Luxoft
A DXC Technology Company

Instruction for new joiners, GL-10-1-38-0-LUX-(ENG)

Quality Management System

Useful links

Corporate System:

Service Desk

MyHome

Outlook Web Access

List of abbreviations and terms

Corporate	Luxoft Company
Luxoft	Luxoft Company
MFA	Multi-Factor Authentication
OATH	Open Authentication
OS	Operating System
SD Request	Service Desk request
VPN	Virtual Private Network

Description

The purpose of this document is to provide instructions for new employees on how to log in to their computer (Windows, Mac, Linux) and account, set up MFA, and connect to VPN. This guide is designed to help new employees quickly set up their work computer and gain access to necessary tools and resources. The document includes detailed step-by-step instructions and screenshots for clarity

NOTE: We recommend you use these instructions in the following order:
1. Account setup and password change
2. Setting up an MFA
3. Initial device setup (depending on the operating system of your device)
4. Setting up and connecting to a corporate VPN

Accounts

By default, each user has two accounts: Luxoft and DXC. The passwords of these two accounts are not synchronized.
You can find your account credentials in the e-mail which was sent from your manager to the personal e-mail address you provided to HR.

These accounts are needed to access different systems.

Luxoft account

- To log in to the computer (Windows/macOS/ Linux);
- VPN authentication;
- Luxoft applications (home, luxproject, servicedesk, etc.)

DXC account

- MS Office License;
- Outlook/Outlook Web;
- Teams/ Teams Web;
- OneDrive;
- SharePoint;
- Office.com.

Please use your Luxoft account to log in to the computer.
To get started, please follow the steps below to activate and finish setting up your account:

- **If you are in one of Luxoft's offices:** use the username provided and temporary password when logging in to your workstation.
- **If you are at a client's premises or working remotely:** please go to https://home.luxoft.com and use the credentials provided.

In both cases, a password change will be prompted during the first login. Please complete the first login and change the password you were provided with no later than 3 days after your first working day; otherwise, your password will expire, and your account will be locked.

Password complexity requirements

The minimum password length is 14 characters. The password must meet complexity requirements and include any combination of at least 3 following points:

- Uppercase letters
- Lowercase letters
- Digits
- Special symbols

It is strictly prohibited to:

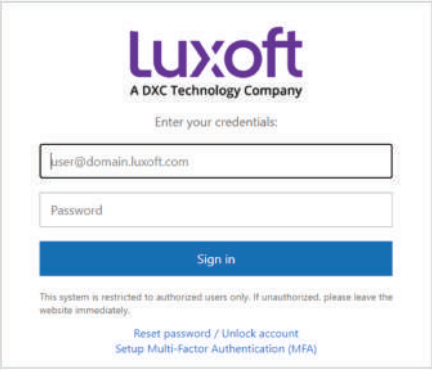
- Use the company name in a password
- Use your first or last name, date of birth, names of your relatives, names of pets, etc. as a password.
- Write the password somewhere and store it in a public place
- Disclose your personal access passwords
- Use your corporate domain account password on any public services. (Facebook, LinkedIn, Gmail, Yahoo, etc.)

Multi-Factor Authentication

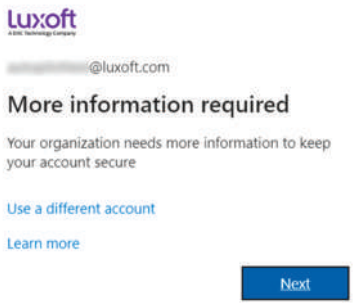
Mandatory action to increase Luxoft account security while connecting to corporate resources outside of Luxoft office – Multi-factor authentication. Configuration may be done at corporate or private device.

NOTE
We recommend the “Microsoft Authenticator” mobile application as a multi-factor authentication method, it is available for iOS and Android operating systems.

