Separating business and personal settings with Enterprise State Roaming

Microsoft IT was excited to take advantage of the Enterprise State Roaming feature in Windows 10 and Microsoft Azure Active Directory Premium, which gives users a unified experience across devices. Enterprise State Roaming offers enterprise-grade security, increases user productivity, helps to address privacy concerns, and simplifies IT management. It also synchronizes personal settings from the Windows operating system and data settings from modern apps to Azure.

Better user experience, privacy, and management

Many users have a range of devices including corporate laptops and tablets, as well as personal devices. Enterprise State Roaming provides a consistent look-and-feel and common settings across all devices without the need to reconfigure them. When users set up a new device or replace hardware, configuration and setup time are significantly reduced, since settings are automatically applied. Users can spend more time being productive and less time customizing the device.

In addition to saving time, Enterprise State Roaming keeps corporate and personal data separate. It syncs business settings when users sign in with Microsoft corporate credentials. And when users sign in with a personal account, these personal settings are stored separately, which helps protect employee privacy. Once Enterprise State Roaming is enabled, Azure Rights Management services encrypts data automatically on the Windows 10 device, and the data stays encrypted in the cloud for added protection.

Reducing administrative overhead within our organization is important. Enterprise State Roaming is simple to set up and maintain. The Azure portal helps us monitor the sync status of devices in a straightforward way.

Implementation at Microsoft

We deployed Enterprise State Roaming as a pilot before the feature release. The first test included approximately 100 users. Password roaming was not included in early test stages. When the pilot was expanded to approximately 1,000 users, however, the data that was stored in Enterprise State Roaming was encrypted, enabling roaming of passwords.

Using a pilot process, we deployed new builds quickly and cost-effectively to many pilot users, with minimal user disruption. This process improved subsequent user participation, which increased the amount and variety of feedback. With the global release of Windows 10 November update, Enterprise State Roaming became available to all our users.

Because our employees use both company and personal devices for work, a multi-identity scenario—where users can sign in to the device with either their corporate account or their Microsoft account—is common. In Windows 10, having multiple identities lets users download and install consumer apps through the Windows Store.

The primary account—either an Azure Active Directory (Azure AD) account or a Microsoft account—is used to sign in to Windows. The settings and app data stay in their respective storage locations and are available based on the identity that’s used to sign in. The app settings are based on the identity of the app acquisition, and the relevant data is available across devices.

Deploying and managing

For us, as with most organizations, enabling Azure AD–joined devices for Enterprise State Roaming is easy via the Azure Portal. From this portal, we chose to enable Enterprise State Roaming for our entire Azure AD, although it’s possible to configure this differently. Our administrators can view the sync status of all our organization’s devices, and can create security groups to enable and disable roaming for each group, if needed.
Figure 1 shows some examples of configurations via the Azure Portal.

![Image of Azure Portal](image)

**Figure 1. Deploying and managing Enterprise State Roaming via the Azure Portal.**

We use Group Policy settings and mobile device management policies (via Microsoft Intune) for fine-tuned control on corporate-owned devices. Table 1 lists the policies. (*MDM=mobile device management; GP=Group Policy)

**Table 1. Policies to manage Enterprise State Roaming**

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Type</th>
<th>Description</th>
<th>Available platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowMicrosoftAccountConnection</td>
<td>*MDM</td>
<td>Allows users to add a Microsoft account to their device. Disallowing Microsoft accounts keeps devices in the business-only scenario</td>
<td>Mobile and desktop</td>
</tr>
<tr>
<td>AllowSyncMySettings</td>
<td>MDM</td>
<td>Allows users to roam Windows settings and app data</td>
<td>Mobile and desktop</td>
</tr>
<tr>
<td>Do not sync</td>
<td>*GP</td>
<td>Has same functionality as AllowSyncMySettings MDM policy</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync personalize</td>
<td>GP</td>
<td>Disables “Theme” syncing</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync browser settings</td>
<td>GP</td>
<td>Disables “Web browser settings” syncing</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync passwords</td>
<td>GP</td>
<td>Disables “Passwords” syncing</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync other windows settings</td>
<td>GP</td>
<td>Disables “Other Windows settings” syncing</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync desktop personalization</td>
<td>GP</td>
<td>Do not use – has no effect</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync on metered connections</td>
<td>GP</td>
<td>Disables roaming on metered connections like cellular 3G</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync apps</td>
<td>GP</td>
<td>Do not use – has no effect</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync app settings</td>
<td>GP</td>
<td>Disables roaming of app data</td>
<td>Desktop</td>
</tr>
<tr>
<td>Do not sync start settings</td>
<td>GP</td>
<td>Do not use – has no effect</td>
<td>Desktop</td>
</tr>
</tbody>
</table>
Figure 2 shows the settings on the user's computer.

The categories of Windows settings that sync include:

- Theme (desktop theme, taskbar settings)
- Internet Explorer settings (recently opened tabs, favorites)
- Passwords (Internet passwords, Wi-Fi profile)
- Language preferences (keyboard layouts, system language, date and time)
- Ease of access (high contrast theme, narrator, magnifier)
- Other Windows settings (notification settings, spelling dictionary)

Figure 2. Settings for Enterprise State Roaming.

To deploy, simply enable the feature for the tenant. From then on, settings are backed up automatically. Management and monitoring services are available in the Azure Portal with menu-based settings. Applications that have their own sync solutions are not affected. We completed our internal deployment without users escalating a single helpdesk ticket, which made it a very smooth operation.

Summary

With Enterprise State Roaming, our employees enjoy the ease of adding a new device to our network. They also appreciate that their business settings and personal settings are separate, for improved privacy. Along with a simple deployment process, the Azure portal helps us efficiently manage and monitor settings. We encourage you to see what Enterprise State Roaming can do for you!

For more information

Microsoft IT

microsoft.com/ITShowcase

© 2016 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.