



LABS GUIDE

Getting Started

ABSTRACT

This document provides attendees with instructions on how to create an M365 with Microsoft Defender for Endpoint demo tenant.

James.Graham@microsoft.com

Microsoft Defender Masterclass

Getting started with Labs.

Pre-requisites

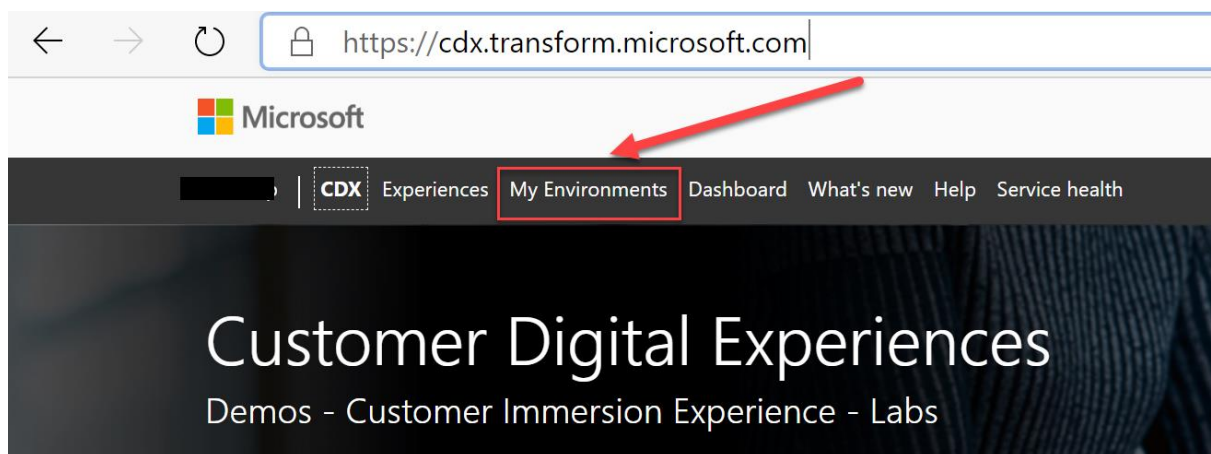
You must have access to Partner Center to complete these labs.

- Partners are required to be enrolled with the Microsoft Partner Center <https://partner.microsoft.com> to access the site. If your organization is not enrolled with Microsoft Partner Center, you will be unable to do these labs.
- If you previously had access to these tools, but cannot access them now, it is likely that your partner organization is not enrolled with the Microsoft Partner Center. Please enrol your organization at <https://partner.microsoft.com> for continued access to these tools.
- If you need further assistance, please review the information on the Partner Center <https://partner.microsoft.com/en-us/support/partner-center-help>

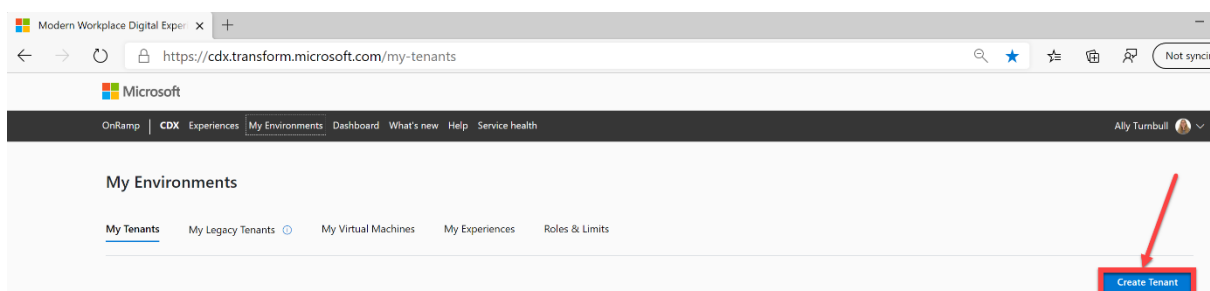
How to Create a new M365 Demo Tenant

Ideally this needs to be completed 24 hours prior to doing the LABS

1. Logon to <https://cdx.transform.microsoft.com/> You should use your partner email address and password that you use to connect to <https://partner.microsoft.com>
2. At the top of the page select My Environments Tab as shown below



3. Click Create Tenant



4. Fill in the details for the new tenant as below - This will start to create in the new tenant in the background.

5. Please make sure you select the Microsoft 365 Enterprise Demo Content with Microsoft Defender for Endpoint. Please note this will likely only be available as a 90 day tenant and limited to specific locations, e.g. North America, Europe.

