Roadshow-WebexAmplify

Enabling Hybrid Work with ThousandEyes

Omer Ilyas

Table of contents

1. Lab

1.1 Overview - Enabling Hybrid Work with ThousandEyes

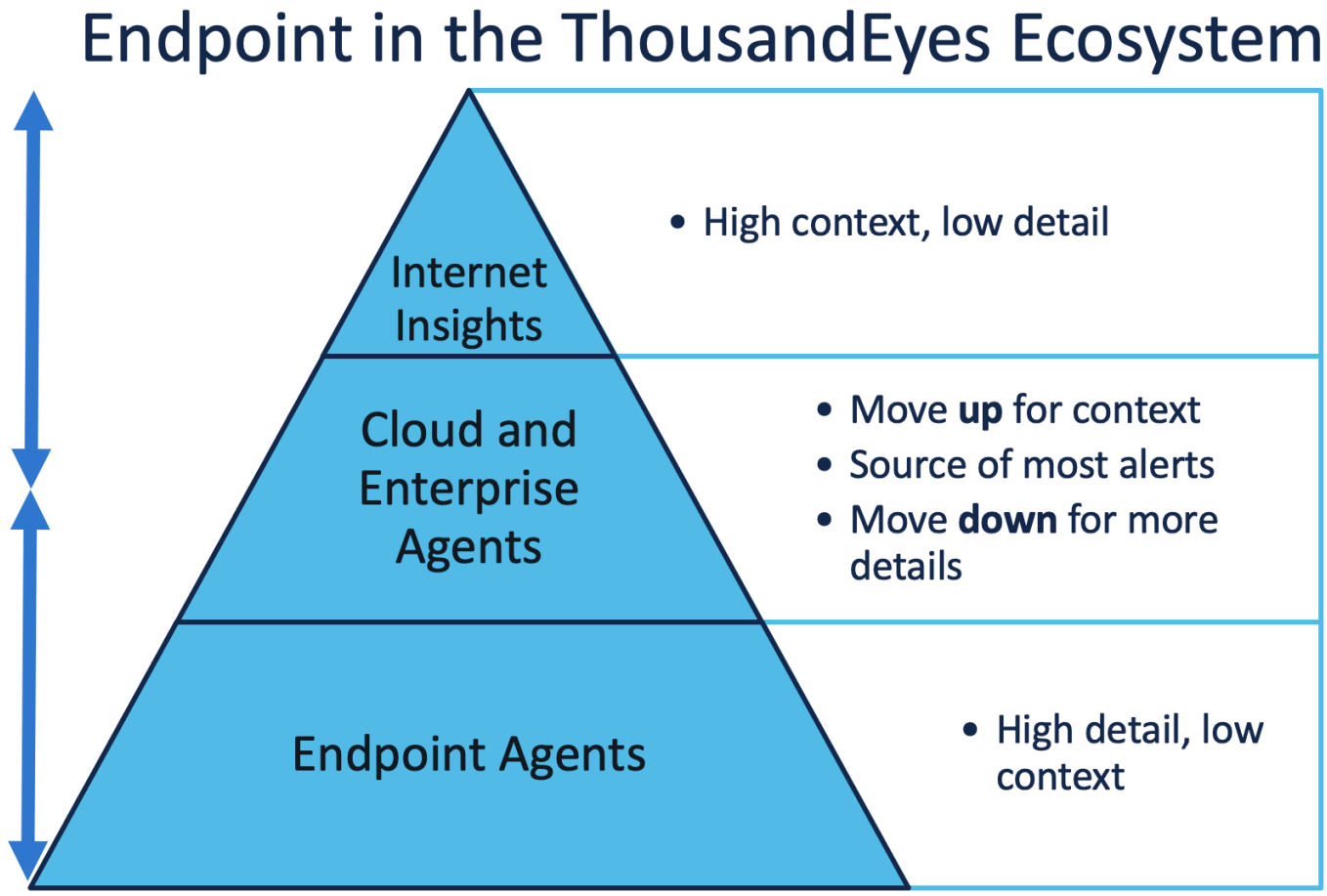
Work from the Office. Work from Home. Hybrid work has opened up the possibility of work from wherever the internet is available. At the same time, it brings new challenges to the IT team managing the end host's security, application performance, local network connection, VPN, proxy, and user's total digital experience. ThousandEyes provides this visibility with Endpoint Agents monitoring. In the lab, you will go through guided steps to start monitoring Endpoint hosts.

1.1.1 Upon completion of this lab you will be able to

- Deploy ThousandEyes Endpoint Agents
- Start monitoring SaaS services
- Learn how to enable Automated Session Testing (AST)
- Configure browser session monitoring
- Use the collected data for live troubleshooting
- Create a snapshot to share with others for colloboration
- Create/Duplicate a Hybrid/Remote Worker Dashboard

1.1.2 Prerequisites

- Understanding of ThousandEyes is helpful, but not required.



1.1.3 Disclaimer

Although the lab design and configuration examples could be used as a reference, this is a sample deployment, thus not all recommended features are used, or enabled optimally. For the design related questions please contact your representative at Cisco, or a Cisco partner or TME's.

1.1.4 Lab Overview - Enabling Hybrid Work with ThousandEyes

- Lab Login and Setup
- Quick ThousandEyes Overview
- Configure and Access the Lab Systems
- Deploy a ThousandEyes EPA
- Setup and Configure AST and EPA Monitoring
- Review Agent Views and Analyze Test Data
- Review Home Worker Dashboard and Alerting
- Wrap up and End the Lab

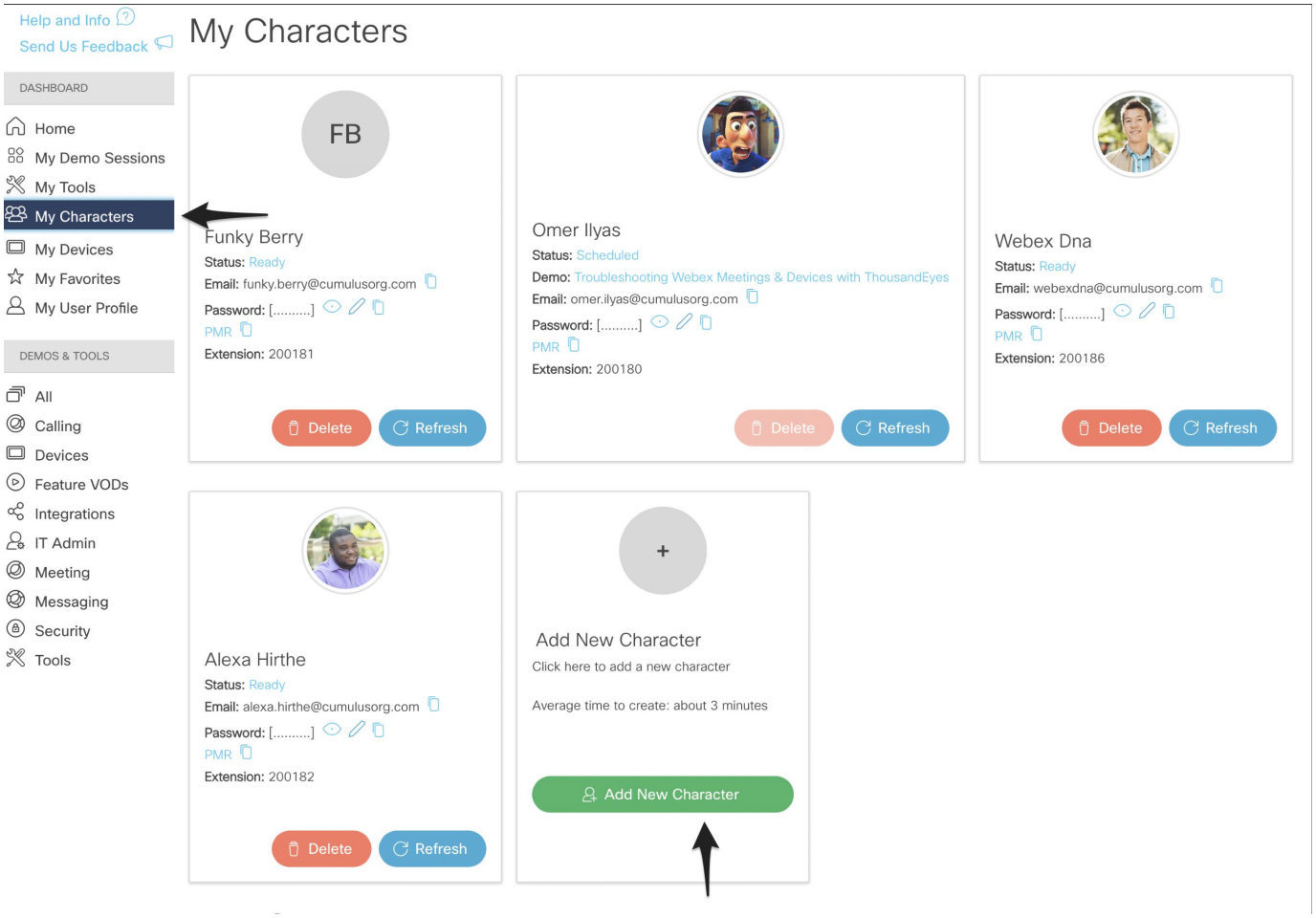
Let's get started! Click on Task 1 - Lab Login and Setup.

1.2 Task 1: Lab Login and Setup

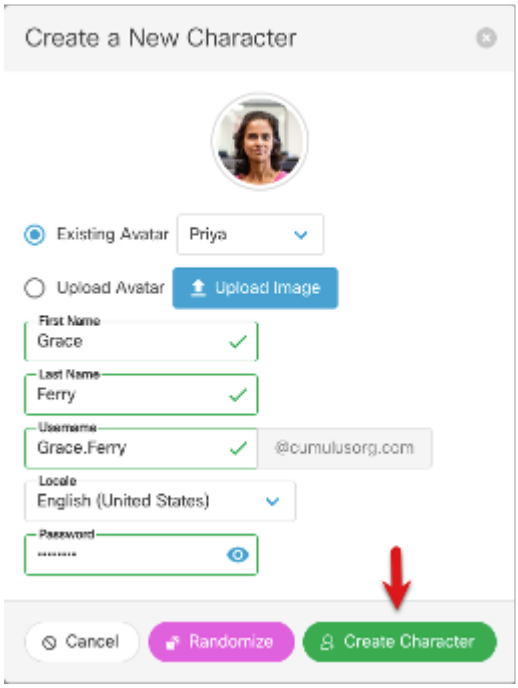
Click to access the lab

This lab requires a set of characters which will be aligned with roles to access ThousandEyes and Webex. **Optional** you can also register your Webex device on the platform that can be used with your demo.

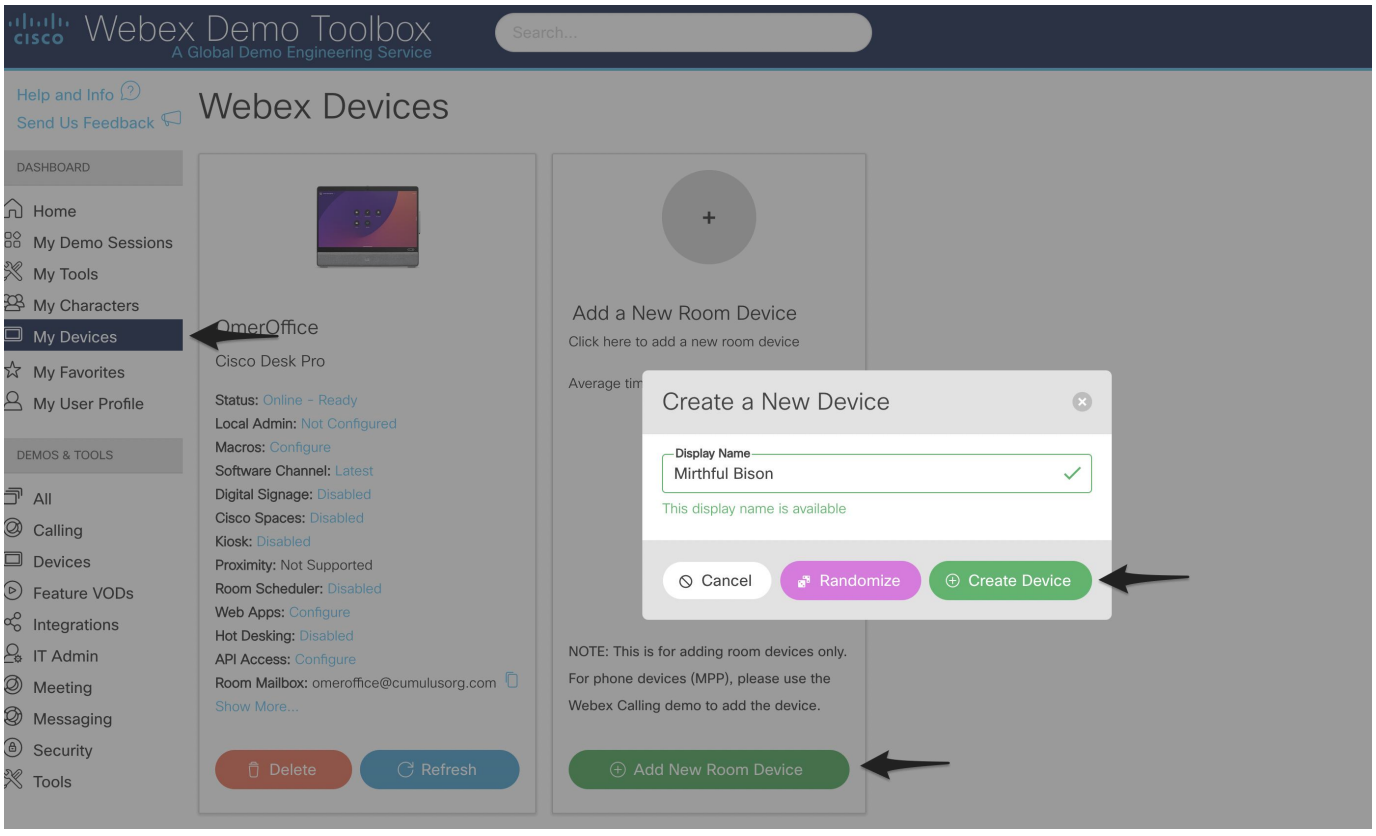
Click **My Characters** then click **Add New Character** as shown in the below image. You only need to create one character for the lab.



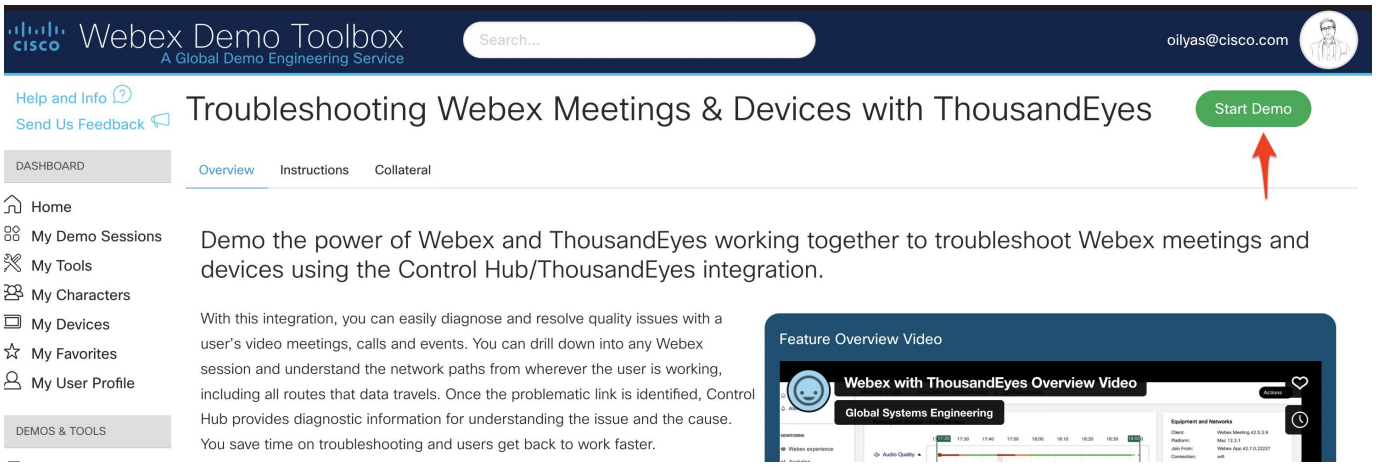
Click **Create Character**. Note (They will be randomly created so yours may not match the below screenshot. Also you have an option to modify the names as per your preferences.)



Optional Step Click on the My Devices tab, select Add New Room Device, if you want your device to be available in the demo and thousandEyes agent installed on your device. Please remember its an optional step.

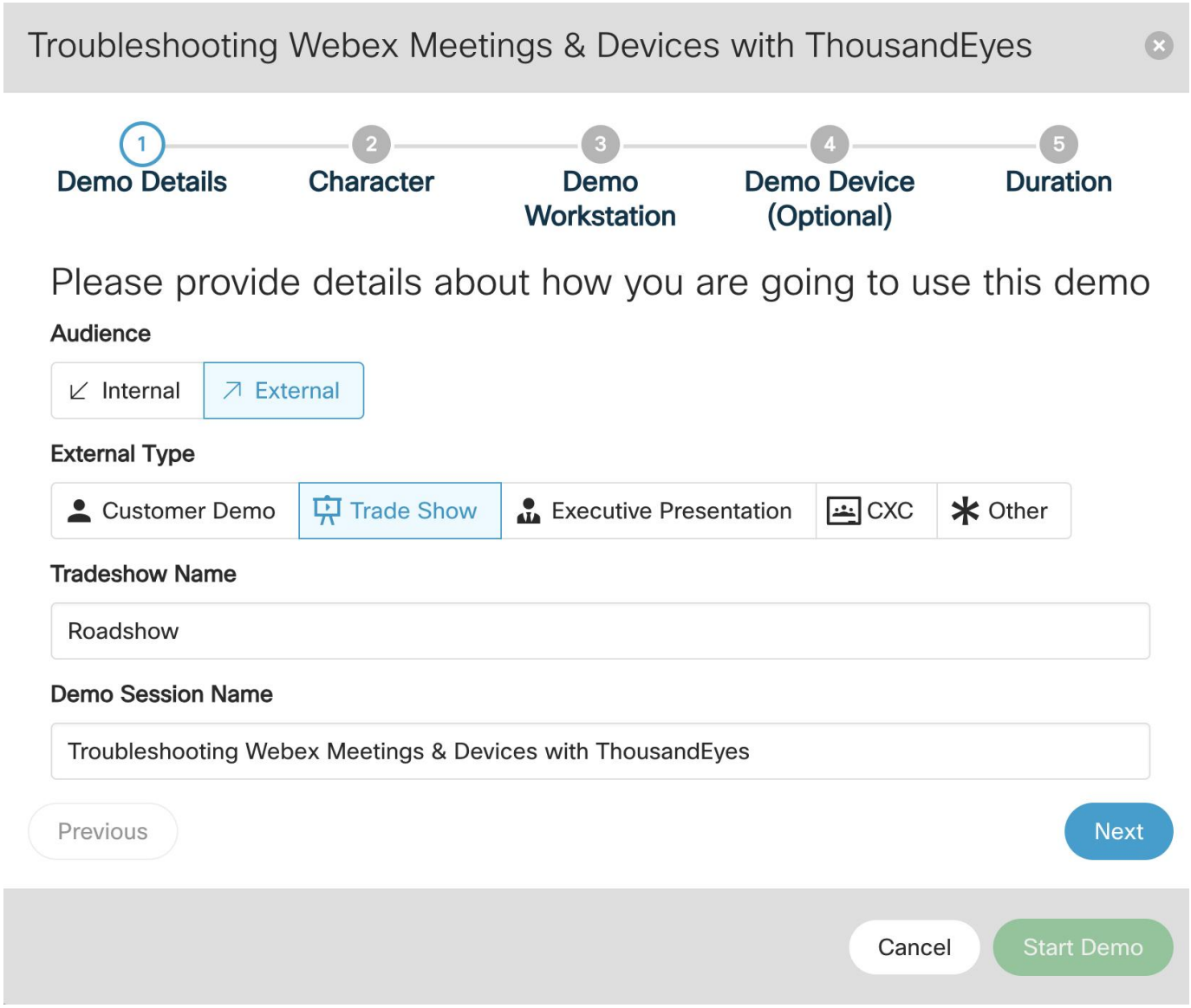


Make sure you are on your demo page Click **Start Demo** (you may have to use the back arrow to navigate back to the main overview page)