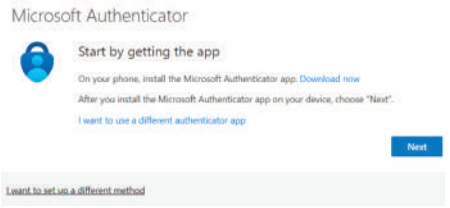
Multi-Factor Authentication registration



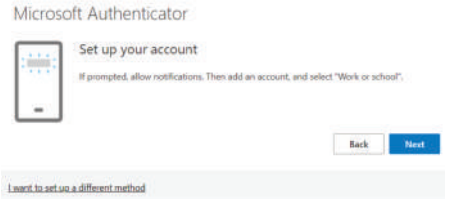
To begin setup, open any corporate resource on your computer, for example https://home.luxoft.com/
Login with your Luxoft credentials (format – user@luxoft.com) and then tap Sign in.



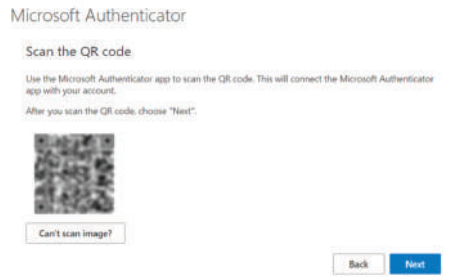
After that, you will be requested to add more information. To continue, click Next



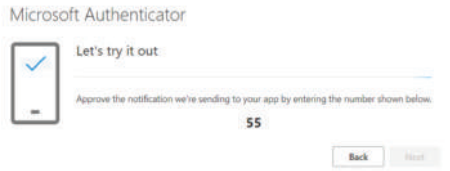
Microsoft Authenticator is the recommended method for MFA, but if you want you can also use another method, such as a third-party OTP application (for example, Google authenticator) or SMS code. If required, select “I want to use a different method” and choose the option that is most convenient for you.
Follow the instructions below to set up Microsoft Authenticator app. To use Microsoft Authenticator, click Next



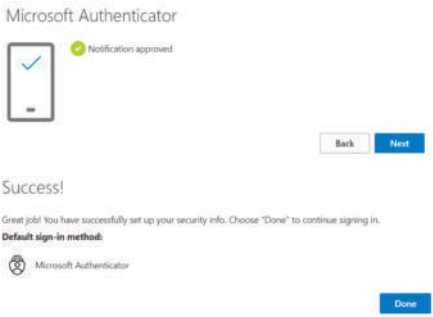
Download the Microsoft Authenticator app from an app store on your mobile device, allow notification for this app, and allow access to the Camera for scanning the QR code.
Open the Microsoft Authenticator app on your mobile phone, select "Add Account" and choose "Work or School.



Scan a QR code via your mobile phone and push next.



You will receive a push notification to your mobile device, enter the digital code from the wizard and approve the notification.



After making these settings, you have successfully registered an MFA using the Microsoft Authenticator application.

After you finish installing and configuring the MFA application on your phone, you need to set the secret questions. Security questions serve as an additional layer of protection for your Microsoft account. By enabling security questions, you can use them to verify your identity and regain access to your account in case you forget your password or encounter other login issues. To set up secret questions you need to click "Next", then select a question and add an answer to it.

Further, you can manage the MFA settings on this page: https://mysignins.microsoft.com/security-info

Using the Multi-Factor Authentication

Log in to your account on one of the corporate systems for example https://home.luxoft.com/.

Enter your username and password, then click "Login".

The page will display a code that you must verify in the Microsoft Authenticator application and you will receive a push notification from Microsoft Authenticator on your phone.

Make sure that the push notification information is correct.

Enter the one-time code from the page and confirm your login.

After that, you will be authorized into your account.

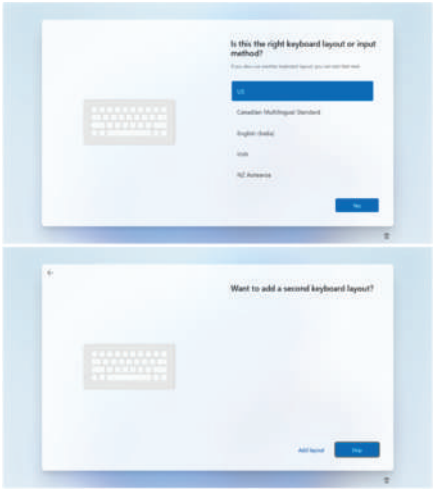
Initial Device Setup Guide for Windows, Mac, and Linux

In order to ensure a smooth start to your work, it is essential to complete the initial setup of your computer, including logging in to your work account and configuring necessary security measures. This guide provides detailed instructions on the steps required to access essential company tools and resources for Windows, Mac, and Linux devices, and will help prevent potential setup errors.