Environments
Create a Tenant

Current Environment Limits:

1 Select type: Quick Tenant

2 Select period: 90 days

3 Select tenant location: North America

4 Select your content packs

Select your base content pack for your tenant. You will be able to request for add-ons after the tenant gets created

Microsoft 365 Enterprise Demo Content with Microsoft Defender for Endpoint

This environment is an option for Microsoft 365 Security demos. In addition to the standard Microsoft 365 demo content, it comes preconfigured with Microsoft Defender for Endpoint service, including dashboards prepopulated with data from a number of Windows 10 machines that were briefly onboarded to the environment. To experience the full demo, you'll be expected to onboard your own endpoints. Note: Due to high demands, this option may not be immediately available. If licenses alone will suffice, we recommend you opt for Microsoft 365 Enterprise with License-Only for Microsoft Defender for Endpoint.

90-day environment not eligible for extension (Specified Microsoft field roles may be eligible for extension to 1 year environment)

Create Tenant

6. Once it has been created you have your own demo tenant to complete the labs in as well as a place that you can use to demo the products to your customers or as a learning tool.
7. You will now be presented with a screen as shown below.

Tenant
M365x654906

Content pack: M365 Enterprise

Location: North America

Period: 90 day

Expiration Date: 8/11/20

Status: Completed

Content add-ons: No add-ons applied

Additional Content: No additional content has been selected

Notes

Admin Details

Password: 3ans3i390E

Admin name: admin@M365x654906.onmicrosoft.com

Email: admin@M365x654906.onmicrosoft.com

Copy this password into a safe location on your computer as you will need it to logon to the tenant

Copy this username into a safe location on your computer as you will need it to logon to the tenant

Tenant
M365x375290 [Edit](#)

Content pack
M365 Enterprise

Location
North America

Period
90 day

Expiration Date
Please check the [admin portal](#) for the expiration date

Status
Completed

Content add-ons
No add-ons applied

Additional Content
No additional content has been selected
[+ Additional content](#)

Admin Details
Password: 8LwDsh5JQH [Copy](#)

Admin name	Email	
admin@M365x375290.onmicrosoft.com	admin@M365x375290.onmicrosoft.com	Copy

User Details
Password: 8LwDsh5JQH [Copy](#)

User name	Email	
Adele Vance	adelev@M365x375290.onmicrosoft.com	Copy
Alex Wilber	alexw@M365x375290.onmicrosoft.com	Copy
Allan Deyoung	alland@M365x375290.onmicrosoft.com	Copy
Christie Cline	christiec@M365x375290.onmicrosoft.com	Copy
Debra Berger	debrab@M365x375290.onmicrosoft.com	Copy

[Show more](#)

The status will update to Completed once done”

8. This will now build your demo tenant in the background.
9. When this is completed please return to My Tenants. Whilst it is building you will see it tenant status as Processing.

Microsoft

OnRamp | CDX | Experiences | My Environments | Dashboard | What's new | Help | Service health

My Environments

My Tenants | My Legacy Tenants | My Virtual Machines | My Experiences | Roles & Limits

Your tenant name [Create Tenant](#)