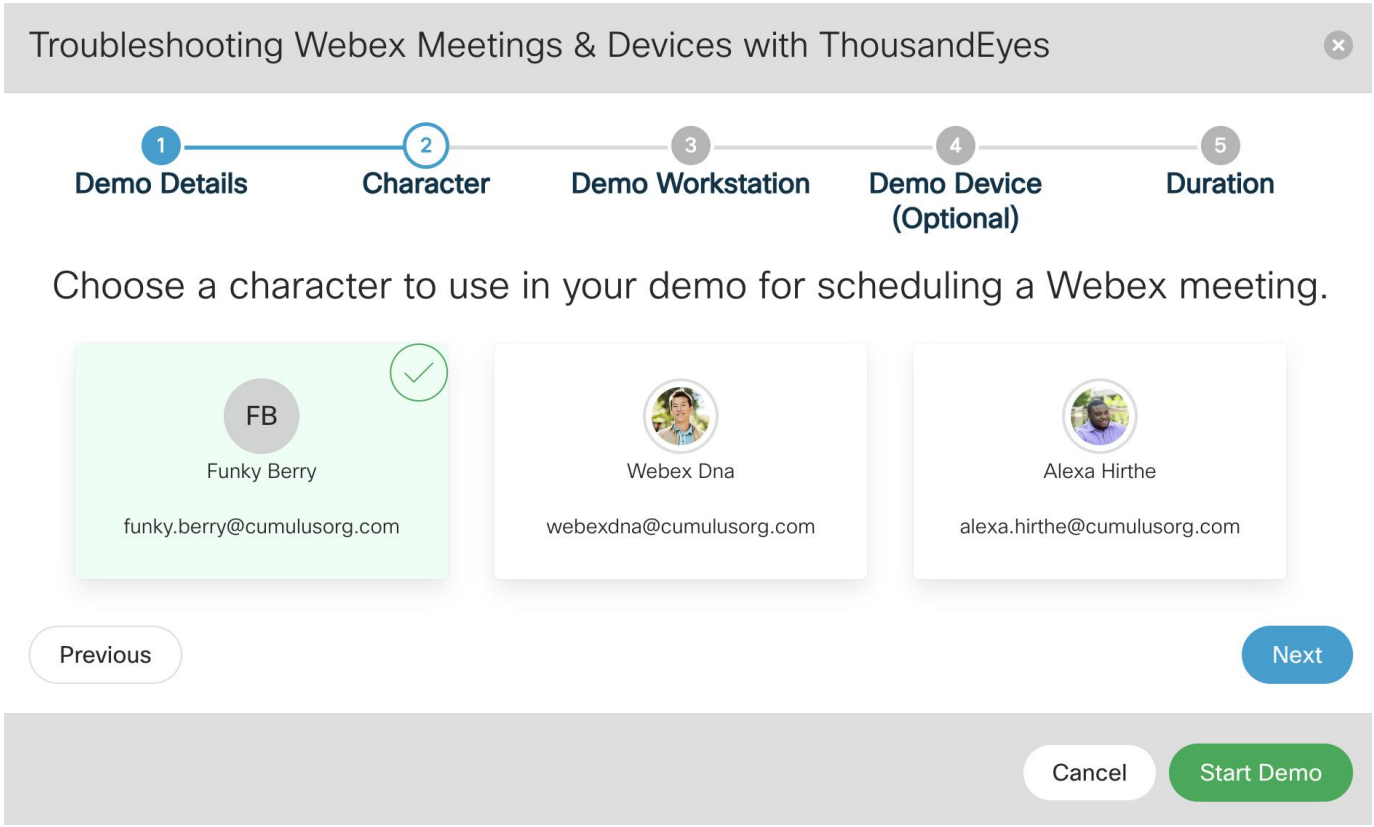


Next we need to provide a few details in order for the lab to be spun up.

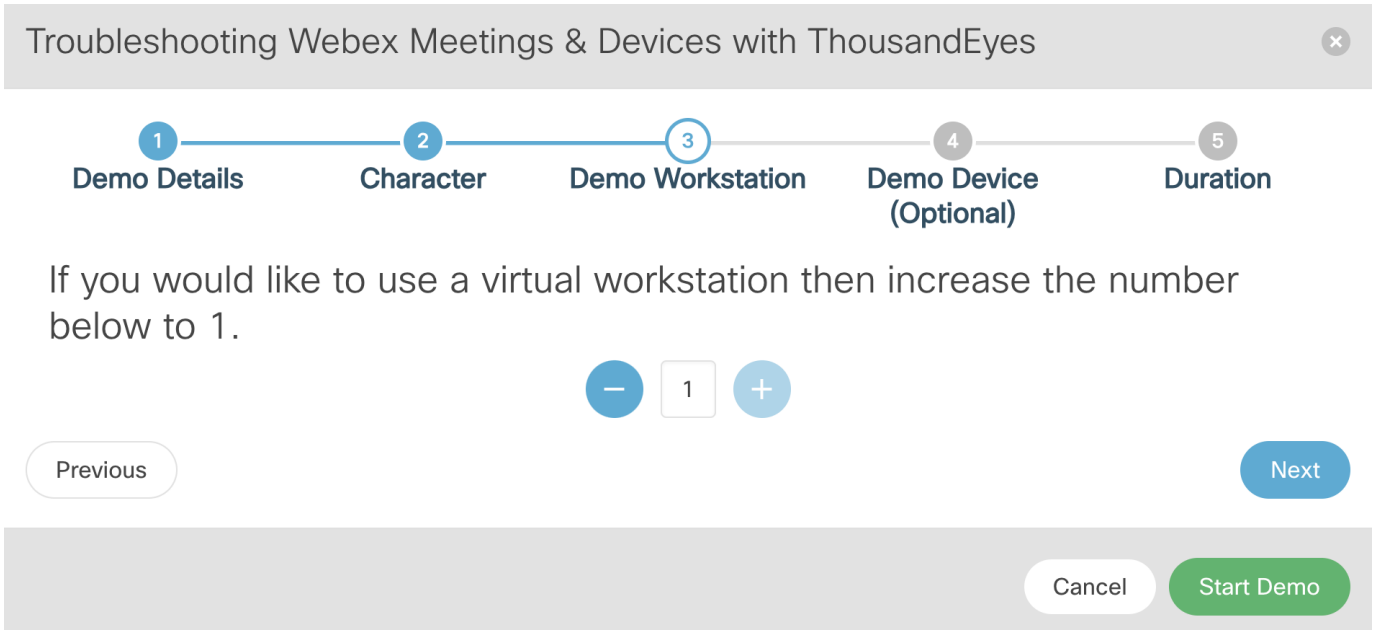
- **Audience:** External
- **External Type:** Trade Show
- **Tradeshow Name:** Roadshow
- **Demo Session Name:** Enter your name – or leave it default



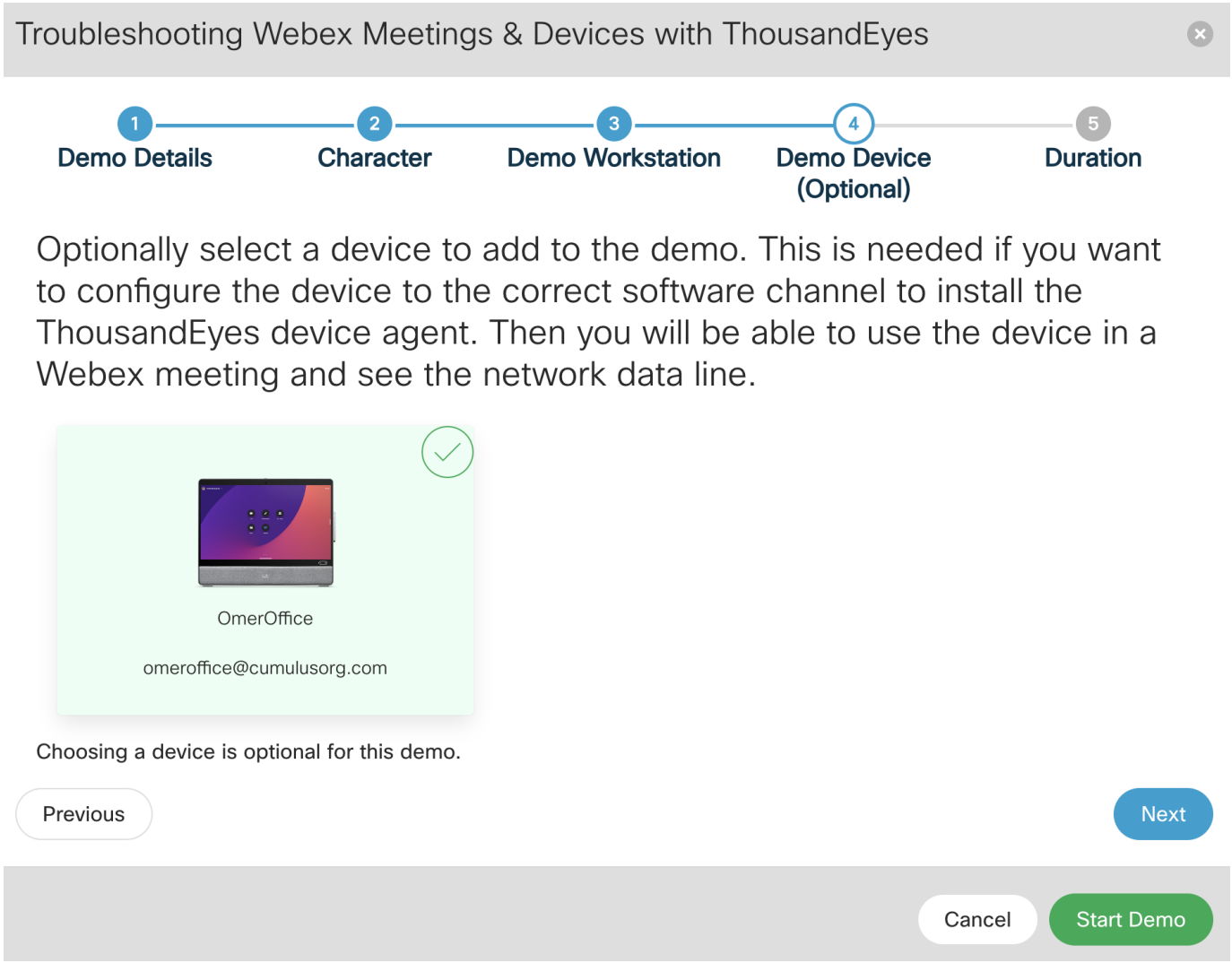
Click **Next** and then choose the character you created previously. (Note: this will be needed for automated session testing - AST)



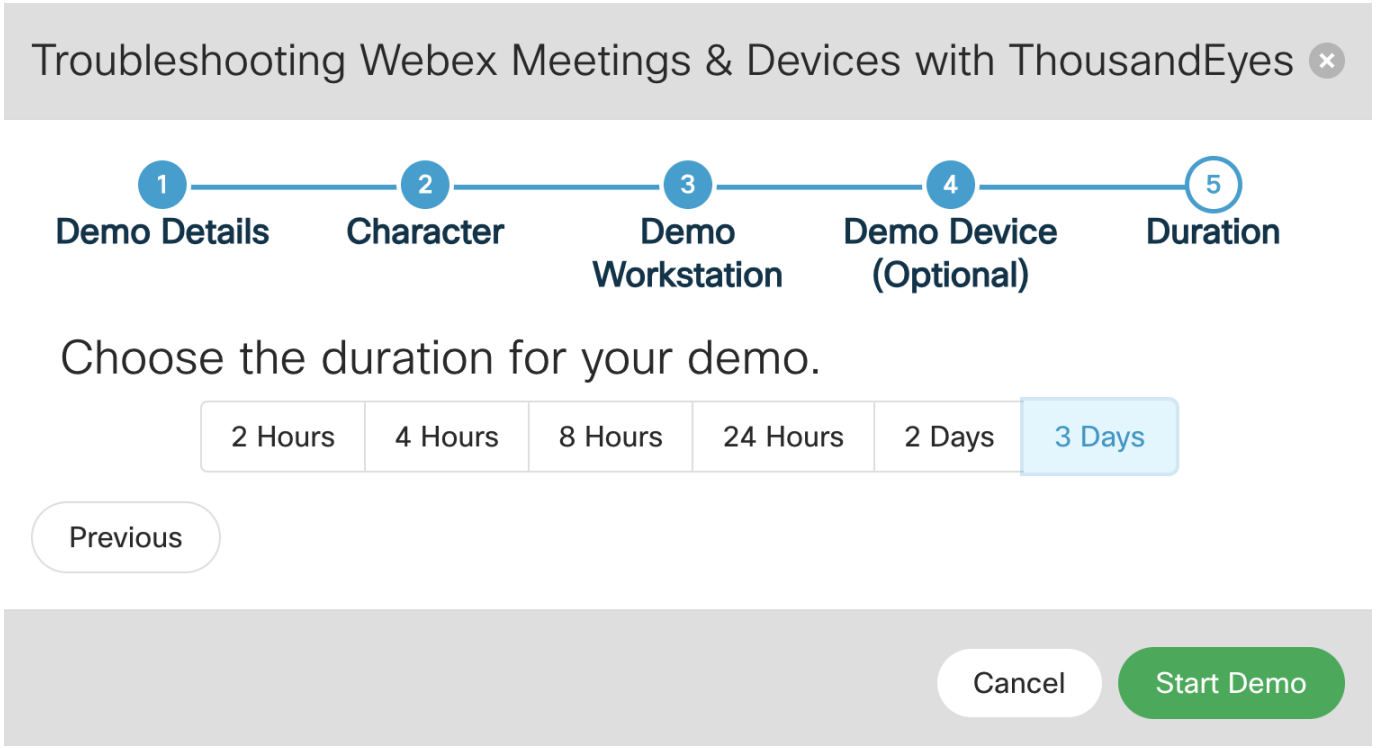
Click **Next** and add a virtual workstation using the '+" sign. This will be used to install the ThousandEyes Endpoint Agent (EPA) which can be configured to monitor web browser sessions, automtically monitor dynamic Webex meeting network connections and run scheduled tests in the background. **Note** you also have an option to install the ThousandEyes agent on your personal machine



Optional Step If you have a Webex device select your device and click **Next**



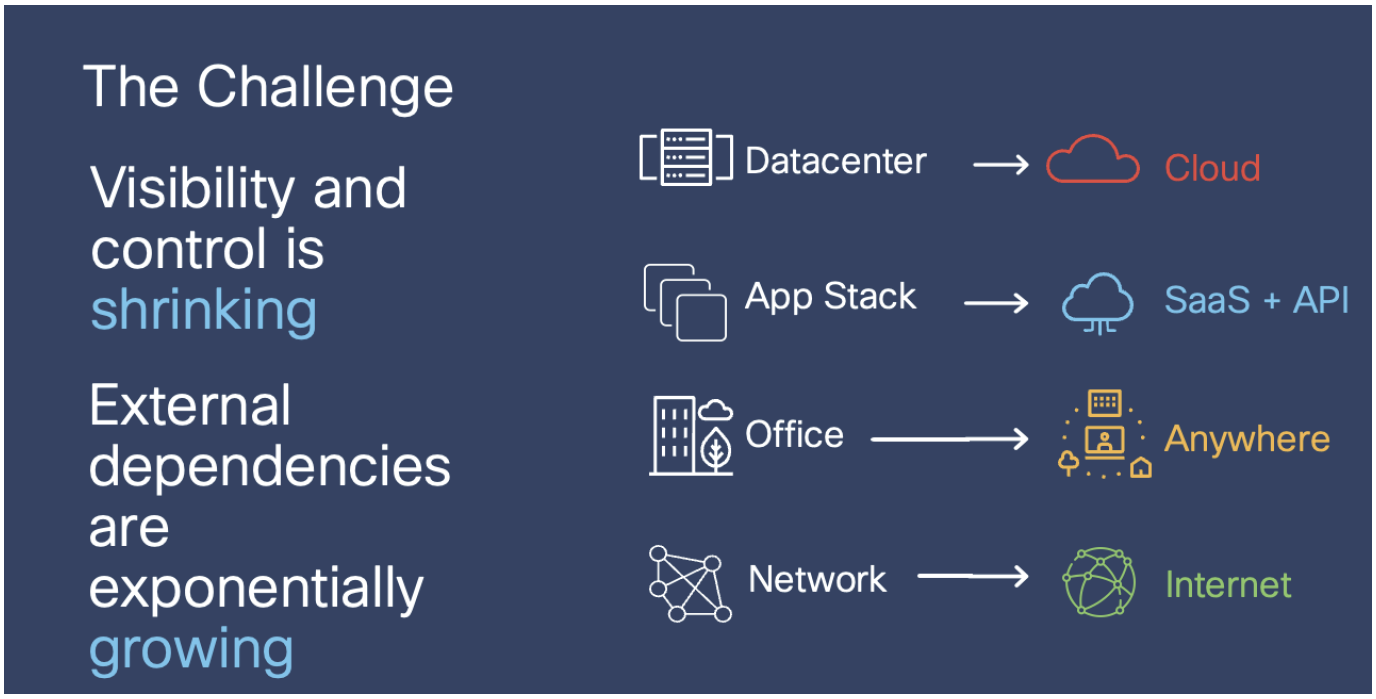
Click **Next** select your duration and Click **Start Demo** as shown in the below screenshot.

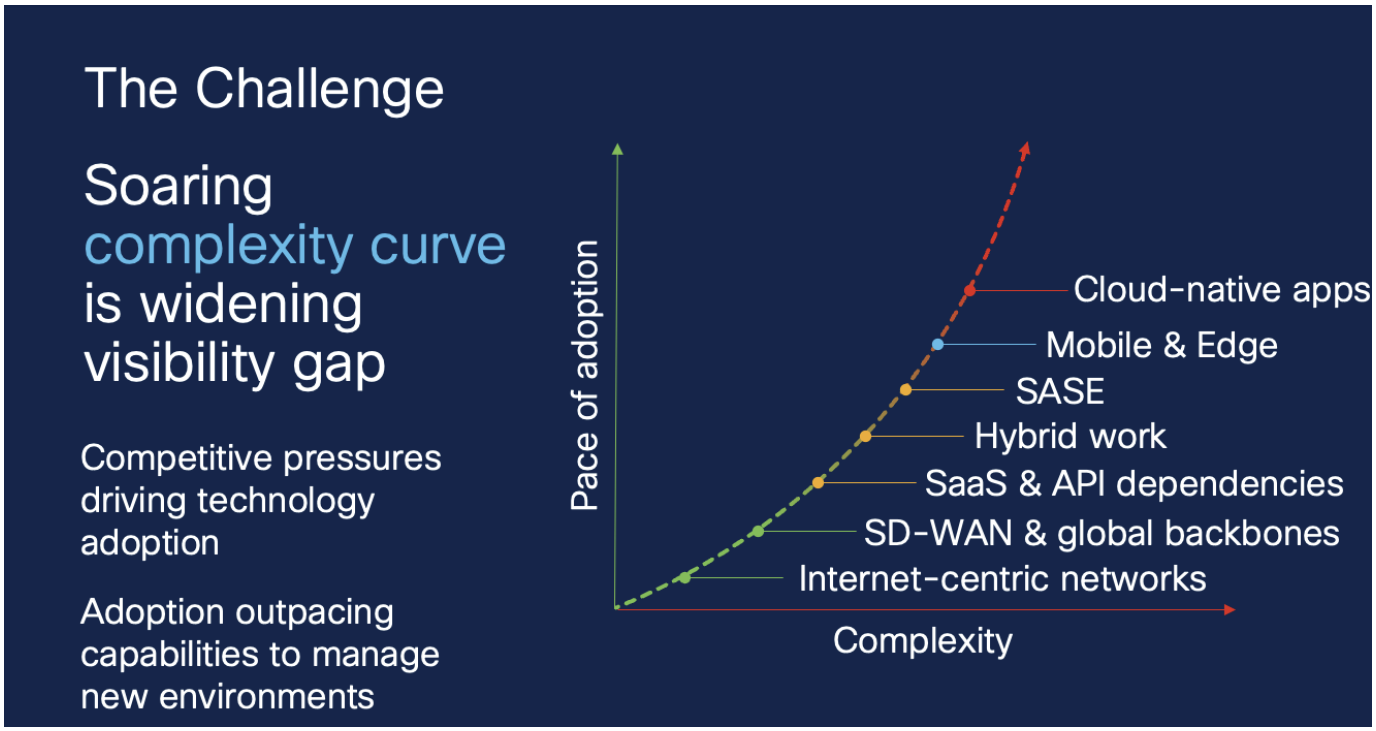


This is roughly a 45 min lab but the access duration can be upto 3 days. It will take a few minutes for the lab to spin up. While this is occurring proceed on to the ThousandEyes Overview content and extra background information in Task 2.

