats. To get further information about these users, the bot must require them to sign in to Azure Active Directory (Azure AD)

Tabs

- The risk profile for a tab is almost identical to that same website running in a browser tab.

Connectors

- The system that posts connector messages doesn't know who it's posting to or who receives the messages: no information about the recipient is disclosed. (Microsoft is the actual recipient, not the tenant; Microsoft does the actual post to the channel.)
- No data leaves the corporate network when connector messages are posted to a channel.

If we allow apps, our employees will just start using all kinds of apps and it will be impossible to control
This is also a valid concern. A few things to consider:

- There are millions of web-based software providers available to users outside of Teams - this is the same problem at its core. Employees should be educated on where it is safe to share or store confidential company information, whether it is through web browsers or Microsoft Teams.
- Many apps require licenses to use their full functionality. This creates a natural obstacle in users adopting new apps. Generally, if a user uses an application outside Teams, they’re likely to use it inside Teams.

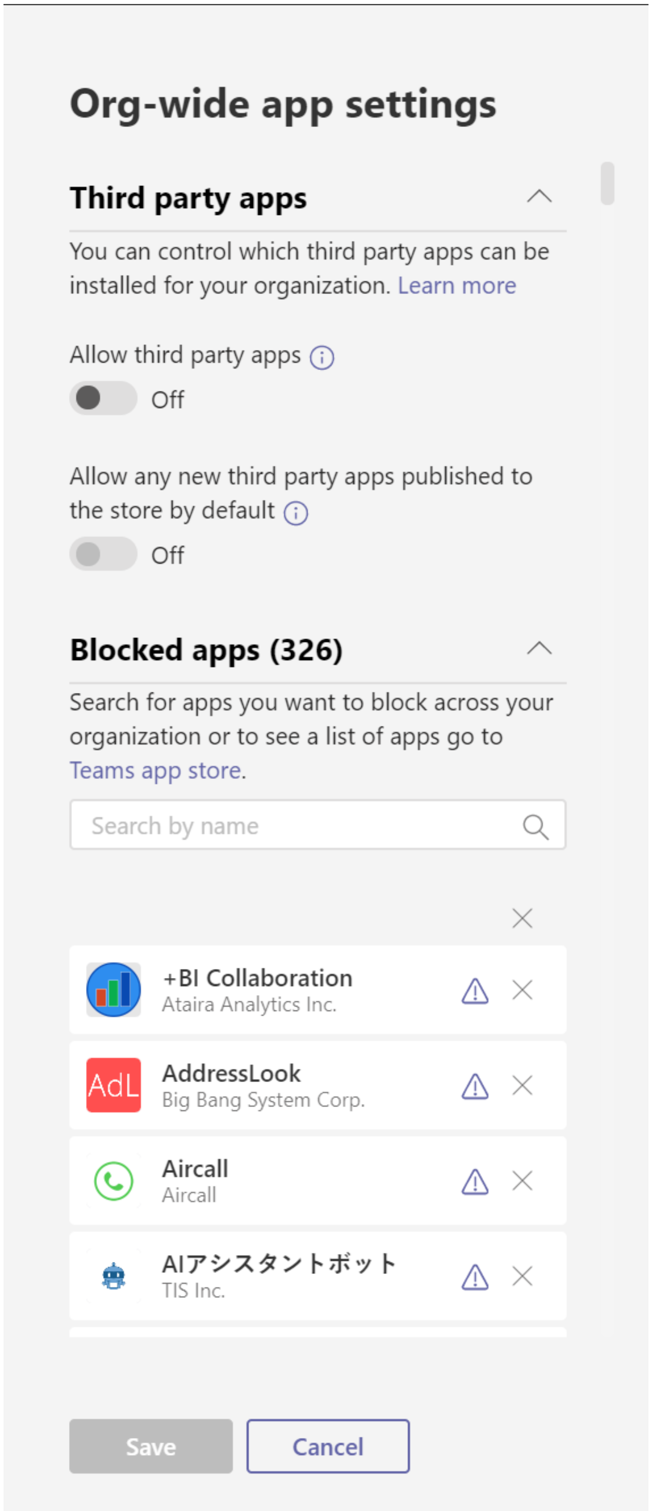
Links and Resources

Description	Link
Video explaining app policies	https://youtu.be/PiqDq9mHNm4
Security and compliance catalog of third-party apps	https://docs.microsoft.com/teams-app-certification/all-apps
App permission policies documentation	https://docs.microsoft.com/microsoftteams/teams-app-permission-policies
App setup policies documentation	https://docs.microsoft.com/microsoftteams/teams-app-setup-policies
Edit user settings in bulk using Powershell	https://docs.microsoft.com/microsoftteams/edit-user-settings-in-bulk
Documentation on pre-installing apps	https://docs.microsoft.com/graph/teams-proactive-messaging
Details on what information apps can access	https://docs.microsoft.com/MicrosoftTeams/app-permissions

Appendix A

Exhibit 1: Org-wide app settings

The settings with the highest precedence over app usage. Use sparingly.



