



ICT UNIT NEWSLETTER



ICT CATCHUP

SPLASH PAGE

The ICT Unit has recently implemented a splash page: a second layer of authentication when trying to access the local network. After putting in a password, the page on the left will open up on your device's browser. You will have to provide your username, ie: yourname.surname and password before you will be able to access the local network and internet



ONESTOP PAGE

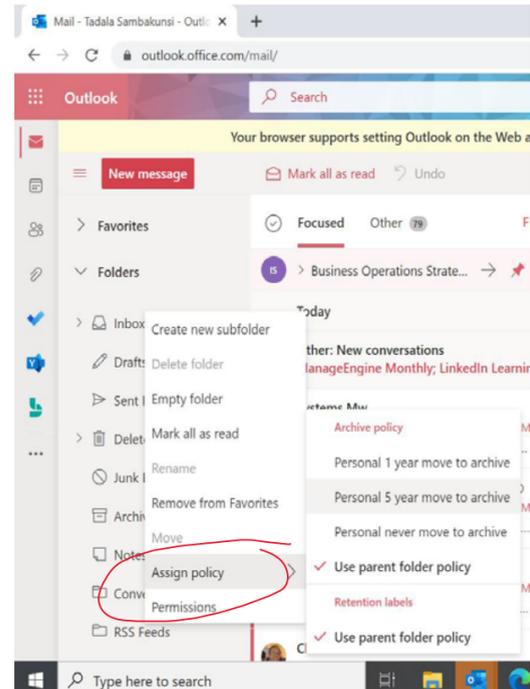
In a bid to increase work efficiency, The ICT unit Has developed the onestop page. This ia a page that pops up soon after authentication from the spashpage. This page has useful links used in day to day work, quick access to updates and trainings happening around the office and digital display.

<http://196.11.84.84>



ICT TRAININGS

How to use the Archive Policy in Outlook

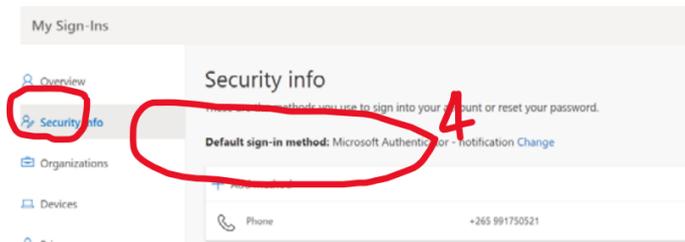
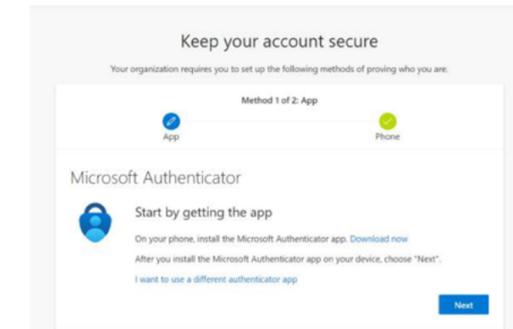


Users can choose an archive policy for each folder on a primary mailbox to move emails into an archive mailbox. To do this:

- Access Outlook Web App (OWA) (login to cloud.undp.org)
- Right-click a folder
- Select "Assign Policy"
- Choose a policy that you wish to apply

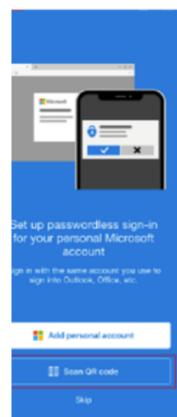
Setting up MFA

- Open your browser and go to <https://mysignins.microsoft.com/> and sign in with your undp email address



Go to security info. If you have your phone number set up already, it will appear as in the screenshot. You should add another authentication method as a backup, in case your phone number cannot be reached. To do that, click on Add Method

- Download the Authenticator app on your phone through play store on android and apple store on iPhone. Once you have downloaded the app, click Next. Open the app on your phone and choose to add an account by through the option Scan QR code and scan the QR code on your computer screen. If you cannot use your phone camera, you will have to manually enter the 9-digit code and the URL. Your account will be added to the authenticator app automatically



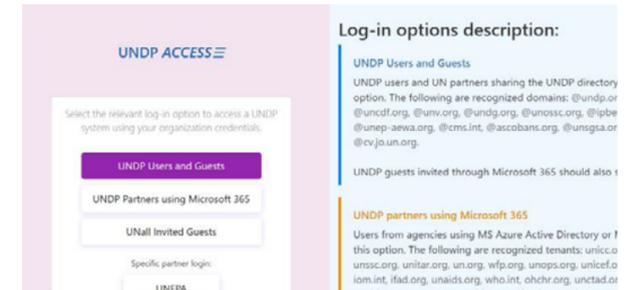
- You will receive a notification on your mobile device. Tap Approve. You have now added the second way of verification. Set the authenticator app as the default sign in method.