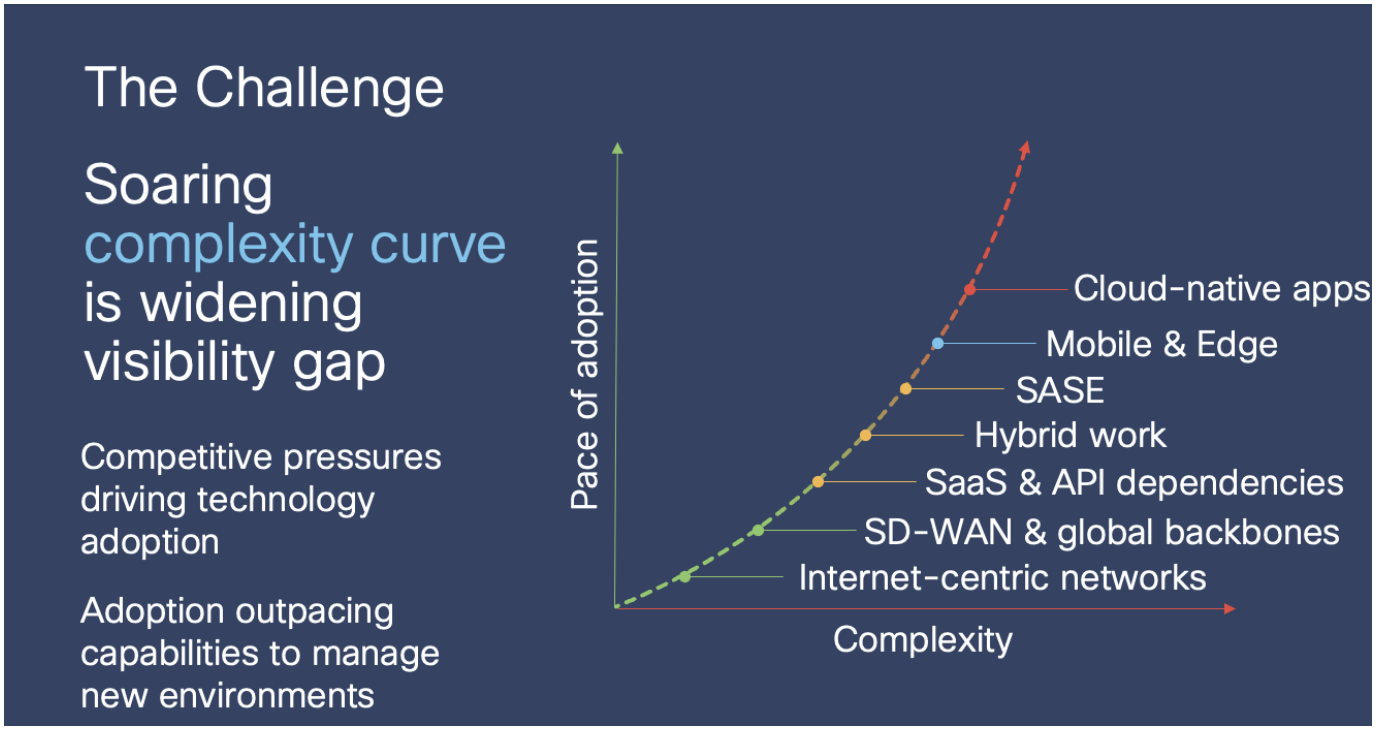
1.3 Task 2: ThousandEyes Overview

Feel free to take a few minutes while the lab spins up and review the Getting Started with Endpoint Agents guide.





Connectivity is your business, but it's changing rapidly. Your brand is only as good as your network. Digital experience is how you are measured, but most of the path is outside your control (outside the core) What do you need to do about it? How can you understand digital experience to the things your customers are accessing and understand health of the Internet cloud and peering providers. Continue your journey to learn how ThousandEyes can help answer these questions and help solve your network and application acceess issues.



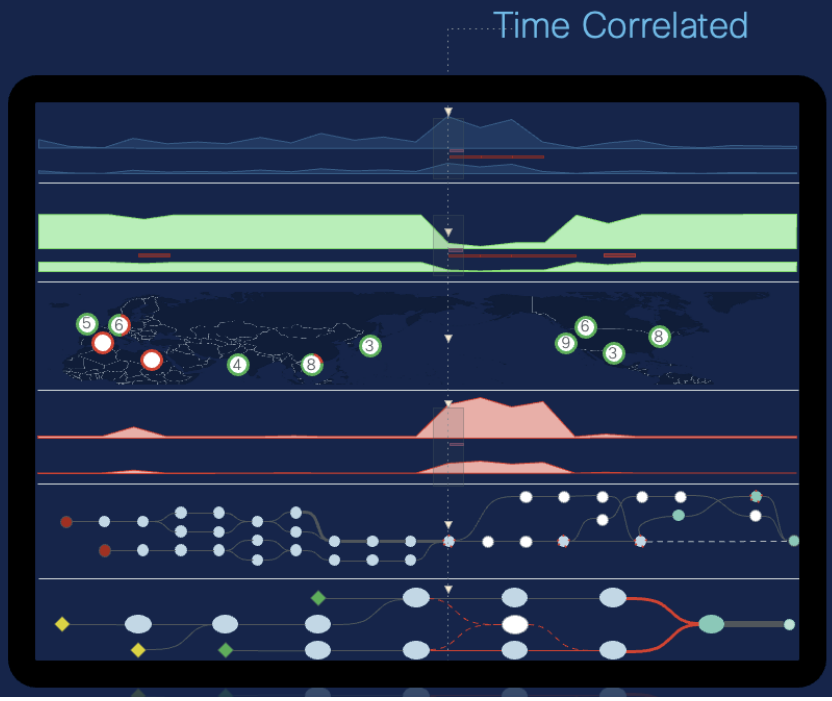
See, understand, and improve digital experiences everywhere

Our Solution

Collectively powered Internet weather map

Our Solution

Correlate performance across every layer

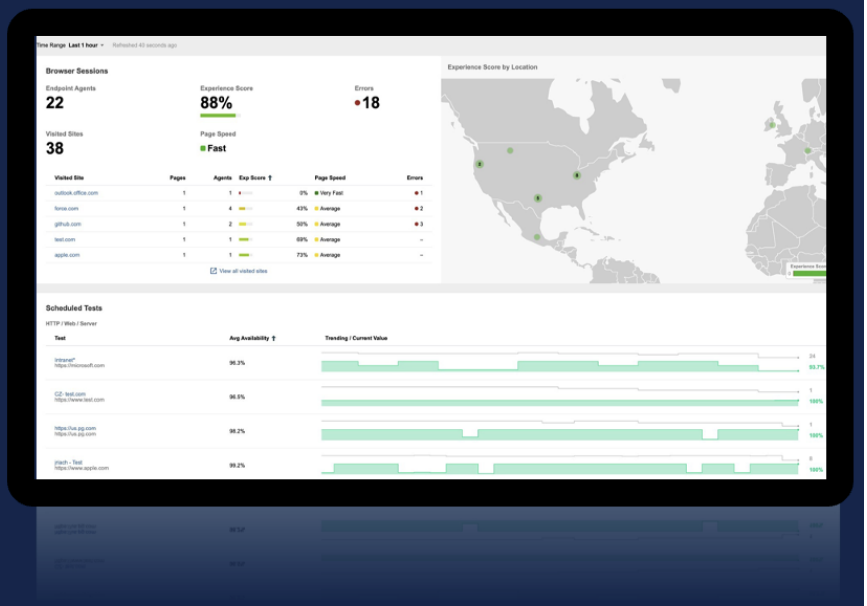


Our Solution

Visualize services end-to-end across every domain

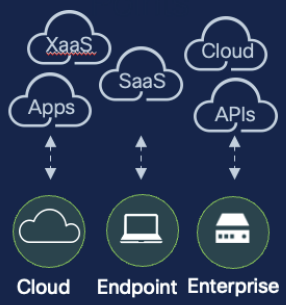
Our Solution

Understand global workforce experience

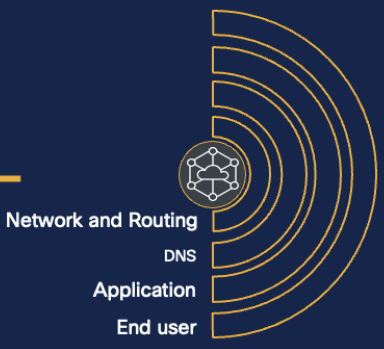


Our Solution
ThousandEyes Internet and Cloud Intelligence

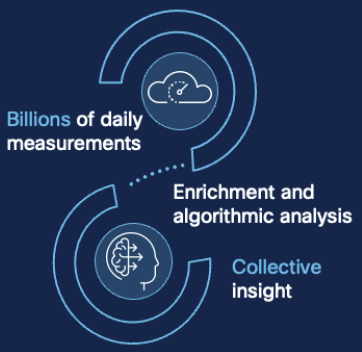
VISIBILITY — 1000s Global Vantage

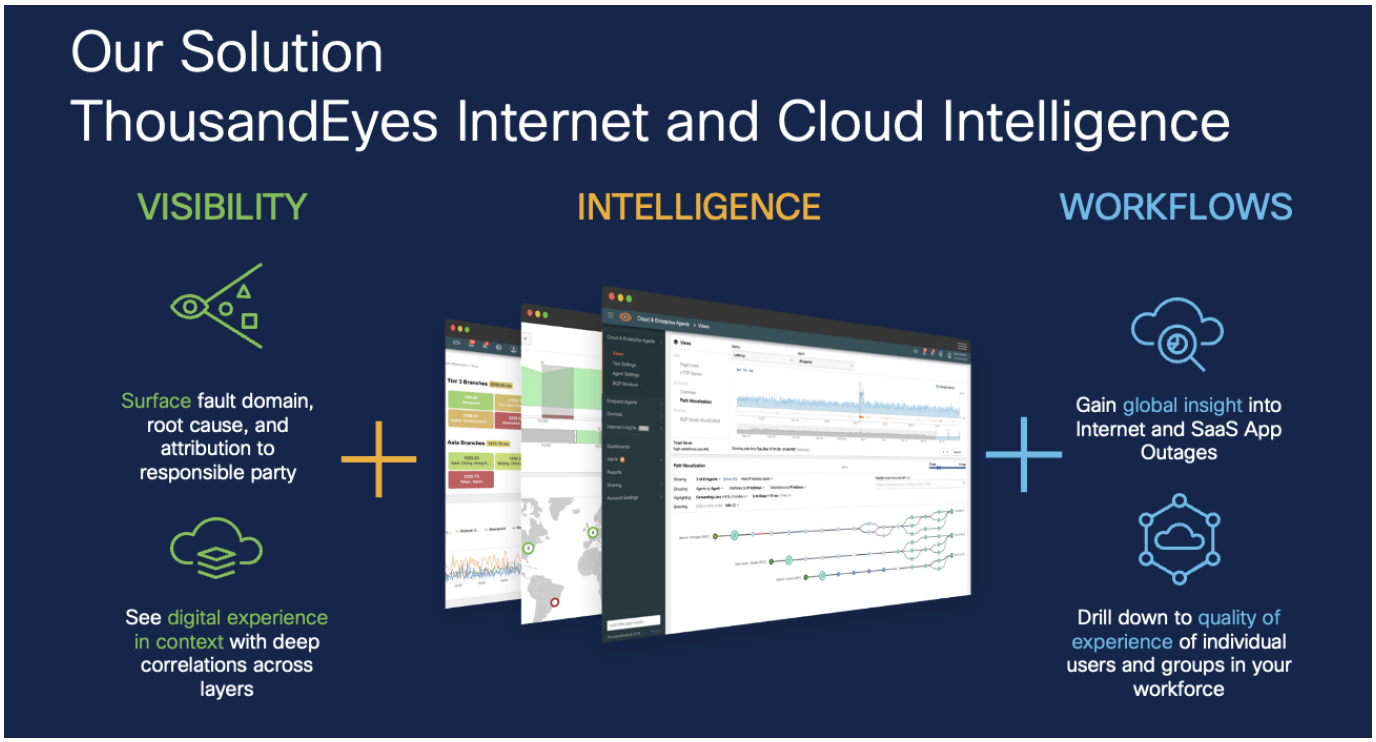


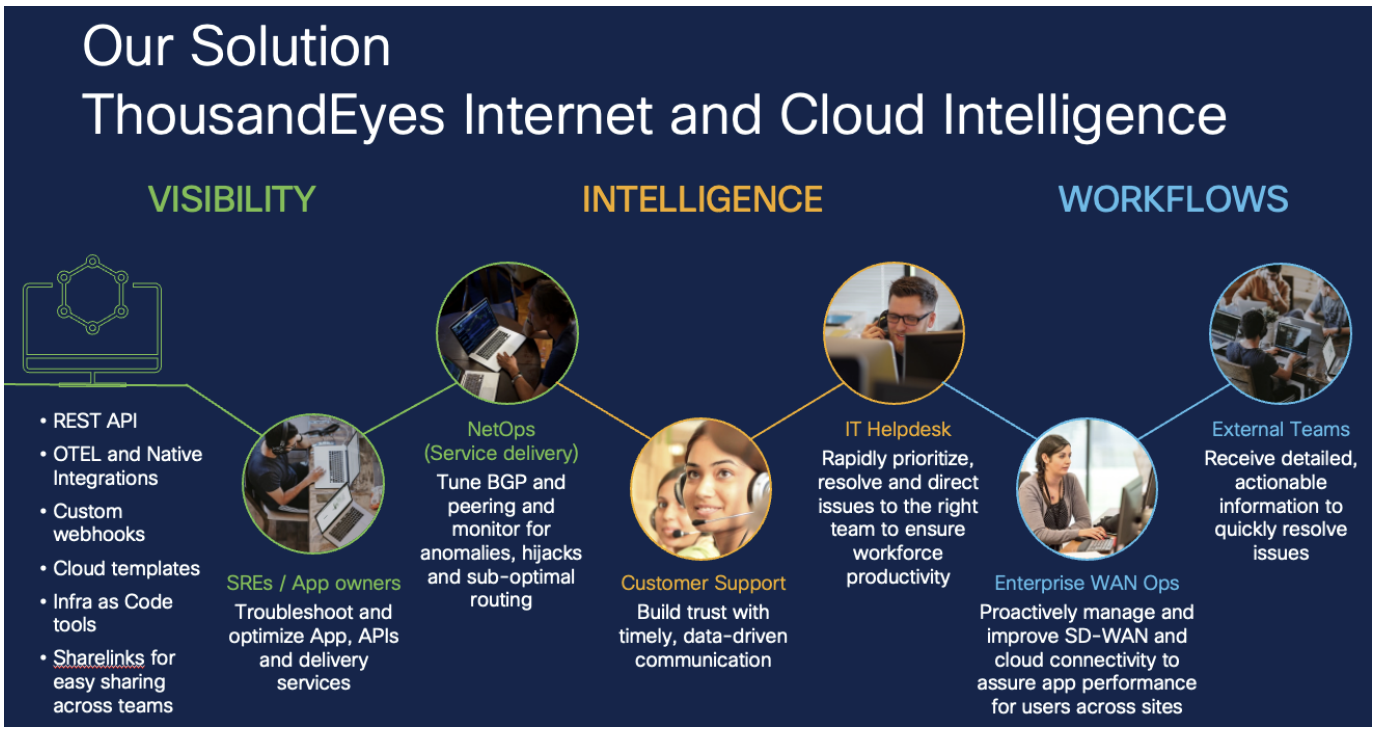
INTELLIGENCE — Unique X-layer Telemetry



WORKFLOWS — Global Collective Insight





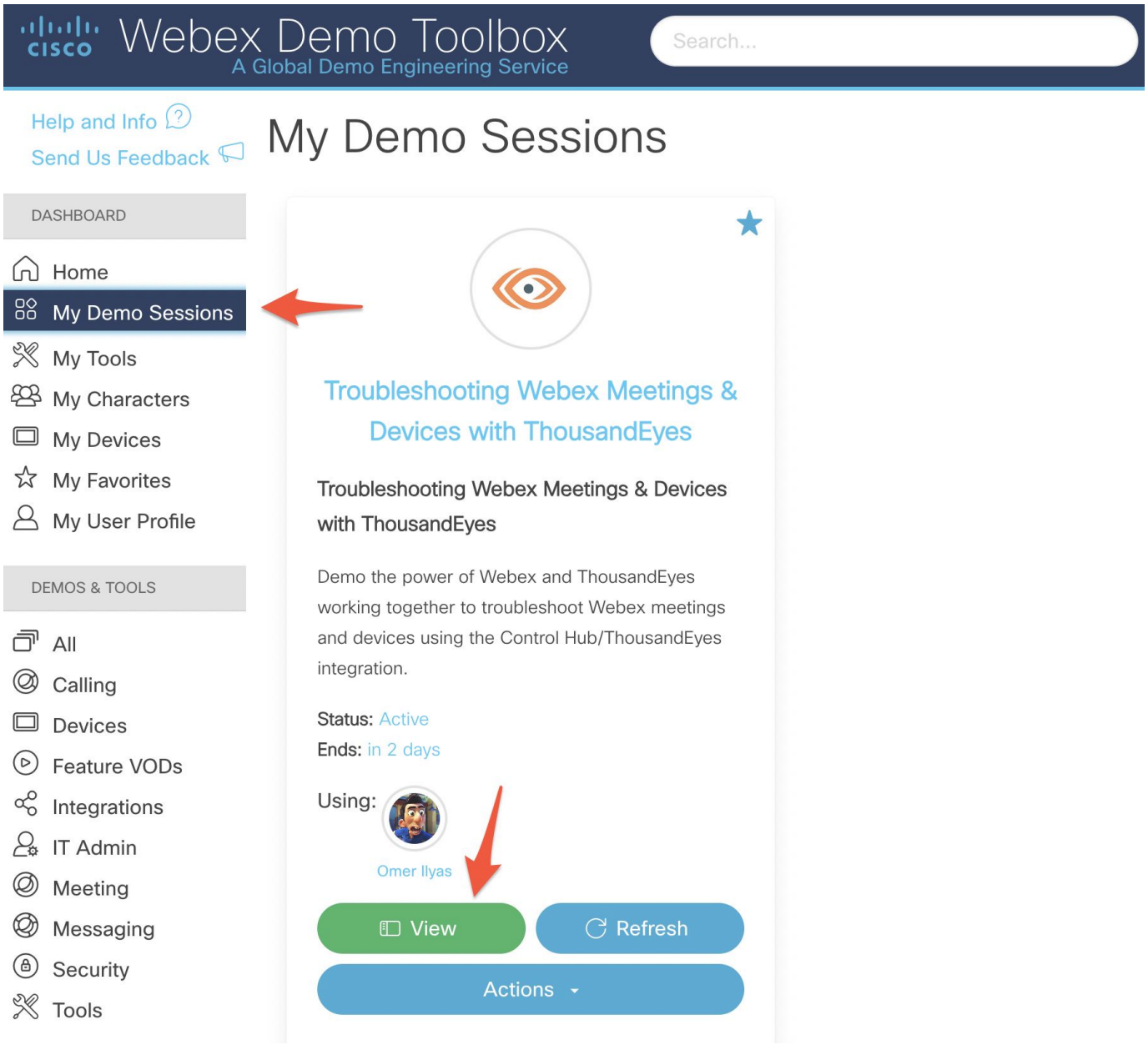


Now that you have a great background on ThousandEyes it's time to go back and verify the lab has started and login. Task 3.