Org-wide app settings

Third party apps

You can control which third party apps can be installed for your organization. Learn more

Allow third party apps ⓘ

○ Off

Allow any new third party apps published to the store by default ⓘ

○ Off

Blocked apps (326)

Search for apps you want to block across your organization or to see a list of apps go to Teams app store.

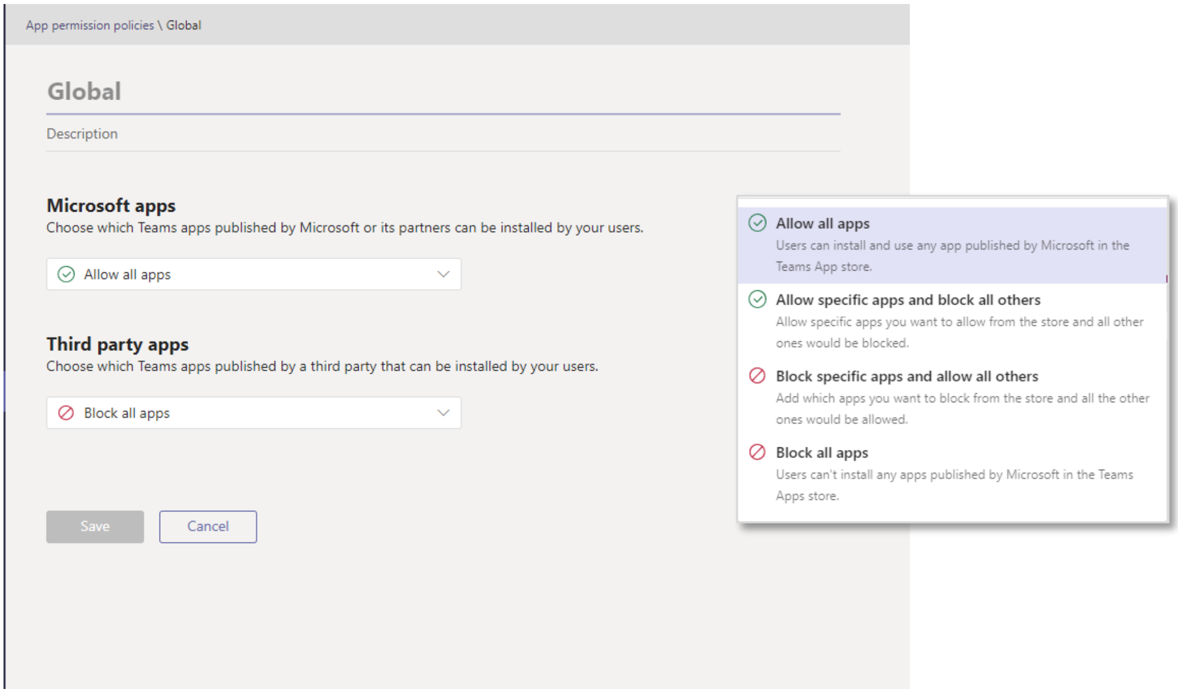
Search by name

+BI Collaboration Ataira Analytics Inc.	⚠	×
AddressLook Big Bang System Corp.	⚠	×
Aircall Aircall	⚠	×
AIアシスタントボット TIS Inc.	⚠	×

Save Cancel

Exhibit 2: Permission Policy

Determines which apps are available to users



App permission policies \ Global

Global

Description

Microsoft apps

Choose which Teams apps published by Microsoft or its partners can be installed by your users.

Allow all apps

Third party apps

Choose which Teams apps published by a third party that can be installed by your users.