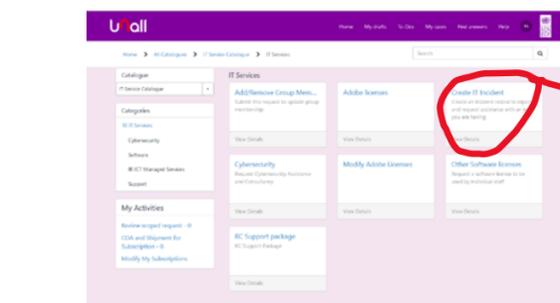
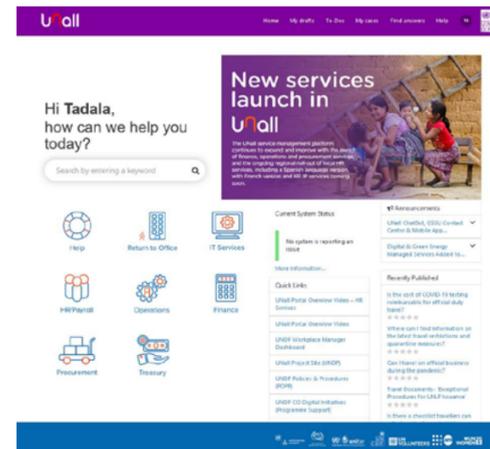
UNALL is a helpdesk for all corporate IT products and Services. If you have an issue with one of UNDP's corporate systems or services, including Atlas (now known as Quantum), office 365, DocuSign, etc.. you need to submit a Global Helpdesk request through Unall portal using the "Create Incident" service as shown below;

<https://undp.service-now.com/unall>

- Follow the link above and you will be taken to this page. Select UNDP Users and guests, you will be asked to sign in with your UNDP email address



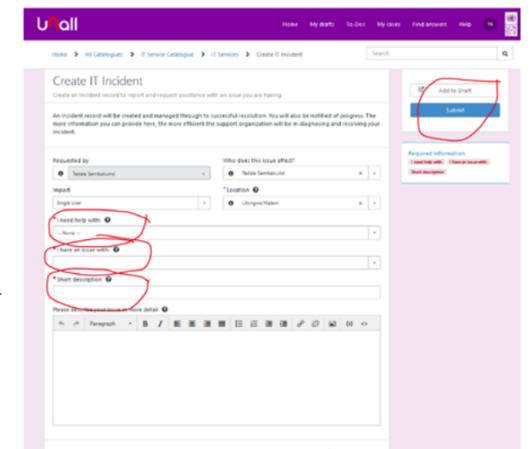
- When logged in, you can choose the service you would like to lodge a complaint about. Click on IT services to report issues related to DocuSign, Atlas, Office 365 (outlook, word, excel, powerpoint, etc..)



When logged in, you can choose the service you would like to lodge a complaint about. Click on IT services to report issues related to DocuSign, Atlas, Office 365 (outlook, word, excel, powerpoint, etc..)

- Your view may be different depending on the rights given to your username. To report an issue, click on Create IT incident

- You will then be given a form to fill to describe your issue. The I need help with section, you will select the problem area (atlas, applications, devices, communications and collaborations for emails or local applications). Then you will select a more specific area under I need help with and then give a short description of your problem. If you need to enter more details of your problem, a textbox and attachment section is provided for you. Then click Submit and wait to be helped!





IT BEST PRACTICES

Unnecessary Application/Services

If a service is not necessary for the intended purpose or operation of the device, that application/service should not be running

Be careful releasing your email address, and know how it will be used

Every time you communicate on the Internet or browse a website, there are opportunities for spammers to intercept your communications to obtain your email address and other personal information. Otherwise reputable companies may sell or exchange your email address with other companies, and this information may eventually find its way to a spammer. Consider the following guidelines:

Subscribe only to essential discussion lists, and ensure that they are moderated.

Think twice before offering your email address to a website. Check the privacy policy for that site.

Remove data securely

Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system.

Do not click random links

Do not click any link that you can't verify. To avoid viruses spread via email or instant messaging (IM), think before you click; if you receive a message out of the blue, with nothing more than a link and/or general text, do not click it. If you doubt its validity, ask for more information from the sender.