Also feel free to check our awesome TE Blog and Webex site.

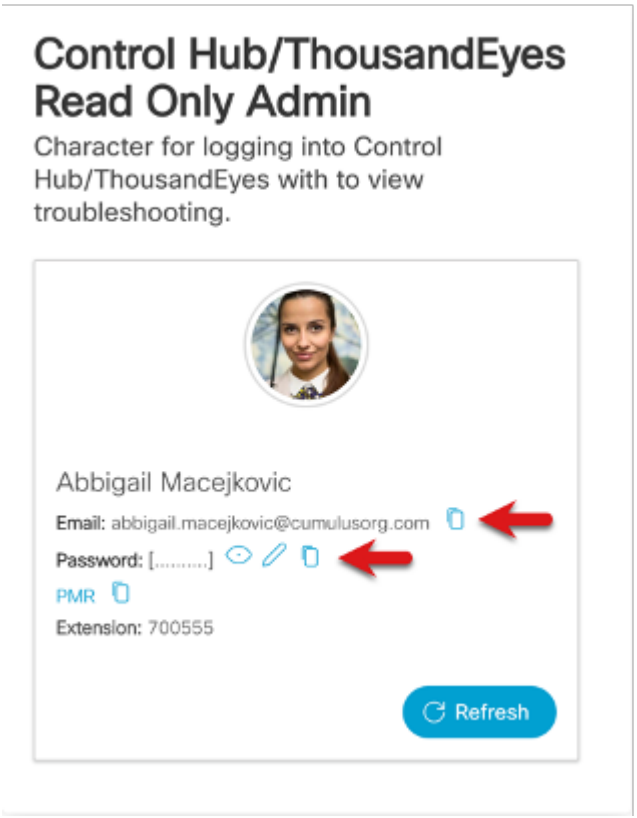
1.4 Task 3: Log into the Lab Environment

Click **My Demo Sessions** select your **ThousandEyes** demo and click the **green View button**

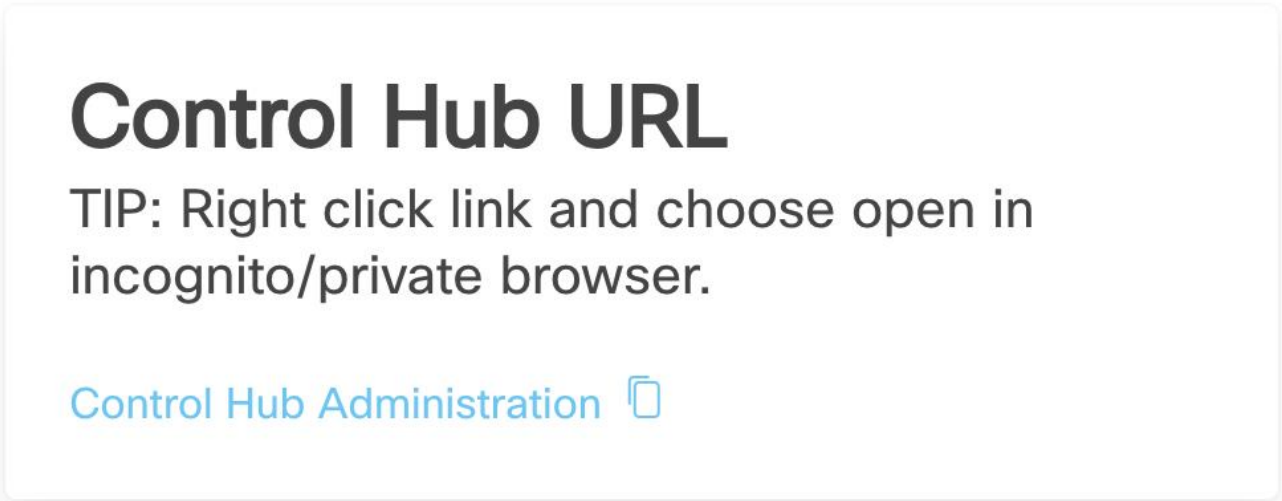


Lab Administration Information (New Read Only Admin User)

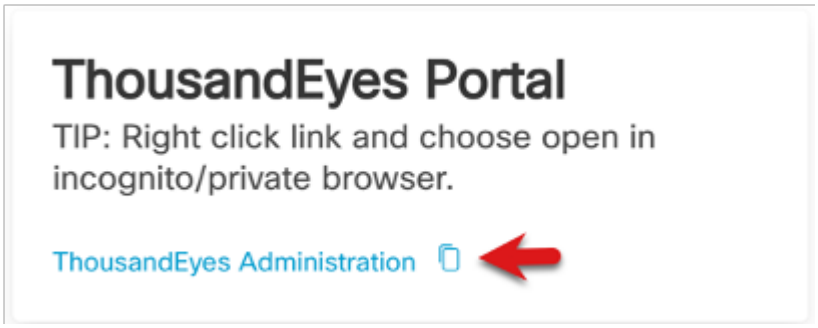
- Webex Control Hub/ThousandEyes Admin Access - A new **read only** admin user will be created. This is the new user you'll use to access the Webex ControlHub and ThousandEyes Platform (**Note:** Your user will most likely be different than this one as they are radomly assigned.)
- Email Address will be used for the SSO login access as well as the Password



• Access information to the Webex ControlHub Portal - right click and use an **Incognito Browser**

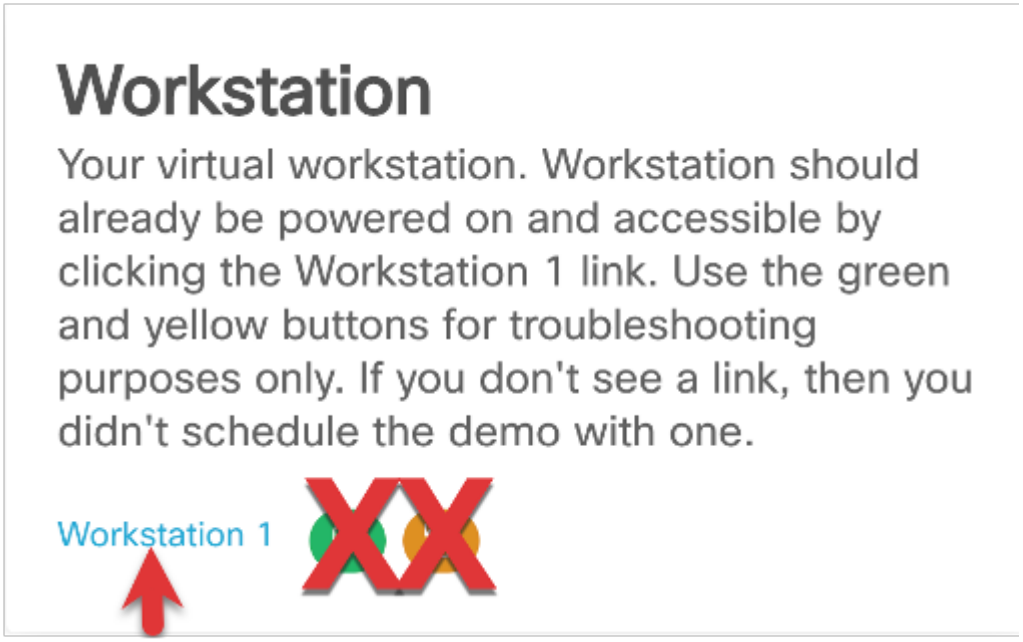


• Access information to the ThousandEyes Portal be sure to right click and use an **Incognito Browser**

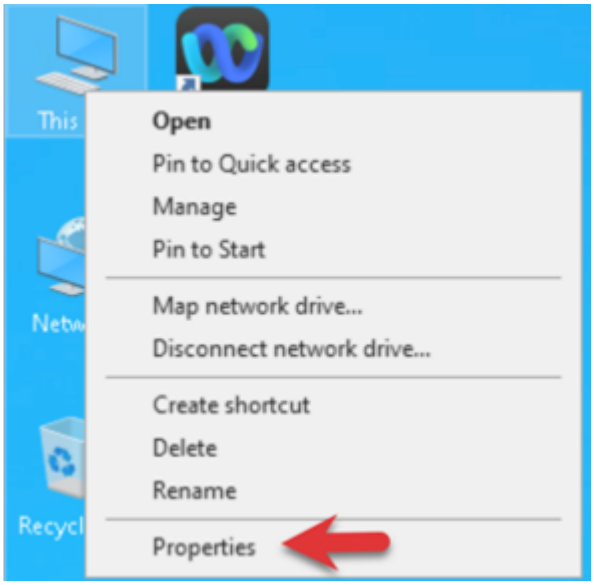


First thing will be to get your VM set up

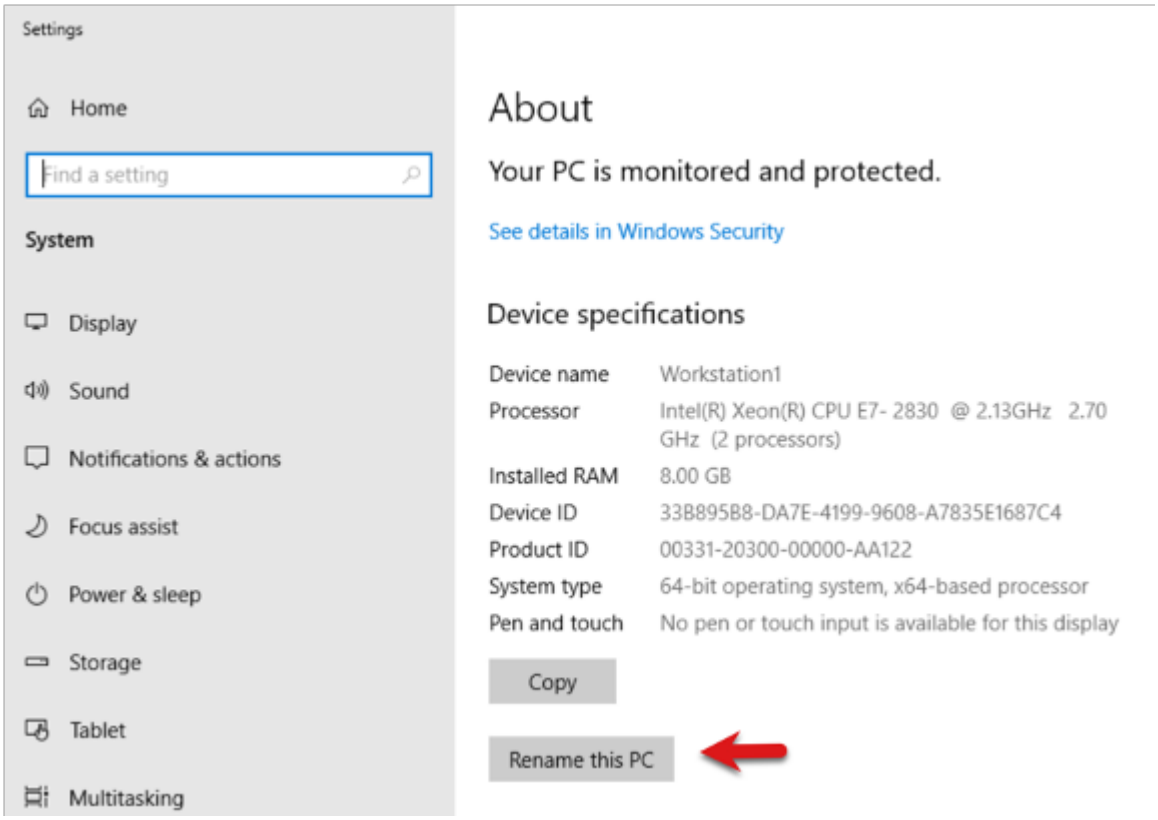
- Click the Workstation 1 link. You should see a Windows Desktop show up in new browser tab.



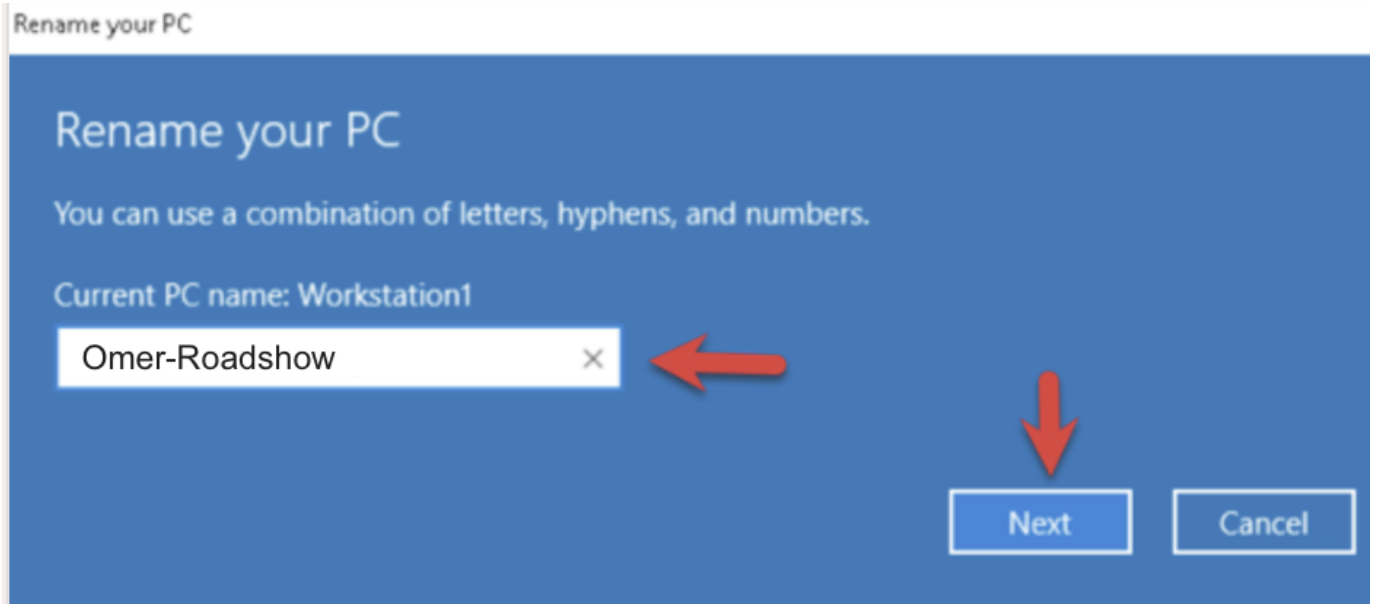
Right Click on the **This PC** desktop icon and click **Properties** so you can rename the VM.



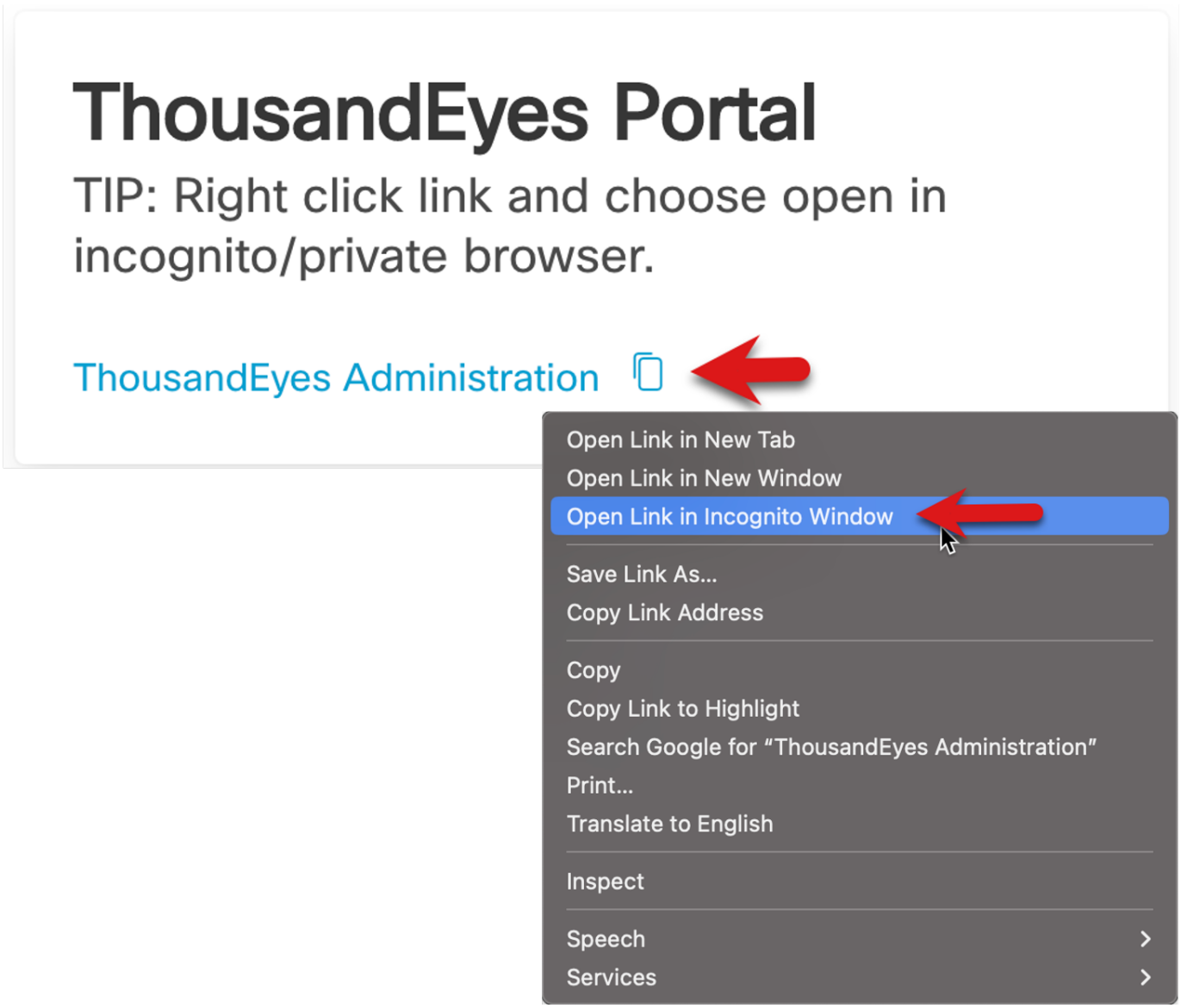
Click Rename this PC



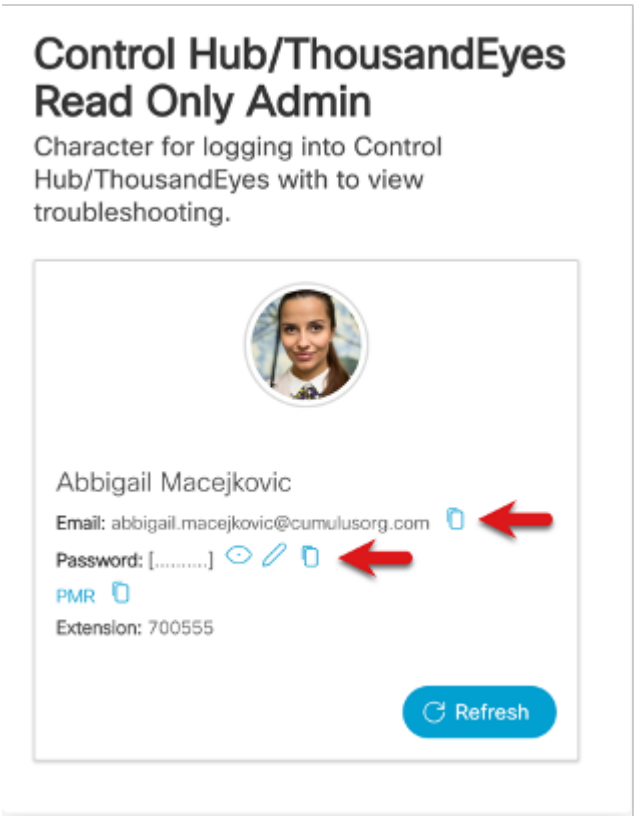
Name the PC your-name-Roadshow (no spaces), click **Next** and click **Restart Now**



