# Laptop Configuration

A book walking you through how your laptop is configured, managed and what restrictions are put in place.

# Single Sign On (SSO)

# Overview

Single sign-on (SSO) has been configured to reduce the number of sign-ins staff need to make throughout their day. SSO is a technology that allows you to sign into multiple services without entering a username or password. SSO authenticate you via a token created on your laptop during sign-in that allows you to sign-in and access other services without any prompts.

The following services currently support SSO:

- Accessing Microsoft 365 via Google Chrome or Microsoft Edge.
- Logging onto LiquidFiles through the web browser.
- IT Support documentation.

Below are instructions on using SSO.

# Microsoft 365 via Web Browser

When working off your assigned laptop, open Google Chrome and browse to https://portal.office.com. You'll be automatically logged into your Microsoft 365 account.

# LiquidFiles

Browse to https://transfer.georgeandbell.com using the Google Chrome web browser. Rather than sign-in using your username and password, press the **SSO Login** button. You will be automatically signed into your account.


Email

Password

Login

Remember me for two weeks

Password Reset

SSO Login

# Periodic Sign In Requests

Due to the interaction between Microsoft and Duo, you'll be periodically prompted to re-sign into your Microsoft 365 account. This is occurring when a window appears in the middle of your screen (uninitiated) asking that you complete a Duo Push Request.

Completing this Duo Push Request will complete the process, after which you will not be prompted for another few months.

# Scheduled Maintenance

Scheduled Maintenance

# Windows Updates

Windows update is a service that runs on your laptop which installs any updates released by Microsoft typically on a monthly basis. Installing Windows updates is important as it helps keep George & Bell's infrastructure secure against outside threats.

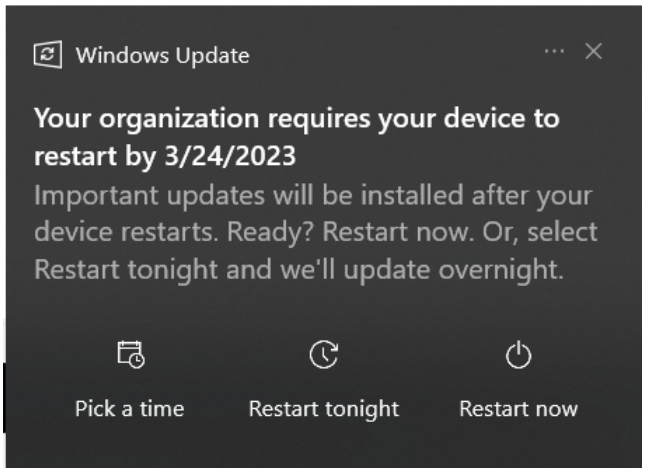
## Update Schedule

Cumulative Updates are released by Microsoft on every second Tuesday of the month. These updates include patches to newly found vulnerabilities and small system improvements. These updates will be deployed to all laptops one week after general public release.

Feature updates which consist of large overall improvements or change to the Windows OS are released every six month by Microsoft. These updates are automatically installed onto your laptop after 3-6 months of general public availability.

## Receiving Updates

Each month your laptop will prompt you asking to install the latest round of updates. Below is what you will see within the bottom right-hand corner of the screen when a update is available.




For the first seven days after the initial notification, Windows Update will only prompt you to install the updates when convenient. After seven days, Windows Update will become more forceful and ask that you install the update immediately or have it scheduled to install, however you'll still be able to defer the update for another three days (14 days in total). After the three days have elapsed, you will be forced to install the update.

Scheduled Maintenance

# Application Management

Laptops are managed and updated via a cloud-based service called Microsoft Intune. This service is integrated into Microsoft 365 ensures all laptops have a consist set of update-to-date applications for employees to use.

## Update Schedule

Below is an outline of how often each application is updated within the organization and if the application requires your input.