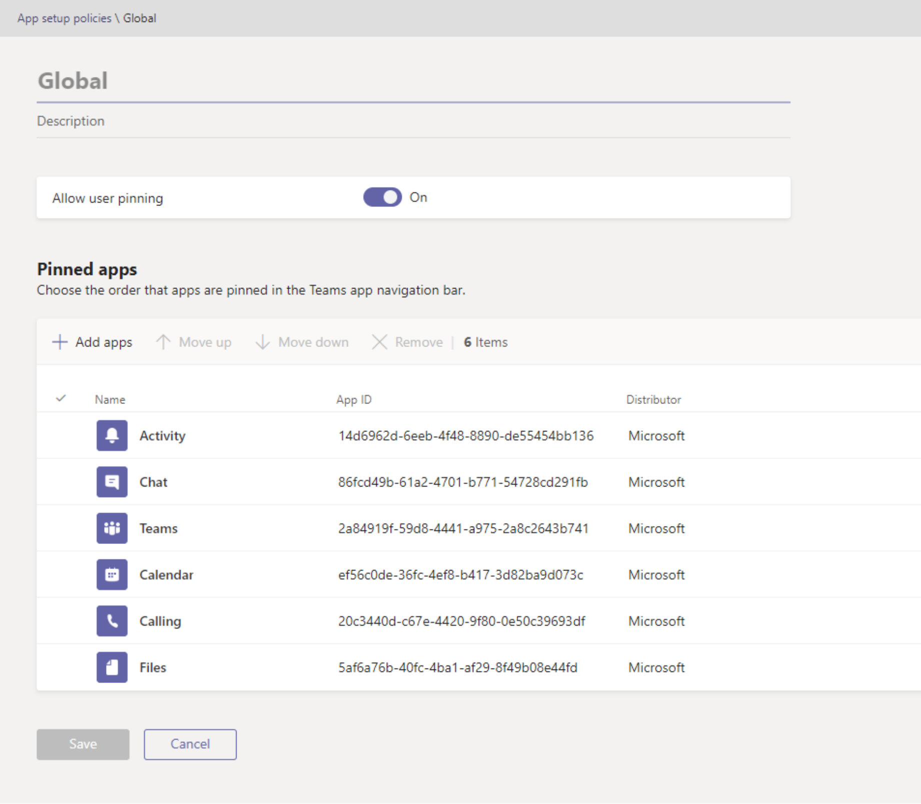
Block all apps

Save | Cancel

- ✓ **Allow all apps**
  Users can install and use any app published by Microsoft in the Teams App store.
- ✓ **Allow specific apps and block all others**
  Allow specific apps you want to allow from the store and all other ones would be blocked.
- ⊘ **Block specific apps and allow all others**
  Add which apps you want to block from the store and all the other ones would be allowed.
- ⊘ **Block all apps**
  Users can't install any apps published by Microsoft in the Teams Apps store.

Exhibit 3: Setup Policy

Customizes the icons in the left navigation bar in the Teams client (desktop, web, mobile)



App setup policies \ Global

Global

Description

Allow user pinning: On

Pinned apps

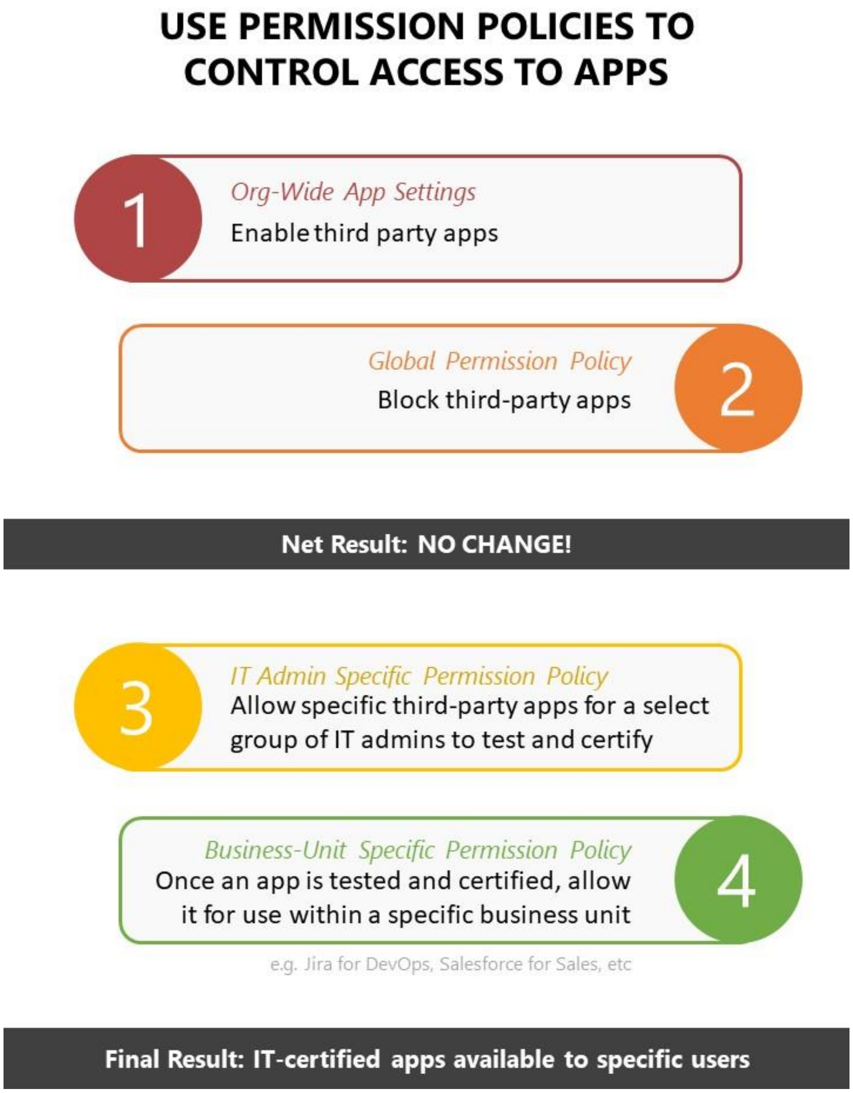
Choose the order that apps are pinned in the Teams app navigation bar.