Be proactive

Adjusting the security settings in your web browser is a good preventive measure. For a higher level of security, have your browser disallow accepting cookies, Listing your name and other personal information in your browser profile, filling in form fields for you.

This will help reduce the amount of personal information transmitted to sites at the expense of full functionality, since many legitimate websites require you to accept cookies.

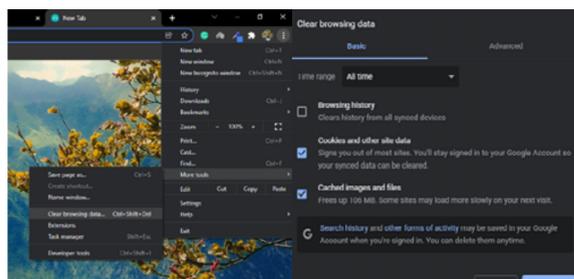
○ Ensure that you have adequate backups of your files. Copy them to a portable storage device like USB drives, and store them in a secure location. Pay particular attention to making backups of your personal data files.

○ NEVER give your password, account numbers, or other sensitive personal information (name, address, phone), or your Internet Address or machine name, out in an e-mail message, newsgroup posting, or in a chat session. Your information can easily be intercepted, forwarded, or redirected without your knowledge, and you really have no way of knowing who is listening in a chat room.

○ NEVER give away sensitive or private personal information on a web page until you trust the company hosting it. Build trust by reviewing the company's privacy and security policies on their web site, and by insisting on a secure connection (look for the closed lock or a key in the lower corner of your browser window). Know what their policies are regarding reuse, sharing or selling your personal information.

○ Never execute or click on a program (e.g., an ".exe") file if you do not know what it is/does, or if you do not trust the source. This is particularly the case for file attachments that are sent to you via e-mail, or are downloaded from a web site that you do not trust.

○ Consider clearing your web browser's cache storage file after visiting web sites where you entered sensitive information, such as a credit card number, or a bank or brokerage account and password, as this information is often stored in your browser too. (Do you select "remember this password" for ease of use in your browser?) If your machine is broken into, account information in your cache files could be used for fraudulent activity or identity theft. While Using Chrome, select the three dots on the top-right, select more tools, then clear browsing data. Select cookies and other site data, then clear, as shown below



DID YOU KNOW?

With your UNDP email, you can use the following Microsoft 365 Applications

- **Microsoft Forms** is a tool that allows users to quickly create quizzes, surveys, questionnaires, and registrations. Data can easily be transferred to excel or built-in data analytics such as Power BI to visualize it and use for further actions.
- **Microsoft Sway** is a presentation program. Content can be pulled locally or from an Internet source directly. Another integration service of Sway presentations include YouTube or Facebook content.
- **MyAnalytics** shows how people spend their time and who they spend it with the most. MyAnalytics is a private dashboard that analyzes work habits.
- **Microsoft OneNote** is an application to gather handwritten or computer typed notes, drawings and audio commentaries. The note taking program makes it possible to easily share the notes with other OneNotes users. It is also perfect for note taking on-the-go.

NEWS AND UPDATES



In the current business environment, many enterprises face Mobility challenges. The work requires that employees have endless accessibility and mobility. They don't want their work to be limited to their desk. They want to be Productive across a variety of devices with constant access to the applications that they need. To this end, Microsoft has upped its Cloud Service portfolio with the inclusion of Microsoft Endpoint Manager aka Microsoft Intune to enable and empower Businesses to leverage mobile device management, mobile application management, and PC Management capabilities. By using Office 365, organizations can provide the employee's access to Data, Resources, and corporate Applications from virtually anywhere to almost all devices, whilst ensuring that the data remains safe and secure.

Microsoft Intune is a cloud-based unified management solution for mobile devices and operating systems. The aim is to protect the corporate data on both corporate and BYOD equipment. The Microsoft solution includes the services and tools you may use to manage and monitor mobile devices, desktops, laptops, etc.

UNDP is implementing Intune globally starting this December, as for Malawi CO we will enroll all UNDP computers and office mobile phones starting first week of January 2022.

Reach out to the IT Team



Victor Msiska
ICT Analyst
Mobile: +265 999 671 209
Email: victor.msiska@undp.org



Tadala Sambakunsi
ICT Associate
Mobile: +265 991 750 521
Email: tadala.sambakunsi@undp.org



Thomson Thom
YP-ICT
Mobile: +265 882 406 903
Email: thomson.thom@undp.org