> All applications which are not continuously updated are manually tested before release.

| Application Name | Update Period | Installation Type |
|---|---|---|
| 1Password | Continuous* | n/a |
| Google Chrome | Continuous* | n/a |
| Mozilla Firefox | Continuous* | n/a |
| Microsoft Office | Continuous* | n/a |
| Microsoft Teams | Continuous* | n/a |
| Adobe Reader DC | Monthly | Prompt Always |
| Zoom | Monthly | Silent |
| Cisco WebEx | Monthly | Silent |
| 7-Zip | As Required | Silent |
| Duo Authentication for Windows Logon | As Required | Silent |
| LiquidFiles Outlook Plugin | As Required | Prompt If Necessary |
| WinTech ProVal | As Required | Prompt If Necessary |

| | | |
|---|---|---|
| Fortinet FortiClient | As Required | Prompt If Necessary |

* Updates are taken care of by the application itself and are not managed nor initiated by the IT department. At times IT may force an update however.

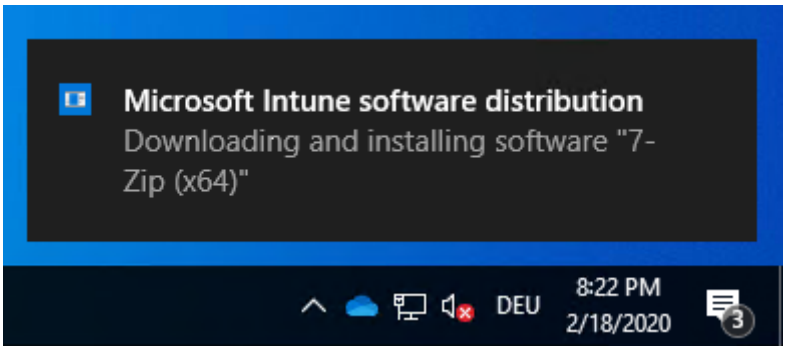
## Installation Types

How an application updates varies based upon a couple different factors including how often its used and how long it takes to install. Below are the different ways an application can perform its update.

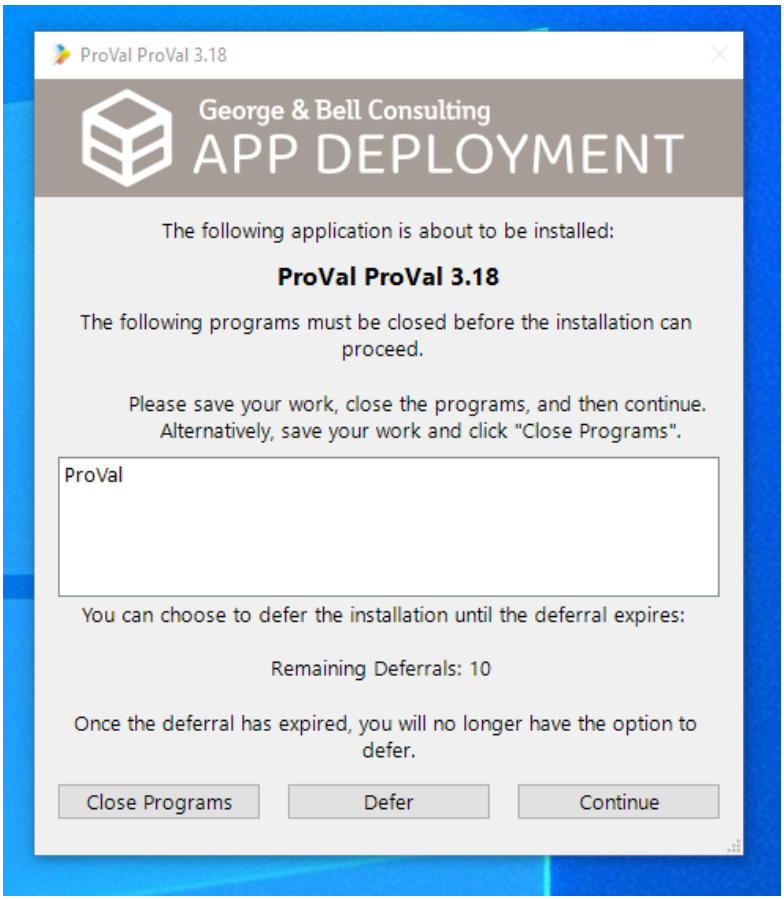
| | |
|---|---|
| Silent | Updates will always be installed in the background without causing any interruption. |
| Always Prompt | Updates will always prompt you prior to installation. |
| Prompt If Necessary | Update may prompt you but only if required to do so. Typically this means that the update will install silently in the background, unless you are actively using the application. |