Name	App ID	Distributor
Activity	14d6962d-6eeb-4f48-8890-de55454bb136	Microsoft
Chat	86fcd49b-61a2-4701-b771-54728cd291fb	Microsoft
Teams	2a84919f-59d8-4441-a975-2a8c2643b741	Microsoft
Calendar	ef56c0de-36fc-4ef8-b417-3d82ba9d073c	Microsoft
Calling	20c3440d-c67e-4420-9f80-0e50c39693df	Microsoft
Files	5af6a76b-40fc-4ba1-af29-8f49b08e44fd	Microsoft

Save | Cancel

Exhibit 4: Recommended action to unblock third-party apps using permission policies

Move the block from org-wide settings to permission policies. Then set up policies that make sense for individual business units.



USE PERMISSION POLICIES TO CONTROL ACCESS TO APPS

1 *Org-Wide App Settings*
Enable third party apps

2 *Global Permission Policy*
Block third-party apps

Net Result: NO CHANGE!

3 *IT Admin Specific Permission Policy*
Allow specific third-party apps for a select group of IT admins to test and certify

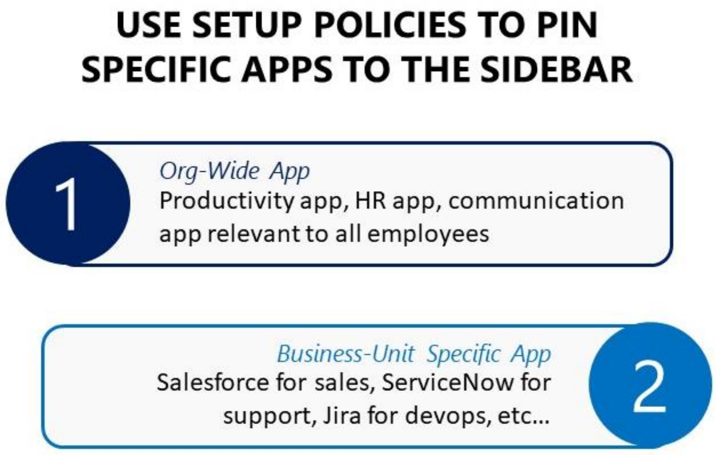
4 *Business-Unit Specific Permission Policy*
Once an app is tested and certified, allow it for use within a specific business unit

e.g. Jira for DevOps, Salesforce for Sales, etc

Final Result: IT-certified apps available to specific users

Exhibit 5: Recommended action to pin apps using setup policies

Consider org-wide apps first and then business-unit specific apps.



USE SETUP POLICIES TO PIN SPECIFIC APPS TO THE SIDEBAR

1 *Org-Wide App*
Productivity app, HR app, communication app relevant to all employees

Business-Unit Specific App
Salesforce for sales, ServiceNow for support, Jira for devops, etc... 2

Final Result: Tools are more visible to the individuals that use them