If you did not take a copy of the credentials you can retrieve them here

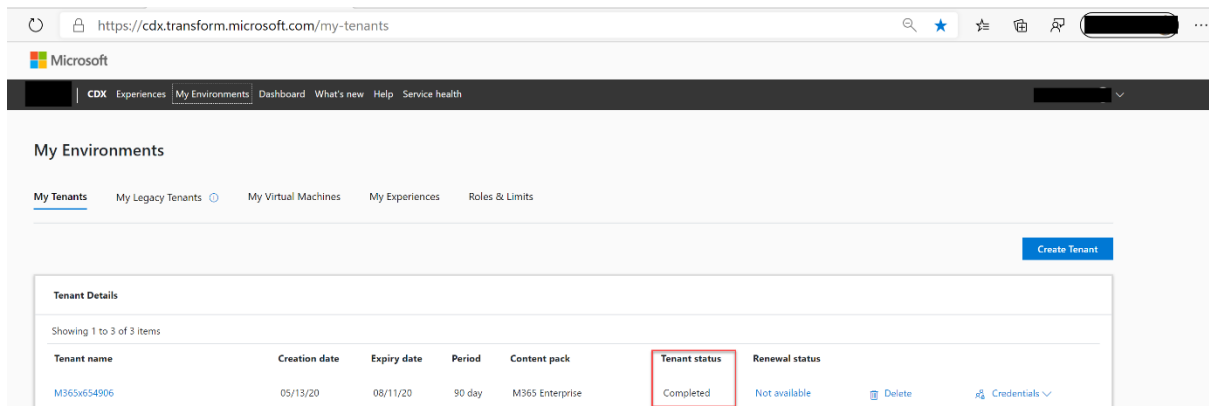
Tenant name	Creation date	Expiry date	Period	Content pack	Tenant status	Renewal status
M365x654906	05/13/20	08/11/20	90 day	M365 Enterprise	Processing Addon Pack	Not available Delete Credentials

10. When it's completed you will be able to use your tenant. It will look as show as below in the console. Make sure you have the correct content pack listed in the demo tenant. The Lite pack does not contain any content.

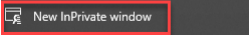
Content pack

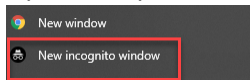
M365 Enterprise MDATP

M365 Enterprise MDATP Lite



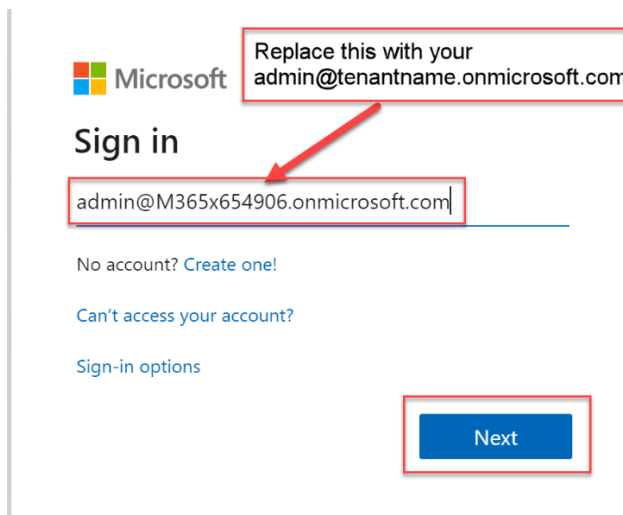
11. Next step is to logon to your tenant. You will need to do this for each lab.

a) Open an Inprivate browser (Edge)  or New in-Cognito (Chrome)



on your machine and then go to <https://admin.microsoft.com/>

b) Enter the admin account username that you saved in Step 6 into the sign in as below and click NEXT.



c) Enter the password and then click "Sign in".

CONTOSO demo

← admin@m365x654906.onmicrosoft.com

Enter password

Enter Password from the saved credentials

.....

[Forgot my password](#)

Sign in

Contoso

12. You are now logged onto the tenant successfully.

Generating Additional Microsoft Defender Alert and Incident Data

The new demo tenants come prepopulated with incidents and alerts, however you may wish to generate additional data.