# Update Process

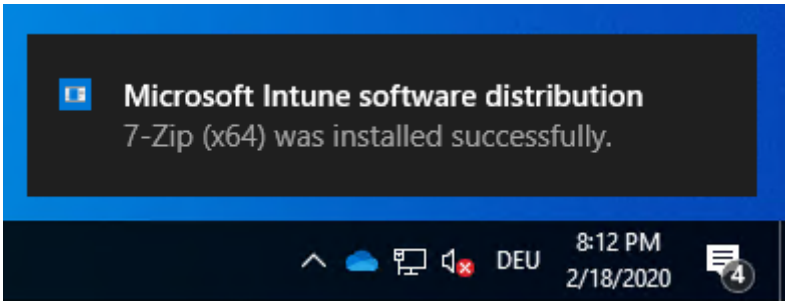
When an application is deployed to your laptop, you will see an series of notifications as the installation progresses. The first notification will inform you that the installer is being downloaded to your laptop (shown below). Once complete, a second notification will appear indicating that the installation is in progress.




If the update process determines that you have an application open that needs to close, a prompt will appear asking that the conflicting application be closed. You will also be given the option of deferring the update/install if desired. If deferred you will not be prompted again for a period of 24 hours. In most cases you can defer the installation three times, after which you'll be forced to complete the installation.




Once the installation has successfully installed, a third and final notification will appear.




# FAQ

**What happens if the application fails to install?**

You can safely ignore the message (unless its impacting you) as IT support will be notified of the failed update. If required, IT support may reach out to resolve the issue.

**After deferring an update, I received a notification saying that the update failed. Is this ok?**

This is expected. When you defer the application, Microsoft Intune's doesn't understand the difference between a deferred update and a failed update so a failed message is displayed. In either case, Microsoft Intune will reattempt the update in 24 hours.

**How long does a deferral last?**

Microsoft Intune's will wait 24 hours before trying the update again.

**I received a prompt for an application that wasn't open. I thought it would install silently without prompting me?**

At times IT may deploy an update forcing a prompt every time. This is usually done if the update takes a considerable amount of time and there is concern that  the laptop may be accidentally shutdown during the updating process.

**Can you force an update to be installed at a certain time?**

Unfortunately not. Every laptop checks in with Microsoft Intune on initial sign-in and every 8 hours there afterwards. Its during these times that updates will be installed. IT has no control over this process.

**Can I force an update to occur?**

Not directly. You can if you wish, force a synchronization with Microsoft Intune. If an update is available, it *should* install shortly after the synchronization. To force an synchronization:

1. Open **Settings** via the Start Menu.
2. Select **Accounts**.
3. Within the left-hand column, select **Access Work or School**.
4. Select **Connected to GBC AD Domain**. An Info button should appear. Select **Info**.
5. Under *Device Sync Status*, select **Sync**.

**I have an application that isn't listed that I think should be included in the regular updates?**

Please let us know and we'll look into adding it.

# In-Place Restrictions

# USB Restrictions

To eliminate the possibility of having a laptop be compromised via Removable Storage Media such as a USB flash drives or external hard drives, Removable Storage Media will not be accessible if plugged into your laptop.

Removable Storage Media consists of the following types of devices:

- USB Flash Drives
- External Hard drives
- Memory Cards
- Digital Cameras
- Smart Phones (charging is not affected)

# Exception

If you require access to a USB flash drive or other Removable Storage Media device, please contact IT Support as exceptions can be given on a case-by-case basis.

# Administrative Rights

To protect against privilege escalation if a laptop were to be compromised, your user account does not have administrative rights and as such cannot perform administrative functions such as:

- Installing/updating software.
- Changing system settings.
- Installing device drivers.

Privilege escalation is is when a hacker has gained access to your account on your laptop but does not yet have full system access. In these situations the hacker will attempt to find a vulnerability, secondary account or other method to gain full system control. Once achieved they can use your device to perform further compromises deeper in the network on more sensitive targets.

## Requesting Assistance

If you require administrative access, please reach out to IT Support for assistance. IT Support will perform a quick remote session on your laptop and perform the administrative request on your behalf.

> At times prior approval from the partners may be necessary before the request can be fulfilled.