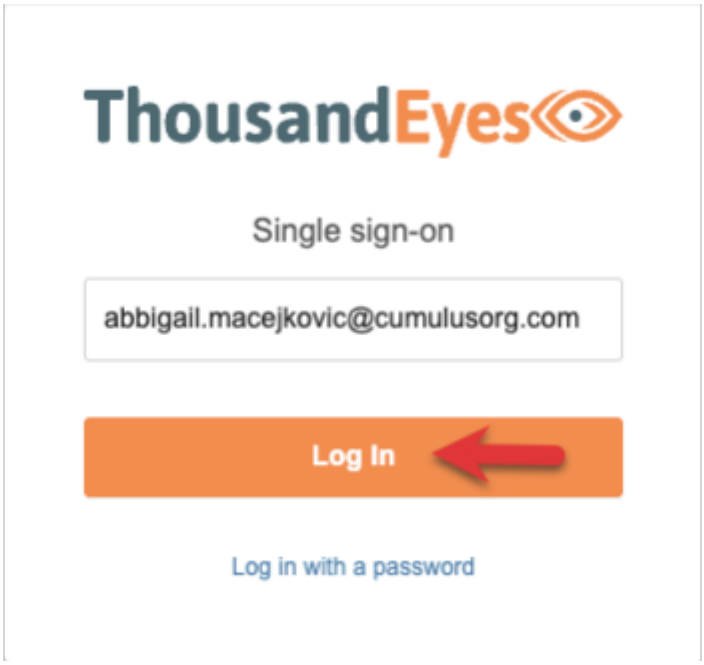
While the VM reboots go back to your previous tab for demo . Right click the **Control Hub URL** and **ThousandEyes Administration** Portal link and open both in incognito browsers as we will be using them in the coming steps. The same creds can be used to login into Webex Control Hub and ThousandEyes

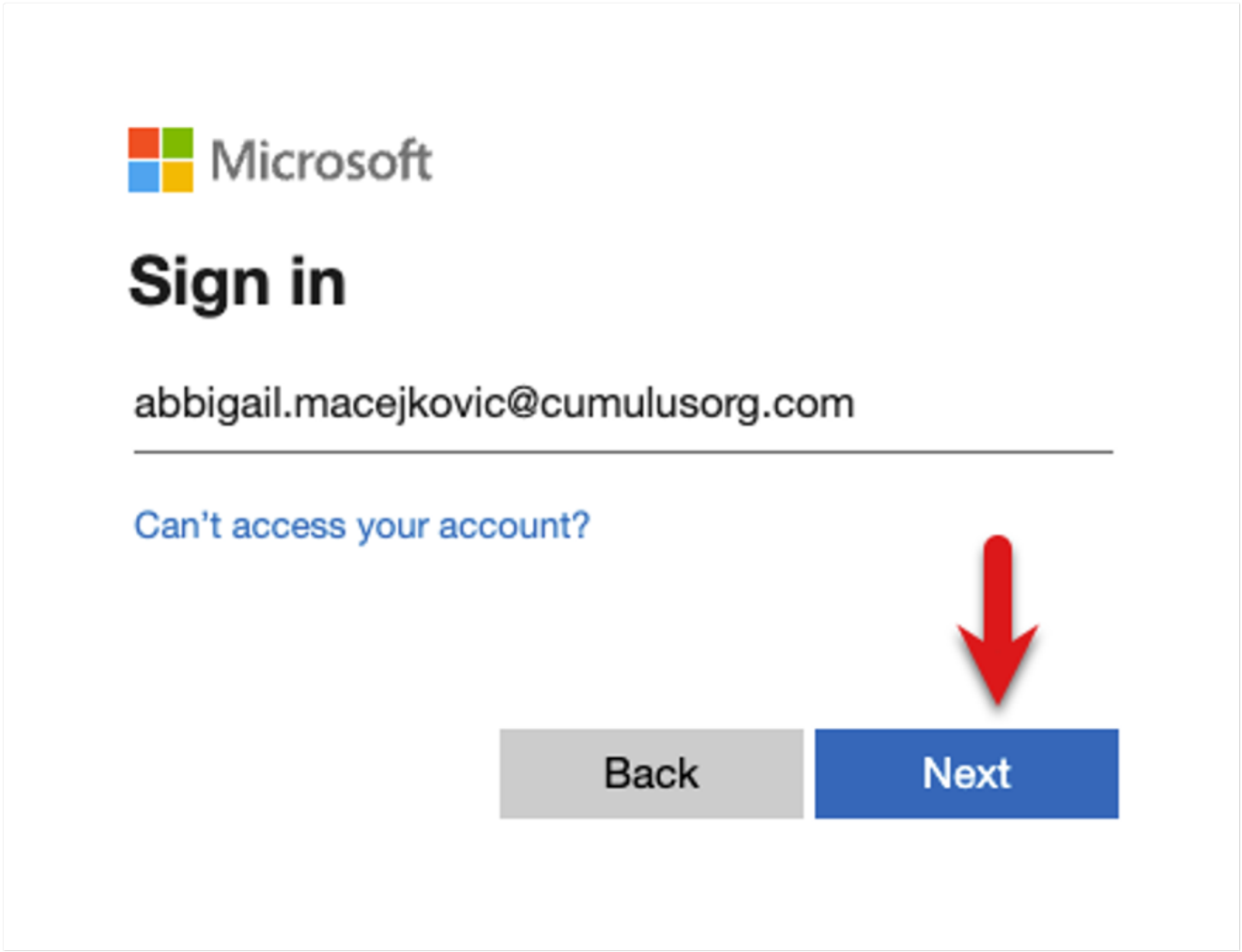


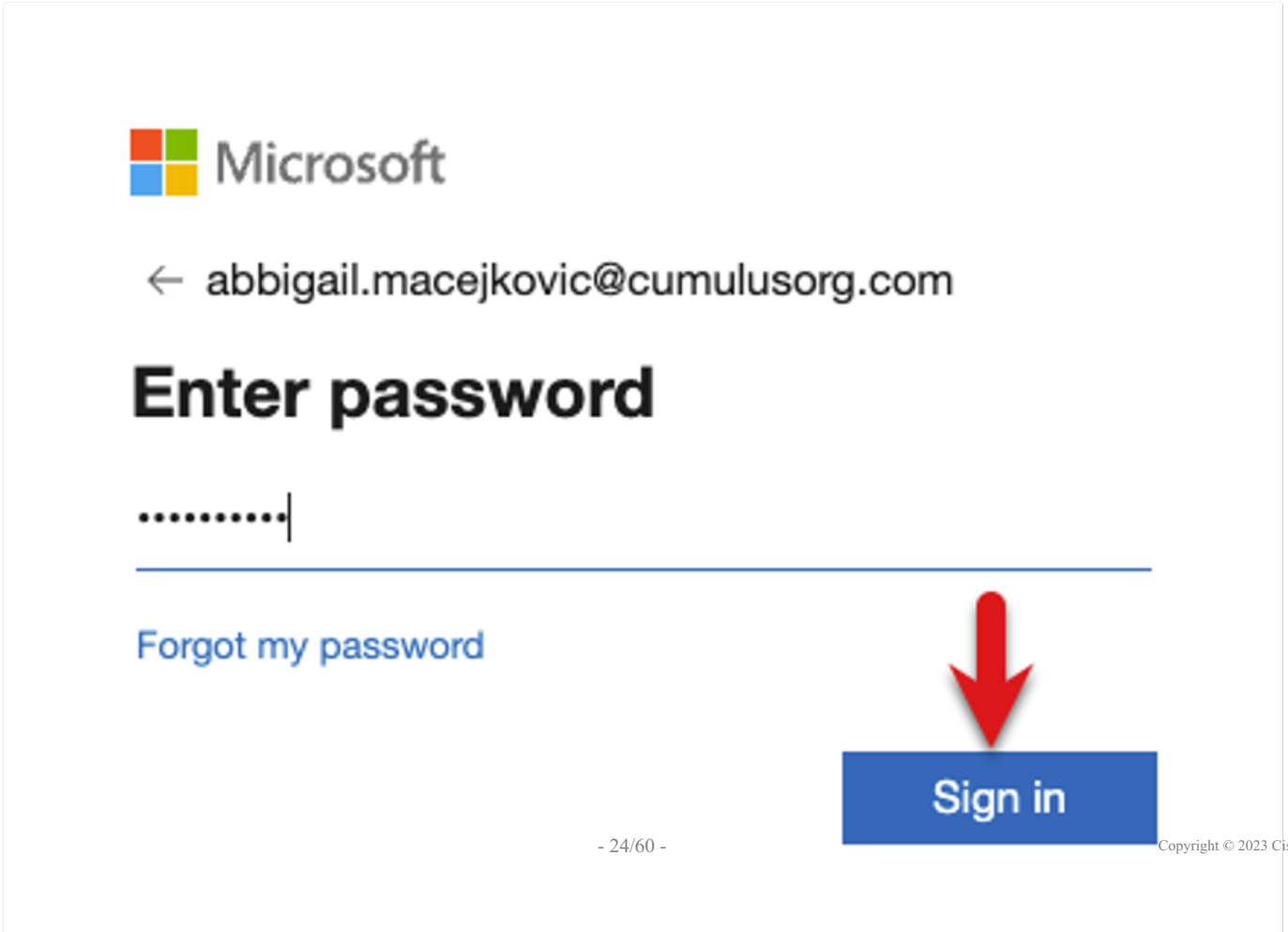
Use the credentials from the ControlHub/ThousandEyes Read Only Admin in the next steps.



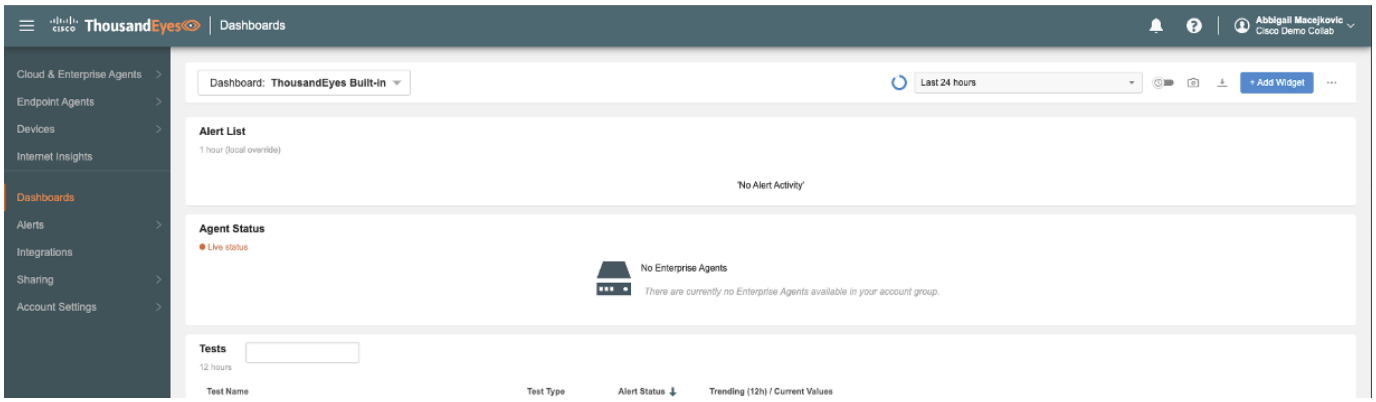
Your incognito browser will open to the ThousandEyes SSO login page as shown in the below image. Use the Username and Password from the ThousandEyes Read Only Admin to complete the login process. Click Don't show this again and Yes in the pop up window after you have completed the SSO login process.





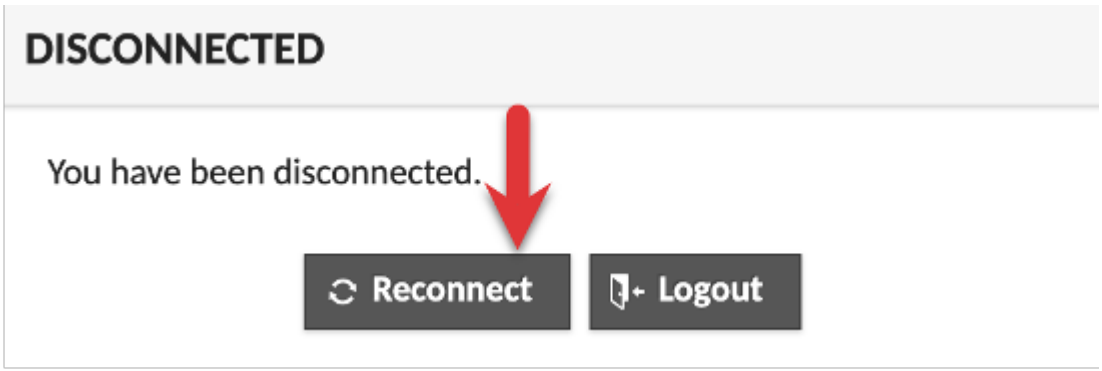


You should now see the ThousandEyes Default Dashboard (see the below image). You can leave this browser open and we will come back to it later.

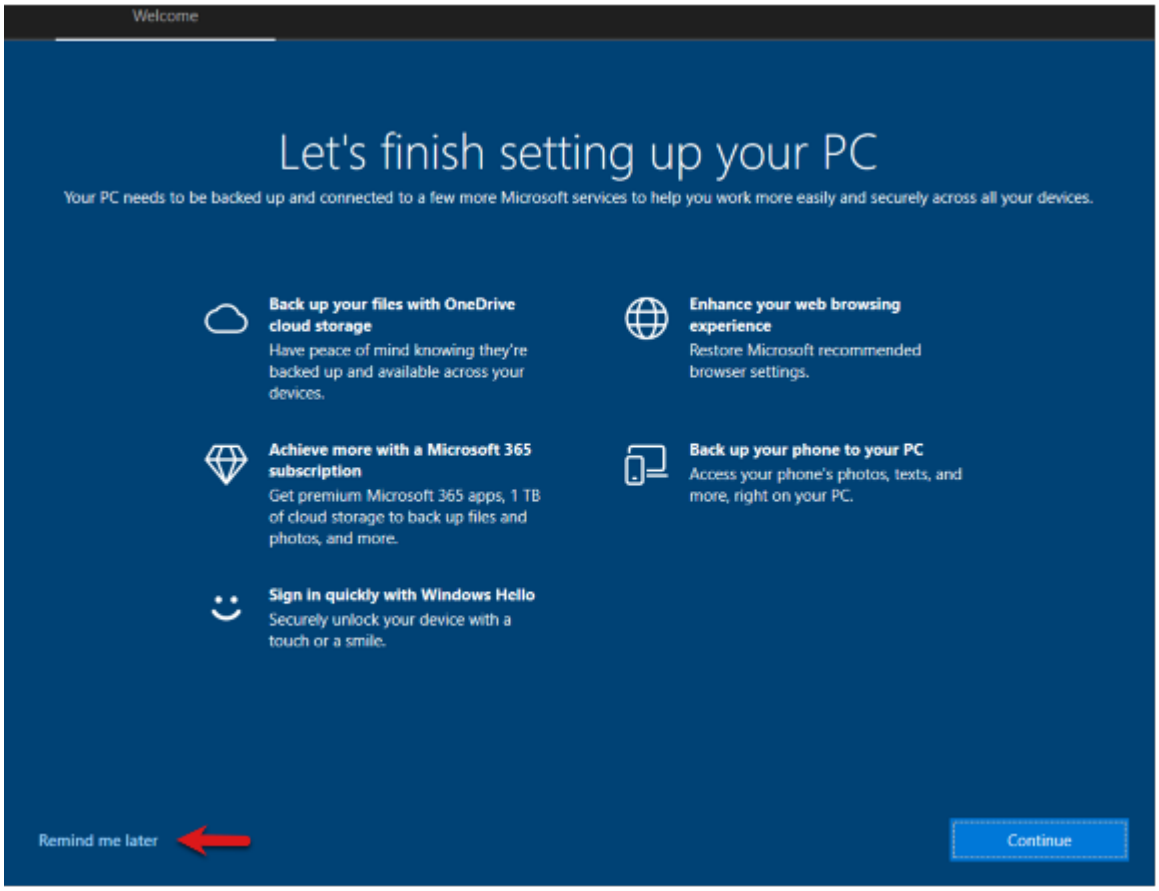


Note: Follow the above creds/steps to login into Webex Control Hub as we will be using them in coming steps.

Log back into the Windows VM. Navigate back to the tab that had the Windows VM running in it and click “Reconnect” or if that tab closed you click on the Workstation 1 link to open a new session to it.



Note if a Let’s finish setting up your PC window appears just click ”Remind me Later". Also close the CC Cleaner browser and Accept the Webex EULA (if they appear).

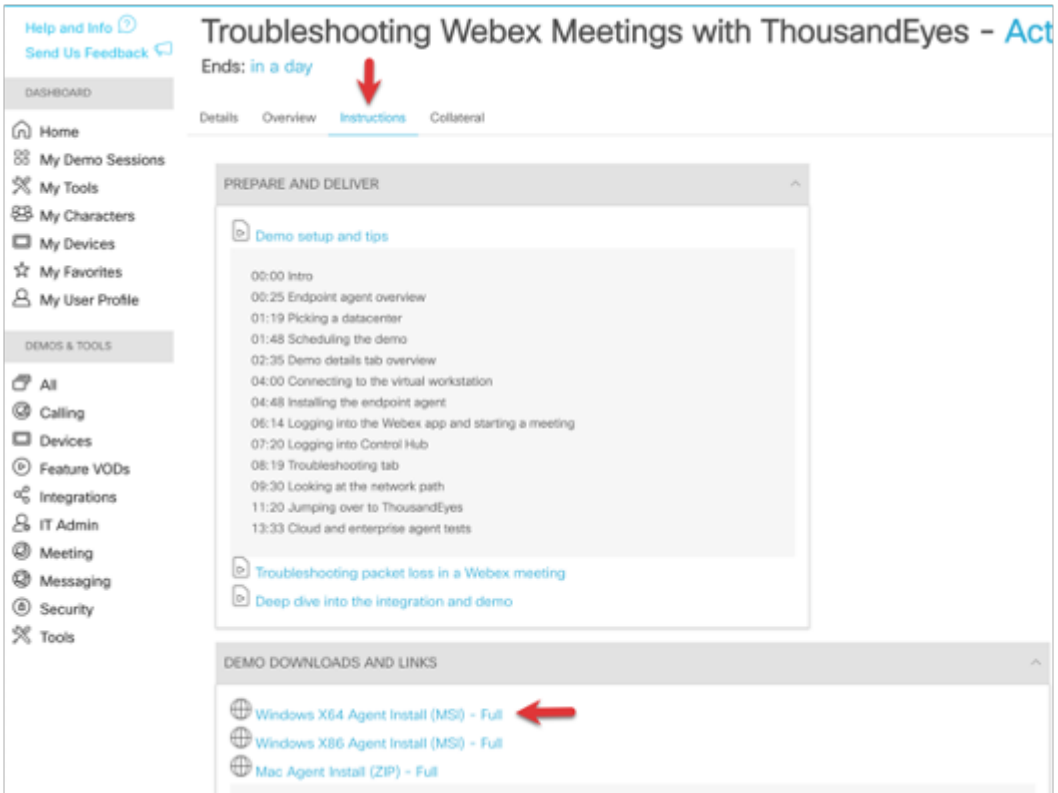


Time to install the ThousandEyes Endpoint Agent (EPA) continue to Task 4.