Please follow this guide if you want to populate your demo tenant with additional threat data:

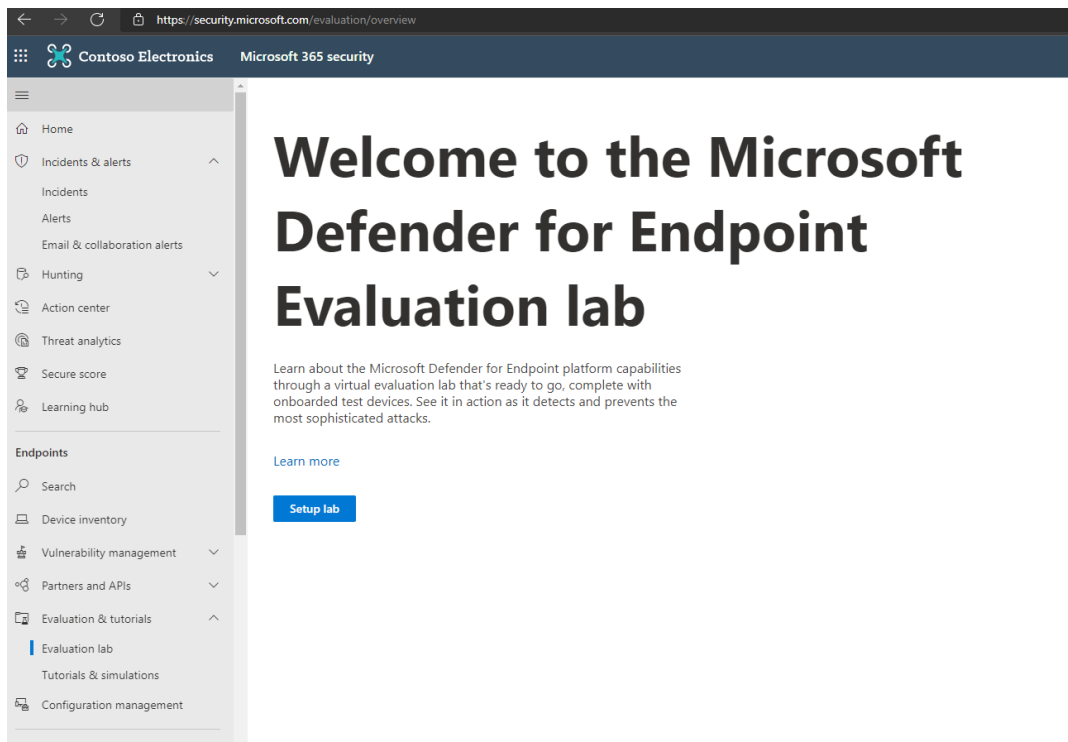
[Microsoft Defender for Endpoint evaluation lab - Windows security | Microsoft Docs](#)

Create some VMs for use in the lab, e.g. a mixture of Windows 10 and Windows Server - [Microsoft Defender for Endpoint evaluation lab - Windows security | Microsoft Docs](#)

Run attack simulations from a set of predefined scenarios on your lab VMs- [Microsoft Defender for Endpoint evaluation lab - Windows security | Microsoft Docs](#)

You also have the option to manually run simulations on the VMs if you wish - [Microsoft Defender for Endpoint evaluation lab - Windows security | Microsoft Docs](#)


The simulated scenarios will generate additional data in Microsoft Defender, thus providing a richer data set to run Advanced Hunting queries against.



Lab configuration

- ☒ Select your lab configuration
- ☐ Install simulators agent
- ☐ Summary

Select your lab configuration

 Please note, first set up can not be edited. [Learn more](#)

The following lab configuration options allows you to choose to run fewer devices for a longer period or more devices for a shorter period. Once the allotted time is met, devices are automatically deleted.

- ☐ 3 devices For 72 hours each
- ☐ 4 devices For 48 hours each
- ☐ 8 devices For 24 hours each
- ☒ 16 devices For 12 hours each

When you've used up these devices and need more, you can submit a request for more devices. Once you've selected the configuration, it cannot be modified. A deleted device can't be restored in any way and does not refresh the available test device count.

Next

Cancel

Lab configuration

- ☒ Select your lab configuration
- ☒ Install simulators agent
- ☐ Summary

Install simulators agent

Threat simulator details

Install threat simulation agents to safely run breach and attack scenarios on the evaluation lab devices. See the power of MDEP in action as simulated threats unfold. [Explore simulation gallery](#)

Microsoft privacy statement

Accept and provide consent to the statements

☒ Microsoft terms

Provide consent by accepting the Microsoft terms

☒ Microsoft information sharing statement

Provide consent by accepting the information sharing statement

Select vendors

 Note: You must first provide consent to the statements above to enable any of the simulators.