Please use the instructions according to the operating system of your computer.

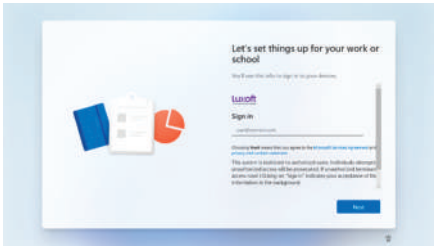
Windows

1. Turn on Luxoft PC.
2. Select the region and keyboard layout



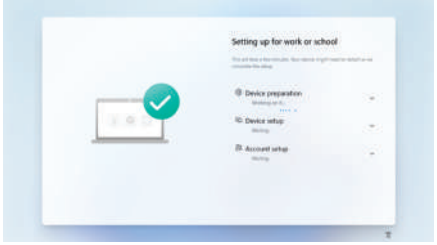
3. Connect to the network. Choose Luxoft Guest network if you're in the office or any other network with unrestricted internet access if you're not in the office (any Guest or home network).

4. Then enter your Luxoft data in format <username>@luxoft.com



5. You`ll then need to enter your Luxoft credentials in the corresponding format e.g., <username>@com.

6. Wait until all preparations are done to your PC. Don't turn it off or disconnect from the network. Make sure PC is being charged during the initial setup. It can take up from 30 minutes depending on network connection.
During "Device setup" essential applications will be installed, including a web browser, productivity tools, and a VPN client.



When all setup is completed, login to the laptop using Luxoft login and password. Luxoft login should be typed in format <username>@luxoft.com

Please note: some applications may take some time to load after you first log on.

After you make your first login, Windows will finish the account setup. **In 24 hours after the first login**, all necessary applications will be installed automatically.

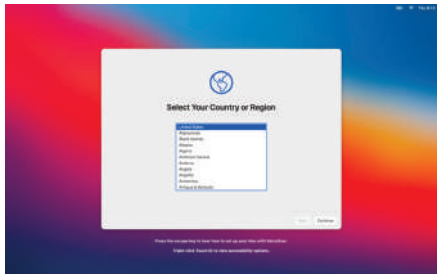
(Optional) If the laptop supports fingerprint recognition, Windows will offer to log in to the laptop using a fingerprint.

Setup PIN for entering the laptop. This PIN will be used only for laptop, for other applications it might now work.

Also, it may require to setup Multi-Factor Authentication if you have not done this before. Follow the "Multi- Factor Authentication registration" instructions in this document to do it.

Mac

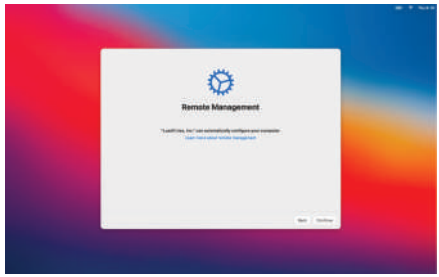
1. Turn on Luxoft PC.
2. Select Your Country or Region



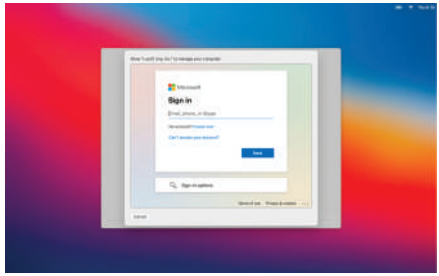
3. Connect to the network. Choose Luxoft Guest network if you're in the office or any other network with unrestricted internet access if you're not in the office (any Guest or home network).