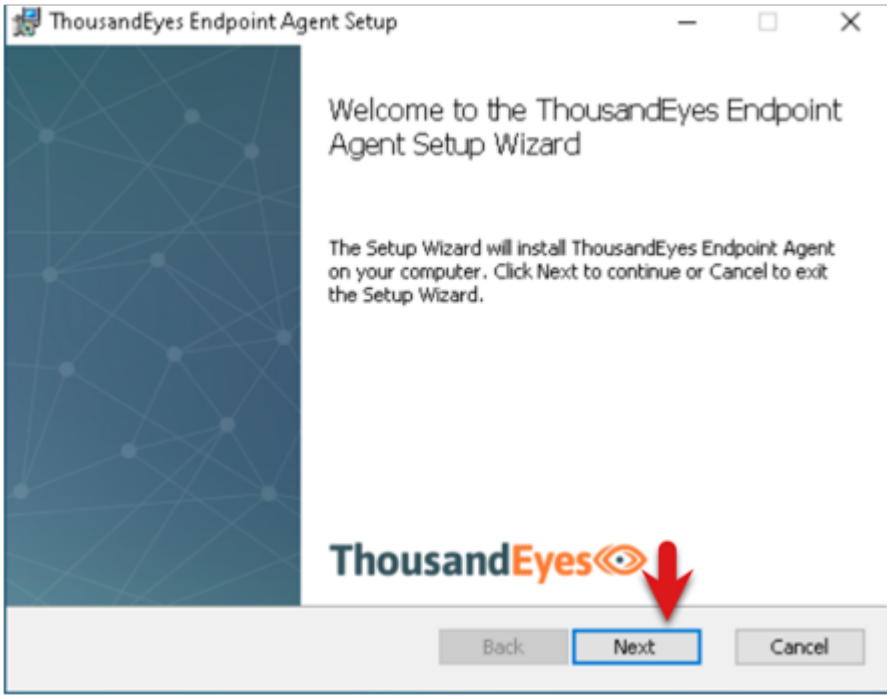
1.5 Task 4: Install the ThousandEyes EPA

Once on your VM station,make sure no browser sessions are running on Window VM then click the ThousandEyes Agent Installer

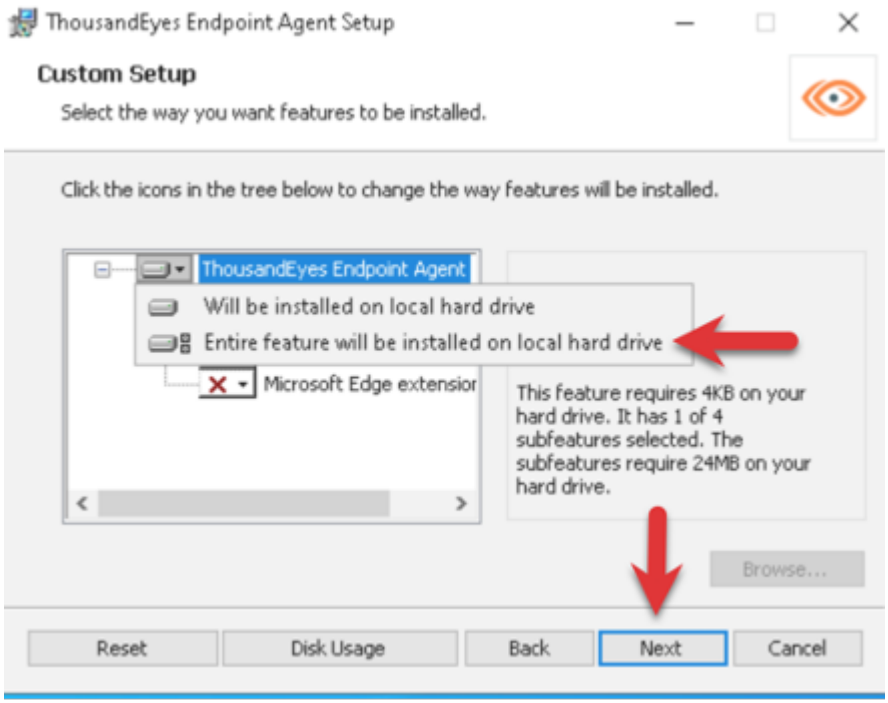
You should **NOT** have to do this but if you don't see the ThousandEyes Agent Installer go back to the tab for the lab and click the **Instructions link** then copy the link for the **Windows x64 Agent Install (MSI) – Full** from the Demo Downloads and Links section. Navigate back to the Windows VM tab, open a browser and paste the link into it to download the installer. Locate the installer and click it to install it.



Click **Next** and Accept the License Agreement



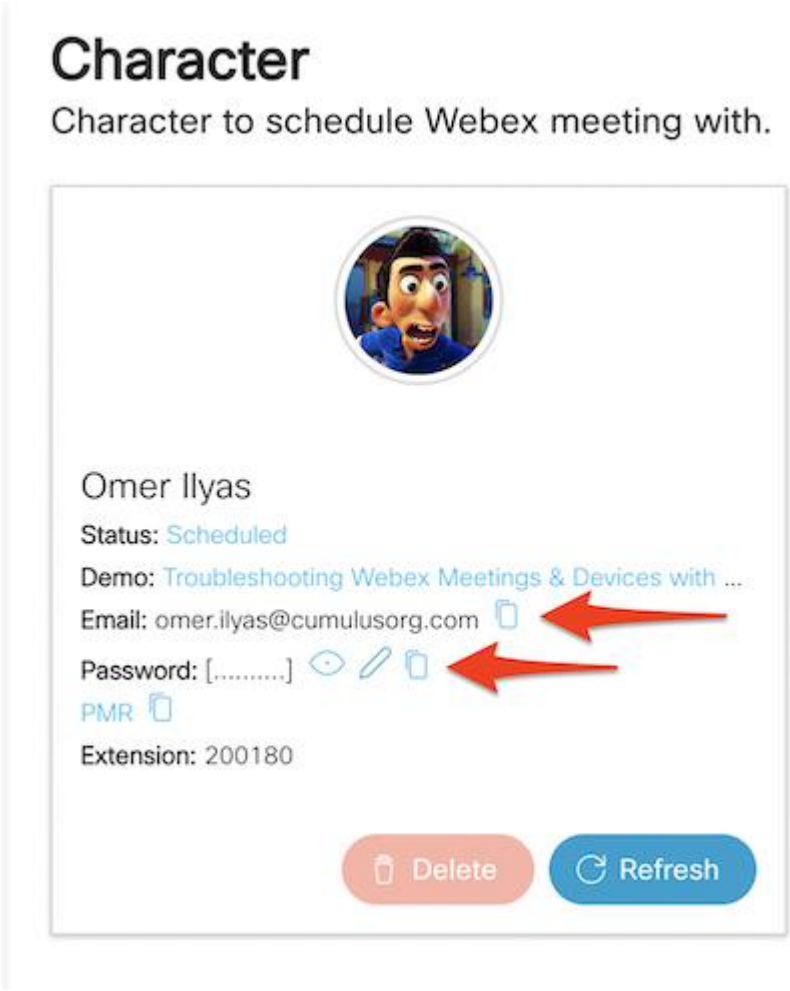
Click the disk icon for **ThousandEyes Endpoint Agent** and **Google Chrome** and select **Entire feature will be installed on local hard drive** then click **Next** and **Finish**.



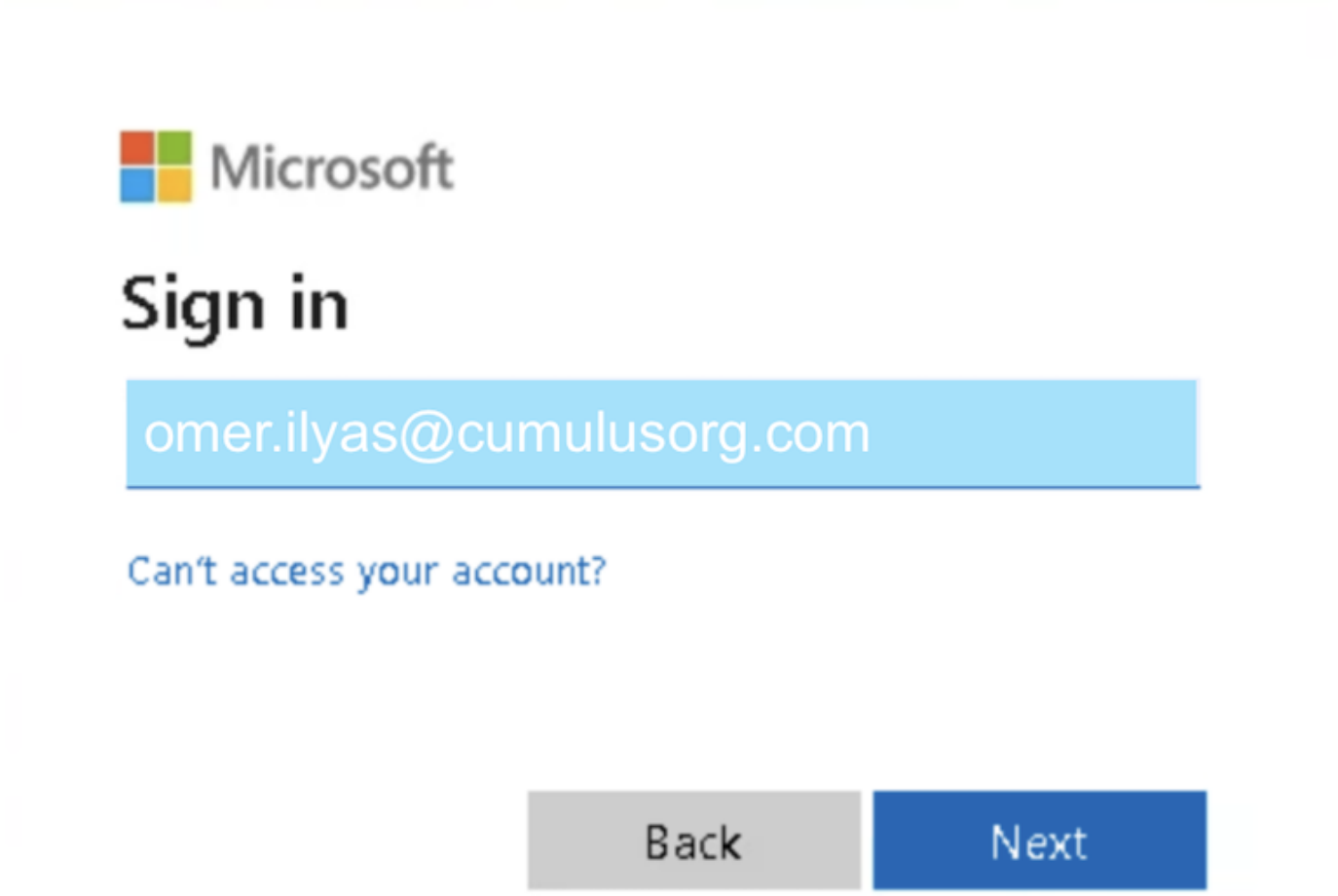
Note the above step will install ThousandEyes Endpoint agent on the VM provided. As mentioned earlier you can also get the install file from the **Instruction** tab and install the same on your personal machine (windows/mac)

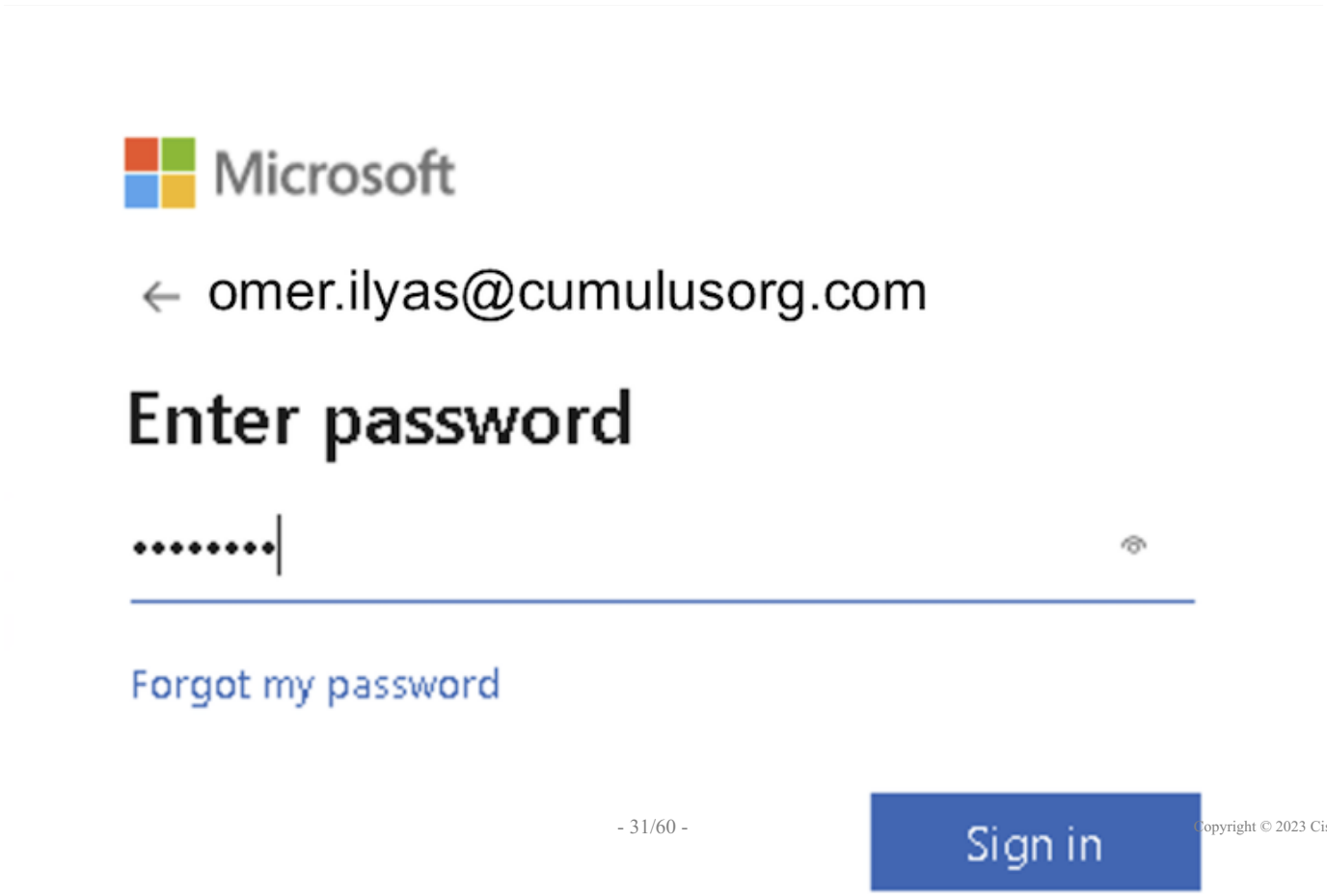
1.5.1 Start up a Webex Meeting on your VM

This will generate Webex traffic which we will view later in the lab. Navigate back to your lab information tab. Copy the email address for the character you **created** to schedule a Webex meeting with. You will use this to login into Webex App and start a Webex meeting session.

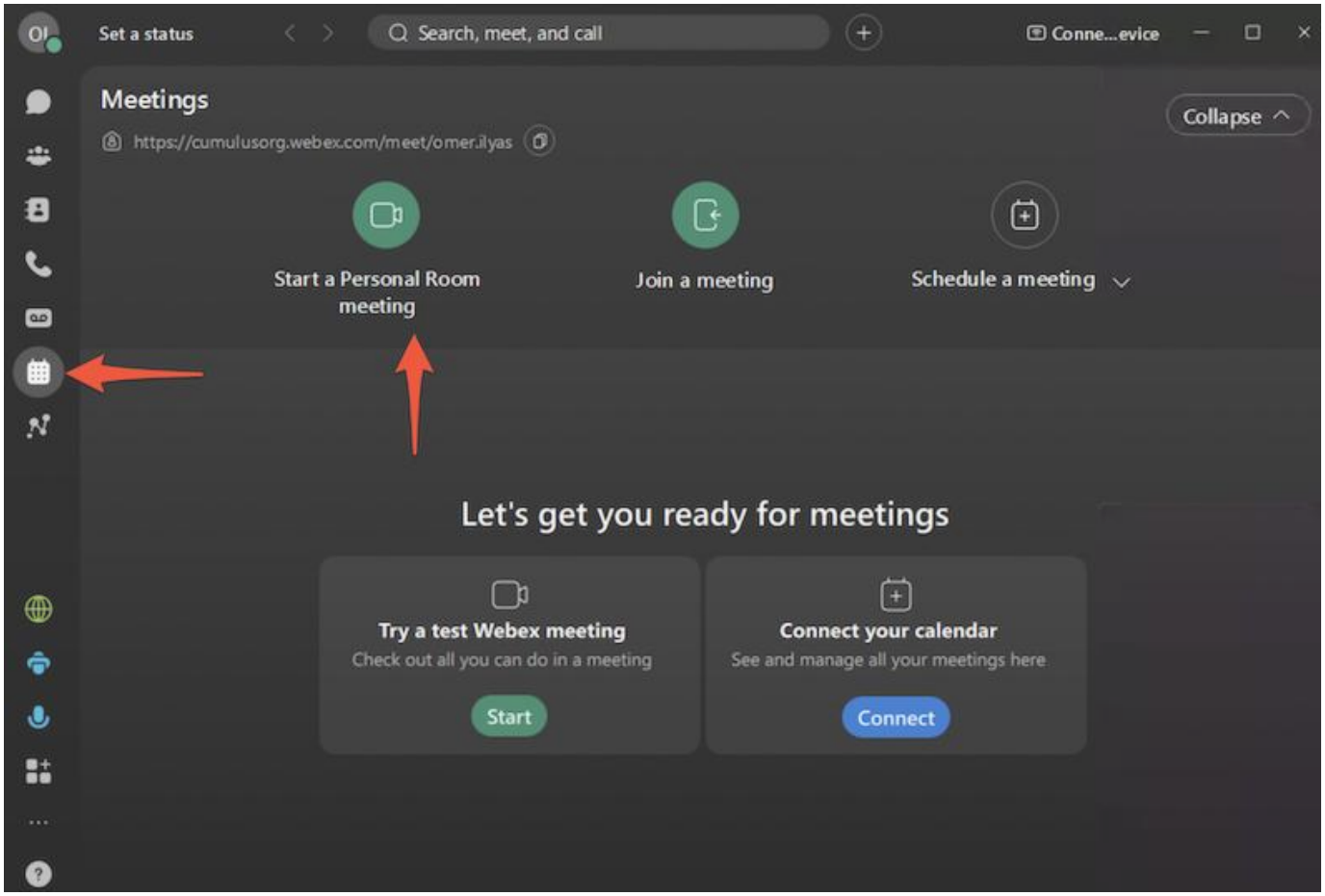


Navigate back to your VM web browser tab and click on the Webex icon then sign in using the email address and password from your character.