☒ AttackIQ

☒ License agreement accepted

AttackIQ Platform packages adversarial behavior including MITRE ATT&CK tactics, techniques, and procedures into a fully managed environment to help you continuously test and measure the efficacy of your security controls.

☒ SafeBreach

SafeBreach safely and continuously simulates real attack scenarios in production to enable security teams to discover, investigate, and remediate breaches and misconfigurations.

Email address *

admin@MSDx734648.onmicrosoft.com

Back

Next

Cancel

Lab configuration

- ✓ Select your lab configuration
- ✓ Install simulators agent
- **Summary**

Summary

You're all set! If you're happy with your chosen lab configuration, go ahead and complete the setup.

Lab configuration

16 devices For 12 hours each

Active vendors (2)

Name

ATTACK IQ

[Learn more](#)

SafeBreach

[Learn more](#)

[Back](#)

[Setup lab](#)

[Cancel](#)

When you are ready to use the lab to generate Alerts/Incidents – click on Add Device. This device will then be available for the time period based on the number of devices you selected above. E.g. If you selected 16 devices, each one is available for 12 hours once provisioned.

Your evaluation lab

Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender ATP capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.

[Overview](#) [Devices](#) [User Actions](#) [Simulations](#) [Report](#)

Device allocation

No provisioned devices

Provisioned devices are limited to 16 devices.

[Add device](#)

Simulations overview

Add simulations

[Create simulation](#)
[Go to simulations gallery](#)

Report overview

Provision some devices.
You'll never know until you try. Provision a few devices to start your evaluation.

Evaluation Highlights

Set up status: Completed

- Configuration**
16 devices for 12 hours
- Simulation integration**
2/2 simulators enabled [Edit](#)

Suggestions

- [Run simulations and tutorials](#)
- [Review incidents](#)
- [Hunt for threats](#)
- [Check for emerging threats](#)
- [Threat & Vulnerability Management data](#)
- [Provide feedback](#)

Add device

The lab only provides 16 test devices. Each device is only available for 12 hours. When these resources are deleted, no new devices are provided.

You have used up 0 of 16 devices.

Device type

Windows 10

Available Tools

The following tools are included in the device during provisioning. You can choose to exclude tools from being installed to reduce provisioning time. These tools are not required for threat simulators to run.

- ☒ Java Runtime
- ☒ Office
- ☒ Python
- ☒ SysInternals

Add device

A device takes around 10-15 mins to provision.

Your evaluation lab

Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender ATP capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.

Overview **Devices** User Actions Simulations Report

1 item + Add device									
Device name	OS Platform	Status	Simulator status	Time left	Risk level	Exposure level	Alerts number	Network	IP address
testmachine1	Windows 10	Setting up	Multiple		None	Low			

Once complete you will see the active device:

Your evaluation lab

Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender ATP capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.

Overview **Devices** User Actions Simulations Report

Device allocation

1 active device

Only 16 test devices are provided. Once provisioned, it is only available for 12 hours. Depending on your monthly allotted resource consumption you may be able to request for more devices.

testmachine1 11/12

[View full list](#)

Simulations overview

Add simulations

[Create simulation](#)
[Go to simulations gallery](#)

Report overview

- 0 Alerts in
- 0 Incidents
- 0 Actions taken in
- 0 Investigations
- 0 Key findings

[View full report](#)

You can now run a simulation against this device. Click on Create Simulation when ready (you can run multiple simulations during the time that the device is active for).



Create simulation

Select simulator


All

Select simulation

SafeBreach: Code Execution

Select device

testmachine1

 Missing a device? Check the Simulator Status in the device list to verify your selected simulator agent is installed.



Create simulation

The simulation will run and once completed will populate the tenant with associated Alerts and Incidents.

FAQ

Which browsers are supported?