4. Activation/Remote Management prompt – click Continue

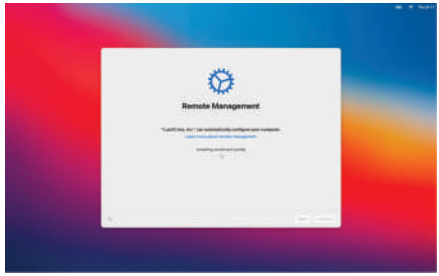
NOTE: Don't be surprised that Luxoft USA will set up your computer automatically, this is normal.



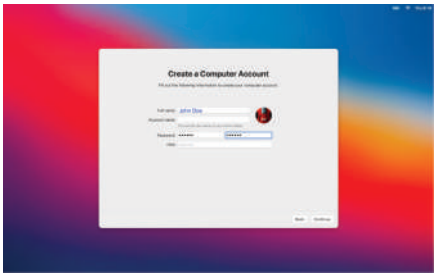
5. Enter your Luxoft credentials in the corresponding format: <username>@luxoft.com



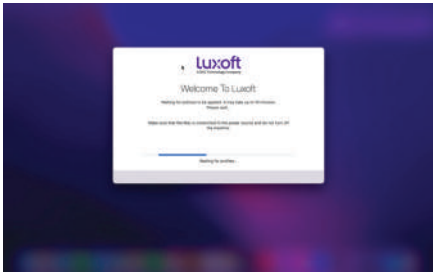
6. After logging in, the Installing configuration profile process will begin. Wait for the installation to complete, then click next



7. Create local account, later you will be asked to use a domain account instead. You can use your name and create your own password (it will be synchronized with your domain password later)



8. After that the Macbook setup is completed, the setup of corporate policies and software will begin automatically. It's not recommended to turn off the computer at this time. The process can take from 15 to 60 minutes depending on your Wi-Fi bandwidth

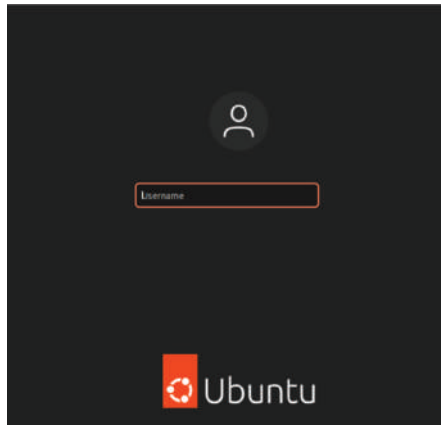


9. When the software is installed and all settings are prepared, you need to restart your Macbook. Proceed with a restart and your device is ready to use.

Also it may require to setup Multi-Factor Authentication if you have not done this before. Follow the "Multi-Factor Authentication registration" instructions in this document to do it.

Linux

1. Turn on Luxoft Linux OS device.
2. Enter the default encryption password, provided by the Helpdesk
3. You will be prompted for a username

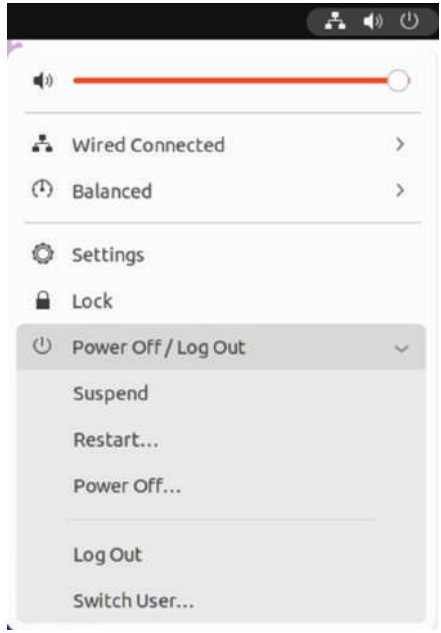


If you are logging in from the office or have logged in before, you can log in directly using your Luxoft account username and password.
*without the "@" symbol, in lowercase - it should be **"username"** and **not** - UserName@luxoft.com

If you haven't logged in before with your Luxoft account and you are outside the office (for example, working remotely), you must first log in with the **"emergency"** user using the password provided to you by the HelpDesk."