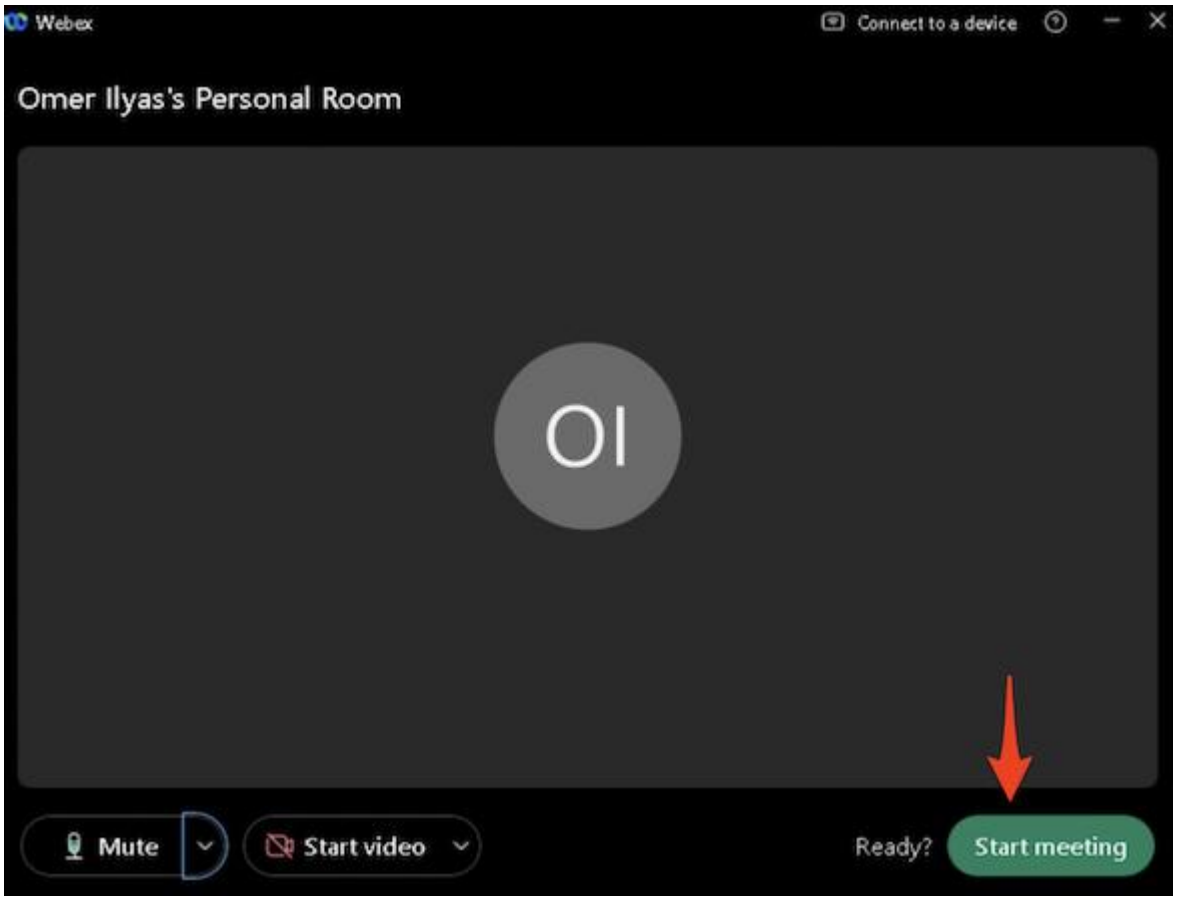




Click the **Webex icon** on the task bar. Click **Meetings**. Click **Start a Personal Room meeting**. **Note** Your WebexApp might do a quick update.



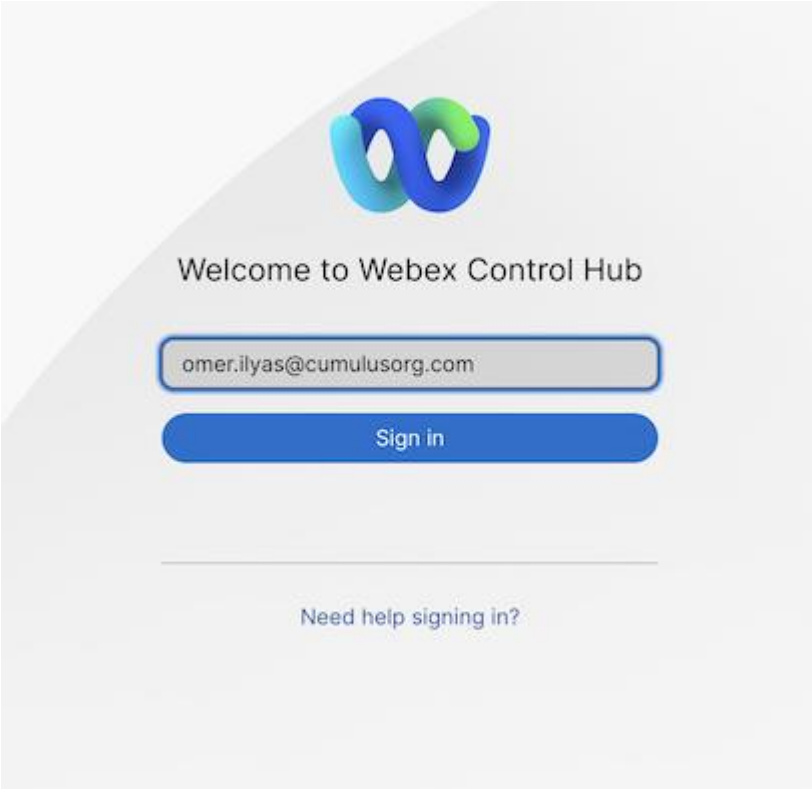
Click **Join meeting** and then click **Start meeting**.



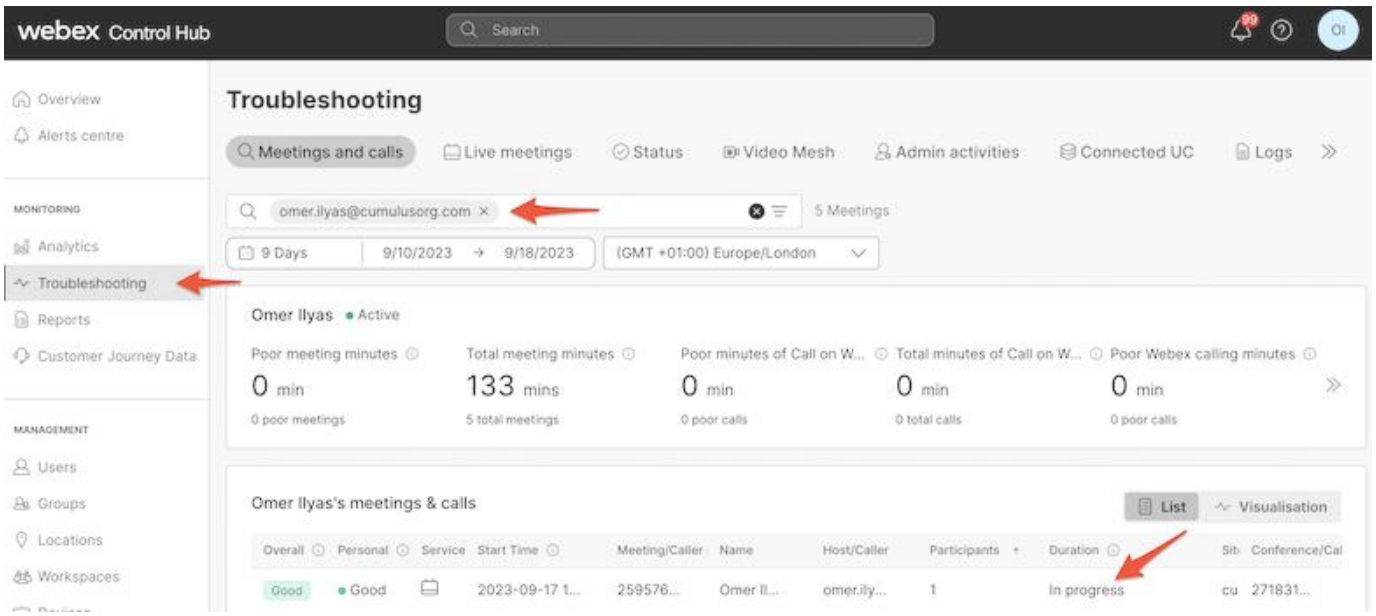
This will generate Webex traffic which you will view later in the lab. **Note:** Since no one is joining the meeting it may have a pop up after a while warning the meeting will end unless you click to keep it active. Feel free to click to keep it active or you can add another participant in that meeting or you can always go back and **Start a Personal Room Meeting** again.

1.5.2 Login to Webex ControlHub

Once the user join a meeting you can login into Webex Control Hub using the (read only admin) credentials provided.



Click on **Troubleshooting** search for your **userid** that you have used to join the Webex meeting.



1.5.3 Locate your ThousandEyes EPA

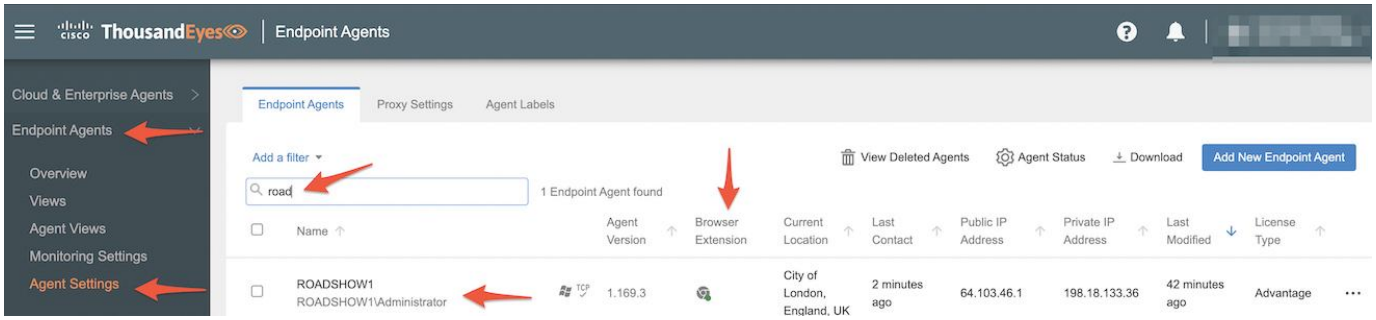
By now you have your ThousandEyes Endpoint Agent running. Let’s verify it has connected to the ThousandEyes Platform.

Navigate back to your incognito browser that is logged into ThousandEyes.

Click **Endpoint Agents > Agent Settings** (if you were already in the tab you may have to click **refresh**)

Search for your EPA

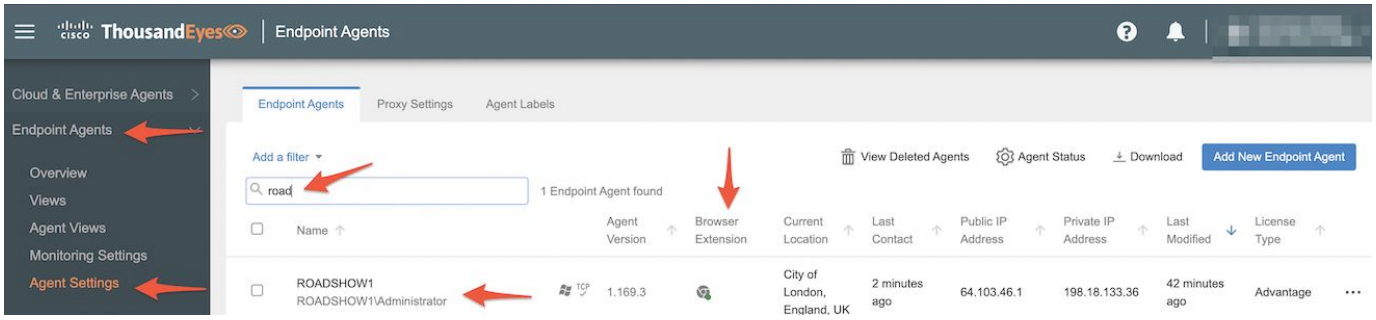
- In the search bar type the name you gave your VM (if it doesn't show up contact a lab proctor). Also verify that the Google Chrome Browser Extension shows up as shown in the below screen shot.



If your Google Chrome Browser Plug-in didn't install. (Note sometimes it take a minute to show up. Please refresh the browser.) Navigate back to your **VM** and click on the **Google Chrome** icon on the task bar.

- Install the Google ThousandEyes Google Chrom Plug-in by pasting this link in your Google Chrome Browser
- https://chrome.google.com/webstore/detail/thousandeyes-endpoint-age/ddnennmeinlkhkmajmmfaojcnpddnpgb

If asked Turn on Sync. Navigate back to the incognito browser logged into ThousandEyes and your ThousandEyes EPA should look like the one below.



You are now ready to continue your journey see how AST (Automated Session tests) can automatically monitor Webex meetings. Customize and see how your EPA monitors browser sessions and set up scheduled tests to montior the health of critical applications in the background. Scheduled tests are a great way to provide a baseline for application and network health. The browser sessions provide the view of what the end users session is like when sites are accessed in the domains you are interested in monitoring. And Automated sessions tests will integrate with Webex and monitor traffic automatically whenever a user joins a Webex meeting from Webex App or the RoomOS devices. Let's carry on with Task 5.

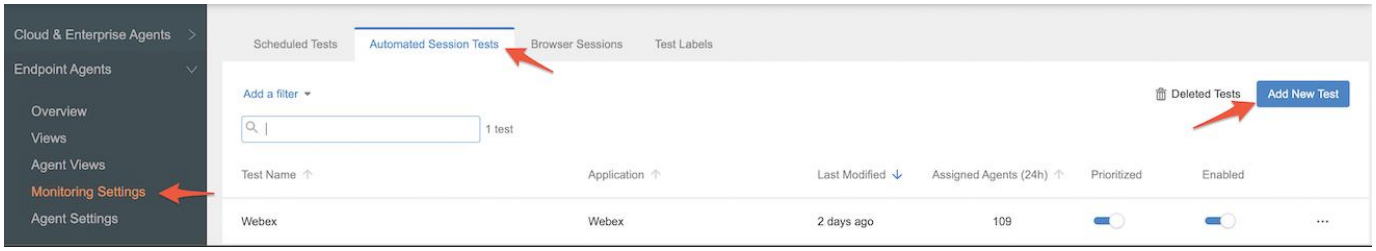
1.6 Task 5: Configure ThousandEyes Automated Session tests and EPA Monitoring

1.6.1 Set up Automated Session tests for Webex Meetings - Optional Step

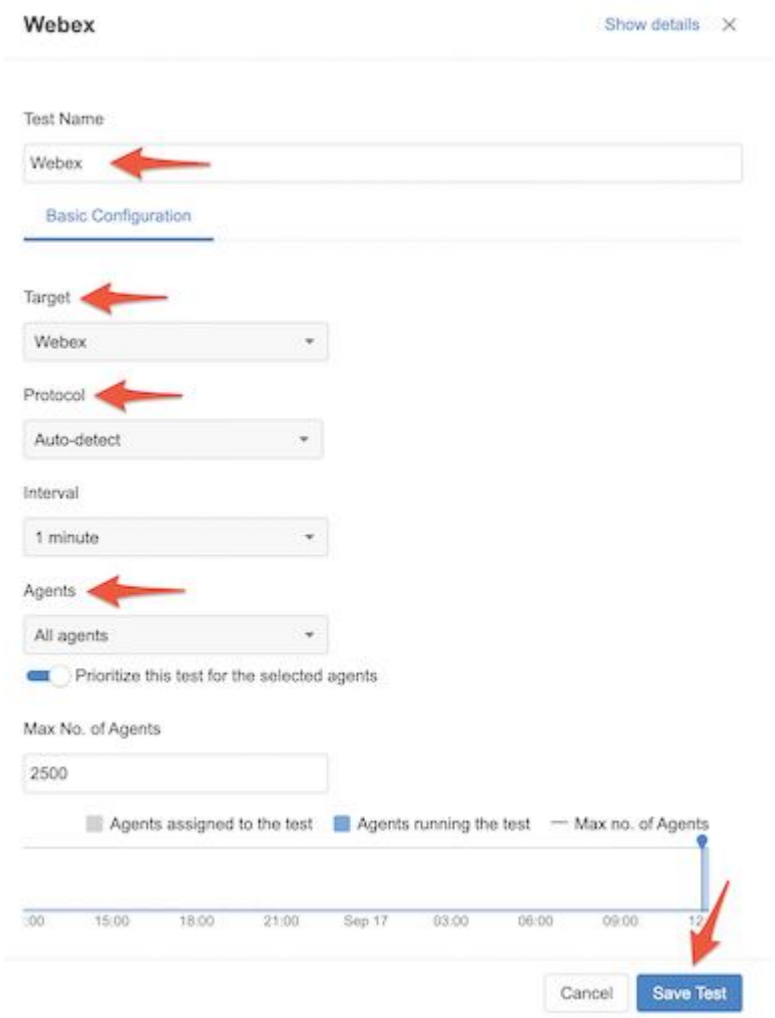
Automated Session Tests enable the Endpoint Agents installed on your workstations to monitor and identify network connections between a user's application and the destination node (Webex); thereby, removing the ambiguity of knowing whether the IP addresses created in synthetic tests are going to the right datacentre or service. Automated Session Tests capture the performance of a desktop application e.g. Webex App, without you having to manually configure an IP address or hostname for the application.

Note: The below configuration steps are for information purpose only

- Navigate to the Endpoint Agents > Monitoring Settings > Automated Session Tests tab.
- Click the Add New Test button.



- Create an AST to monitor Webex Meetings in your organization



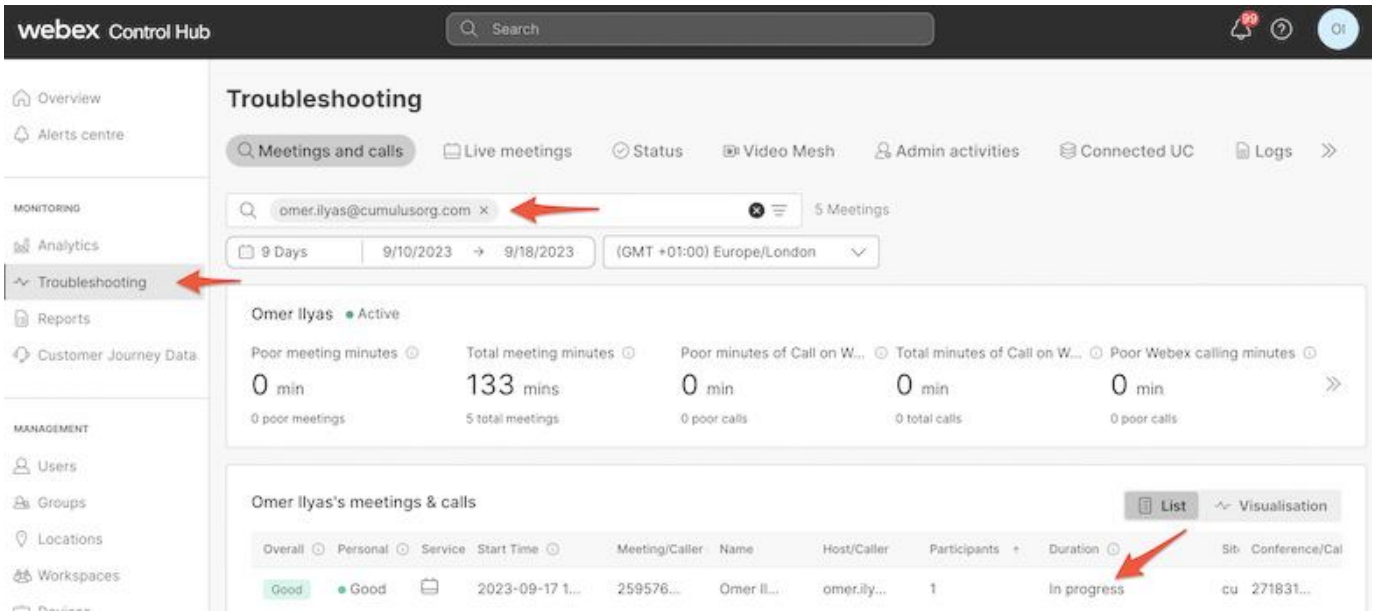
Note: The above steps have already been configured. Showing for **information purpose** only.