- The latest Microsoft Edge released on January 15th 2020 is the latest supported browser for all applications within <https://cdx.transform.microsoft.com>. All Demos, Customer Immersion Experiences and Labs from <https://cdx.transform.microsoft.com> will adopt the latest Microsoft Edge browser as the supported version, and the Windows Virtual Desktop experiences will be updated. The Transform support team will address web browser related support requests by first asking to upgrade to the latest version of Microsoft Edge before attempting to troubleshoot. We encourage you to [download and install Microsoft Edge now](#). Read [Joe Belfiore's blog post here](#). Google Chrome also has been tested and confirmed to work with the <https://cdx.transform.microsoft.com>.

403 Unauthorised error accessing cdx.transform.microsoft.com

- Instead of logging into cdx.transform.microsoft.com try transform.microsoft.com

Authorisation issue logging on cdx.transform.microsoft.com

1. You must have access to Partner Center to complete these labs.
 - a. Partners are required to be enrolled with the Microsoft Partner Center <https://partner.microsoft.com> to access the site. If your organization is not enrolled with Microsoft Partner Center, you will be unable to do these labs.
 - b. If you previously had access to these tools, but cannot access them now, it is likely that your partner organization is not enrolled with the Microsoft Partner Center. Please enroll your organization at <https://partner.microsoft.com> for continued access to these tools.
 - c. If you need further assistance, please review the information on the Partner Center <https://partner.microsoft.com/en-us/support/partner-center-help>

Reached maximum capacity of 90 days when creating a tenant

- Try a refresh / logout / log back in again or create a different tenant that has e5 licences. Scroll down for the options

Something when wrong whilst creating your tenant

- This is due to high demand. Try and create a different tenant that has E5 licence or without an add-on pack or come back later to provision. Priority is always given to Paying customers so demo trials and tenants can often be affected when demand is high

How can I submit a support Request

- a. Navigate to Help
 - b. Select "Submit Request"
 - c. Complete form
 - d. Select "Submit"
- Launch will take you to the associated Experience card, with your customer(s) added
 - Click the Launch button from the Experience card

- Session will open with the remaining amount of time available

How can I renew my Tenants

1. Navigate to My Environments.
2. Locate the Tenant in My Tenants Details Table
 - *If available to renew:*
 - Select renew button on the summary screen, or within the Tenant details screen
 - Fill out the form
 - Select Submit
 - *If not available to renew:*
 - Navigate to Help section
 - Submit a ticket requesting a renewal

How do I create Virtual Machine

- Currently, creating a Virtual Machine is not available in the CDX portal, but is coming soon. Please contact support via a Support Request in the help section if you require assistance.

How do I create a Quick tenant

1. Navigate to My Environments
2. Select Create Tenant
3. Choose Quick Tenant from Type Selection

What Experience Types are available?

- **Customer Immersion Experience - with Virtual Machines** Utilize an Office Tenant to facilitate a session using a requested number of virtual desktops to share with customers.

Customer Immersion Experience - Tenant Only Utilize an Office Tenant to facilitate a session using a device kit with customers.

Lab Utilize a tenant and a virtual machine to learn how to configure and implement products and features in a hands-on environment.

Demo - Asset Only Access downloadable assets intended to demonstrate products or technology that a demo environment is not available for at this time.

Demo - With Virtual Machine Utilize a configured virtual desktop and a tenant to demo products and features.

Demo - Tenant Only Utilize a configured tenant to demo products or features.

What is the difference between demo tenants and a traditional Office 365 trial offer?

- Traditional Office 365 B4trial offer provides users a 30 day Office 365 E5 license containing 25-seats with no tenant content.
- Demo tenants provides users with licenses pertinent to the tenant type selected and also includes rich, demo-ready sample content (document libraries, emails, OneDrive contents, Yammer posts, etc.).

Is there a limit on the number of demo tenants you can create?

- Yes, there are limits in place for Partner users, regarding the number of active tenants a user is allowed to have:

Partner Users:

- One Year tenants: 1
- 90-Day Tenants: 5

How long does it take to provision a tenant?

- Standard Microsoft 365 tenants take approximately 12-48 hours (NOT including Add-Ons).
- Dynamics 365 tenants take approximately 24-60 hours.

How do I access a tenant after it's been created?

- Navigate to My Environments to locate your tenant. Use the provided credentials and log into portal.office.com.