4. Next, you should connect to the VPN (as described in paragraph **VPN**).

5. After connecting, you should log in with your credentials, as described before. Using the "Switch user" option, without disconnecting from the VPN. The next time, you can log in as usual.



Also it may require to setup Multi-Factor Authentication if you have not done this before. Follow the "Multi-Factor Authentication registration" instructions in this document to do it.

VPN

By default, all employees have access to a VPN. A VPN is needed to access the Company network and internal business applications.

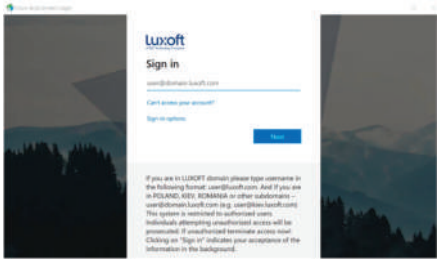
Please use the following instructions to set up and connect to a Company VPN.

Cisco AnyConnect Secure Mobility Client

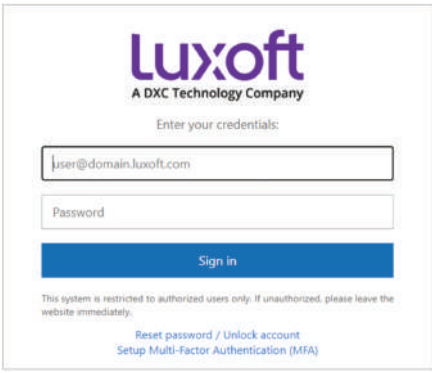
1.Look for the **Cisco AnyConnect Secure Mobility Client** application on your device (Windows, Mac, Linux) and open it (it is preinstalled application on all Luxoft computers).

2. Fill in an empty field with Luxoft VPN gateway: luxoft.com and click “Connect”.

NOTE: The following screenshots show an example of the process of connecting to a VPN for Windows devices The connection window may look different on different operating systems, but **the process is no different**

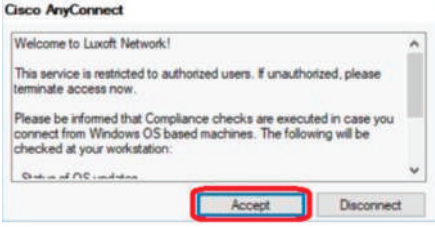


3. In the opened window, enter your login and domain name – login@luxoft.com, and click the “Next” button



4. In the next window, enter your domain password

5. After logging into your account, you will receive a notification on your phone from the "Microsoft Authenticator" app. Approve your login to Luxoft network in "Microsoft Authenticator" app.



6. After confirmation, the information banner will be shown on your device, read it and click "Accept".

After that you will be successfully connected to the corporate VPN and you will have access to corporate resources

Additional information

In case of issues at any of the steps you can request support from our HelpDesk team.
You can create a support request in any available way:
Submit a request in the corporate system — Service Desk
Send an email (even from your private mail address, but please provide your name and surname) — lux-sd@dxc.com / sd@luxoft.com / servicedesk@luxoft.com
Call our technical support (English language speaking specialists):

— Brazil	+55 11 4680 2740
— Bulgaria	+359 2 904 3977
— Germany	+49 711 490 480 77
— India	+91 80 6934 9677
— Italy	+39 11 1874 6177
— Malaysia	+60 4 287 9977
— Mexico	+52 3 33 001 9537
— Poland	+48 12 211 0677
— Romania	+40 21 655 0507
— Serbia	+381 11 696 3077
— Singapore	+65 6511 4177
— Sweden	+46 31 357 7777
— Switzerland	+41 41 726 4577
— Ukraine	+380 44 481 2937
— United Kingdom	+44 203 818 3877
— USA	+1 347 809 6077
— Vietnam	+84 28 3965 1777

We will do our best to resolve your issues as soon as possible so that you can continue your work without any obstacles.

List of changes

Approval date	**Version**	**Subject of change**	**Issued by**
08.05.2023	1.0	Document created.	Viktor Kustov/Ene, Razvan Costin