Note: More info can be found on Webex help that explains how to create a configuration between ControlHub and ThousandEyes platform.

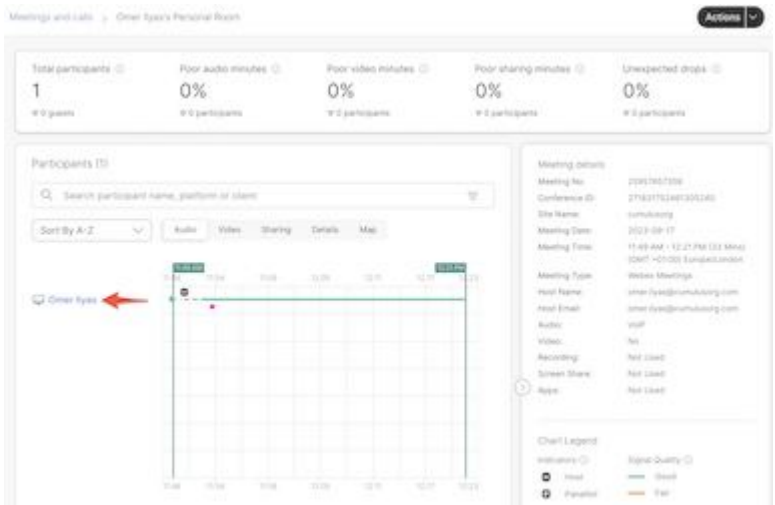
When the user (that was created by you) initiate and join a Webex meeting from the WebexApp, you be able to view the ThousandEyes path in ControlHub troubleshooting section.

- If you have logged out, log back in ControlHub using Readonly admin creds provided . Click on Troubleshooting, search for your userid that you have used to join the Webex meeting and click the meeting that is in progress.

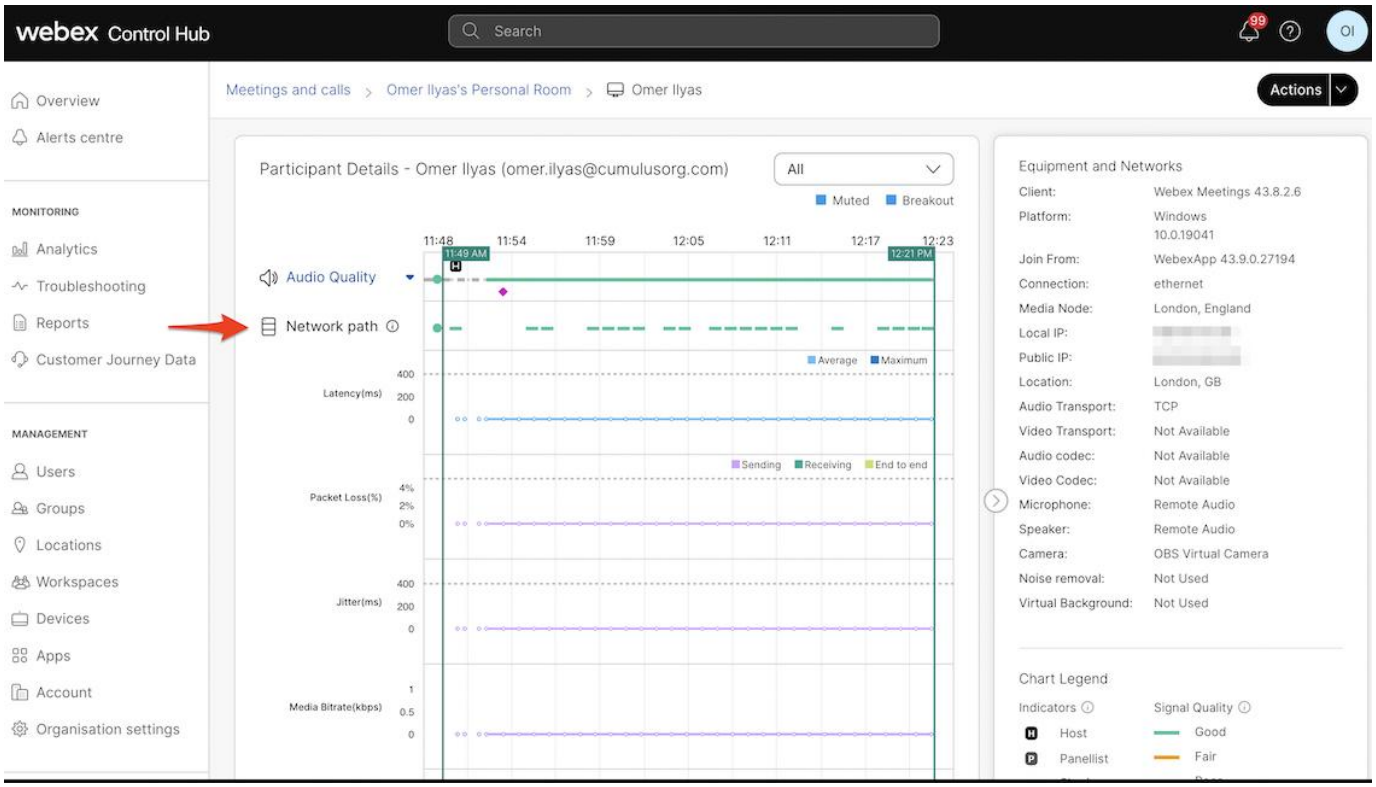
Note Make sure the Webex meeting is still going on in the virtual machine. As you are the only participant, it will disconnect in some time. If disconnected, please start the meeting again.



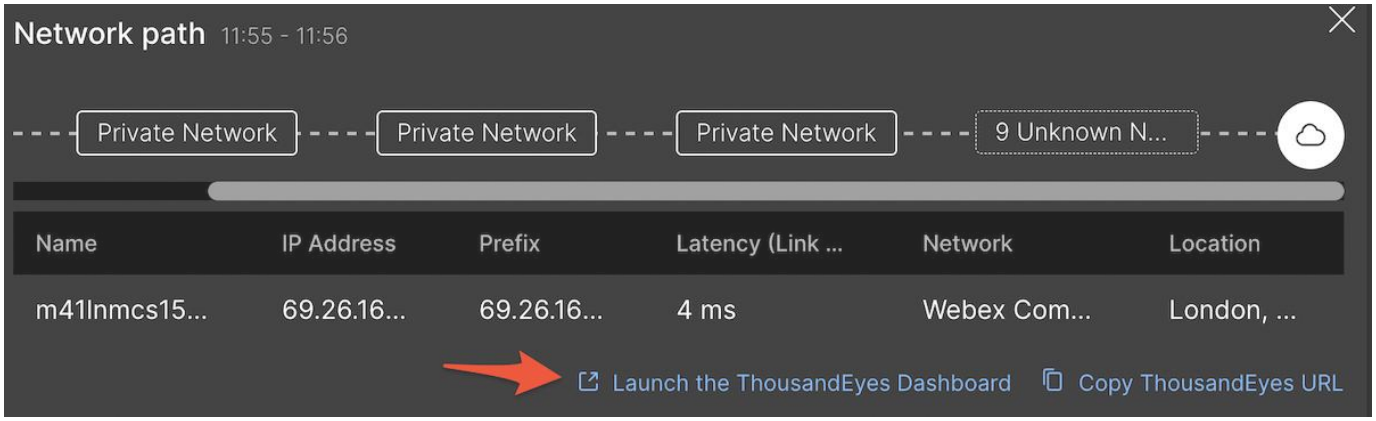
- Click your demo user id



- You will notice ThousandEyes path. **ThousandEyes AST** starts capturing network path data as soon as the meeting starts. However, there could be a delay of up to five minutes before that data populates in Troubleshooting section.



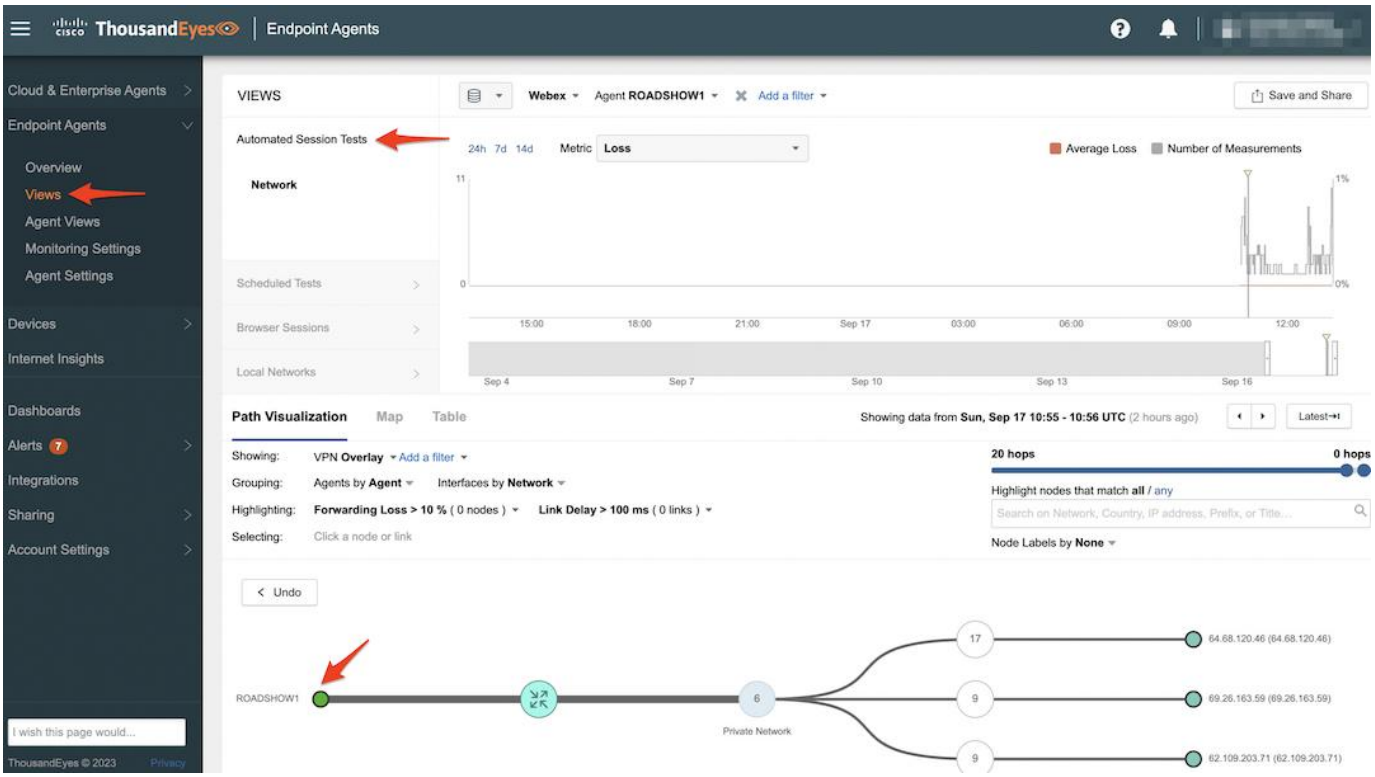
• The network path route shows the details for each node that the hop connected to. Click on any of the dotted lines



• You can hover over a dotted line to see the user's latency (round-trip) average value during that interval. The color changes depending on the threshold that the value met. Thresholds in Webex are are calculated as:

```
- Poor (red)—Latency > 400ms or Loss (round-trip) > 5%
- Good (green)—Latency < 300ms or Loss (round-trip) < 3%
- Fair (yellow)—Neither of the above.
- Unknown (grey)—Not available yet. You still be able to retrieve the metric from the TE dashboard.
```

• You can also click on **Launch the ThousandEyes dashboard** . It will cross-launch from the Webex ControlHub Network Path into ThousandEyes platform. You will be navigated to the Automated Session Tests view, which is found within the **Endpoint Agents > Views > Automated Session Tests** section of the web application. The view is pre-filtered to the corresponding user and time segment from Webex Control Hub.



1.6.2 Understanding Scheduled tests

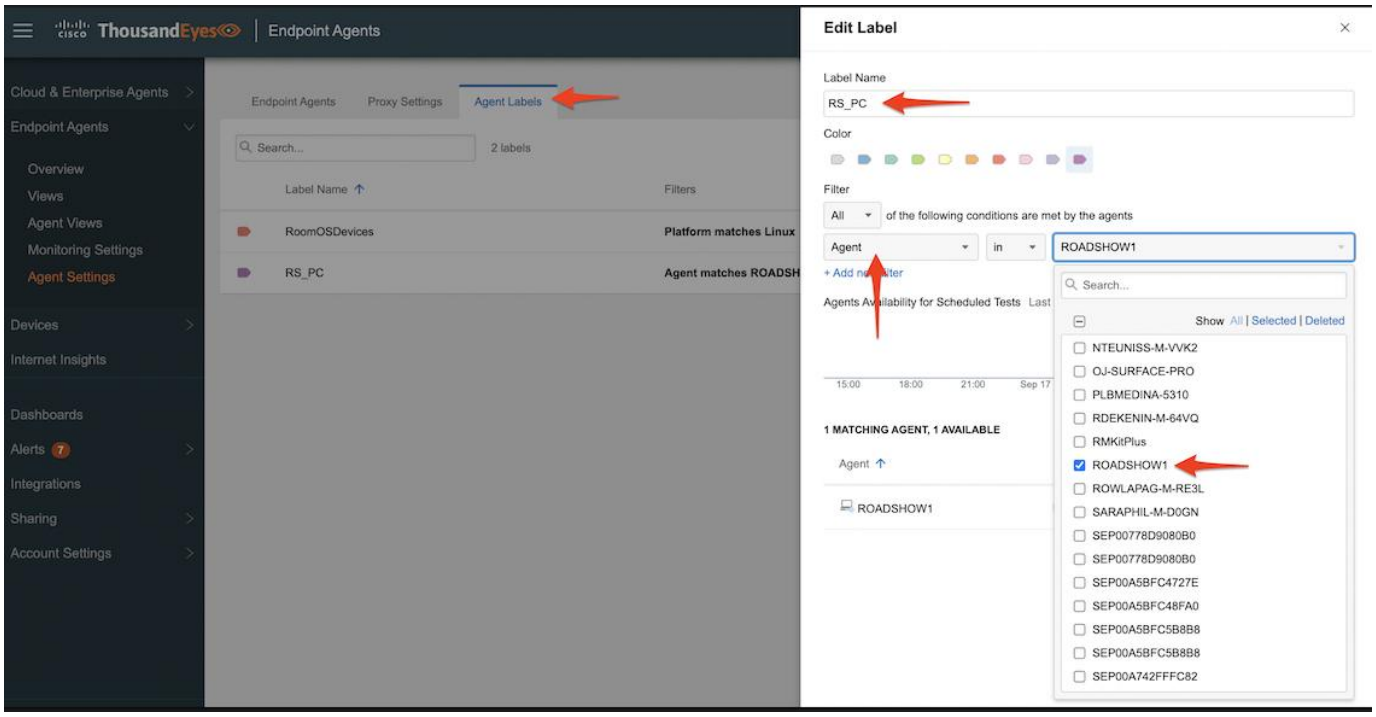
Before setting up scheduled tests it's a good idea to create an Agent Label and assign your EPA to it. Labels are a super powerful way to dynamically manage how ThousandEyes Endpoint Agents are configured for testing and reporting.

For more information on Endpoint Agent Labels check out our documentation.

Click the **Agent Labels** if you are still viewing your EPA otherwise navigate to **Endpoint Agents > Agent Settings > Agent Labels**.

Click **Add New Label**. Name the label e.g RS_PC, select any color.

In the Filter section select **Agent in** and use the pull down to select your agent (note you can use the search field to quickly find your agent). Click **Save**. See the image below for and example of how to add your agent to your label.



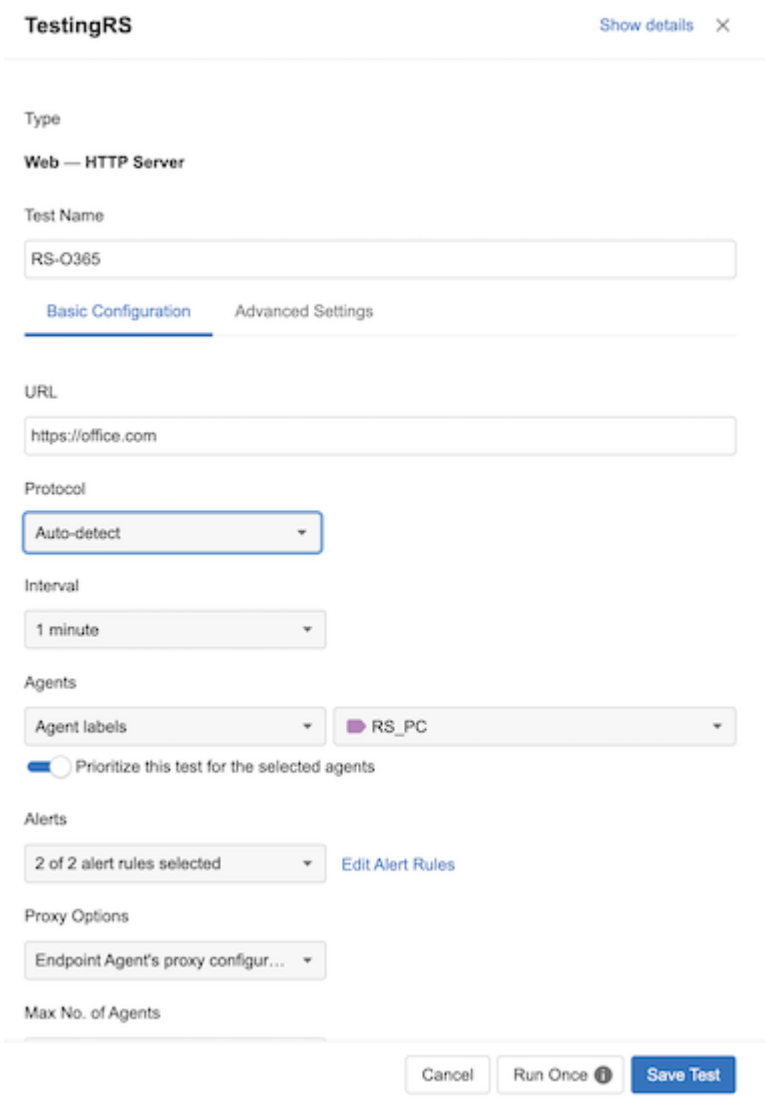
1.6.3 Set up Scheduled Tests for your ThousandEyes EPA

You will build a test that will run every minute to https://office.com for this lab but feel free to build other tests. You can have up to 10 tests run on an EPA.

Navigate to **Endpoint Agents > Monitoring Settings**

Click **Add New Test**

- Type Web, HTTP Server (this is the default)
- Test Name: Set a unique name
- URL: https://office.com
- Interval: 1 minute
- Agents: Agent label then select the label you created
- Click the prioritize slider (as this is an important test)
- Click **Add New Test** (note you can also Run Once but if you do this don't forget to save the test!)



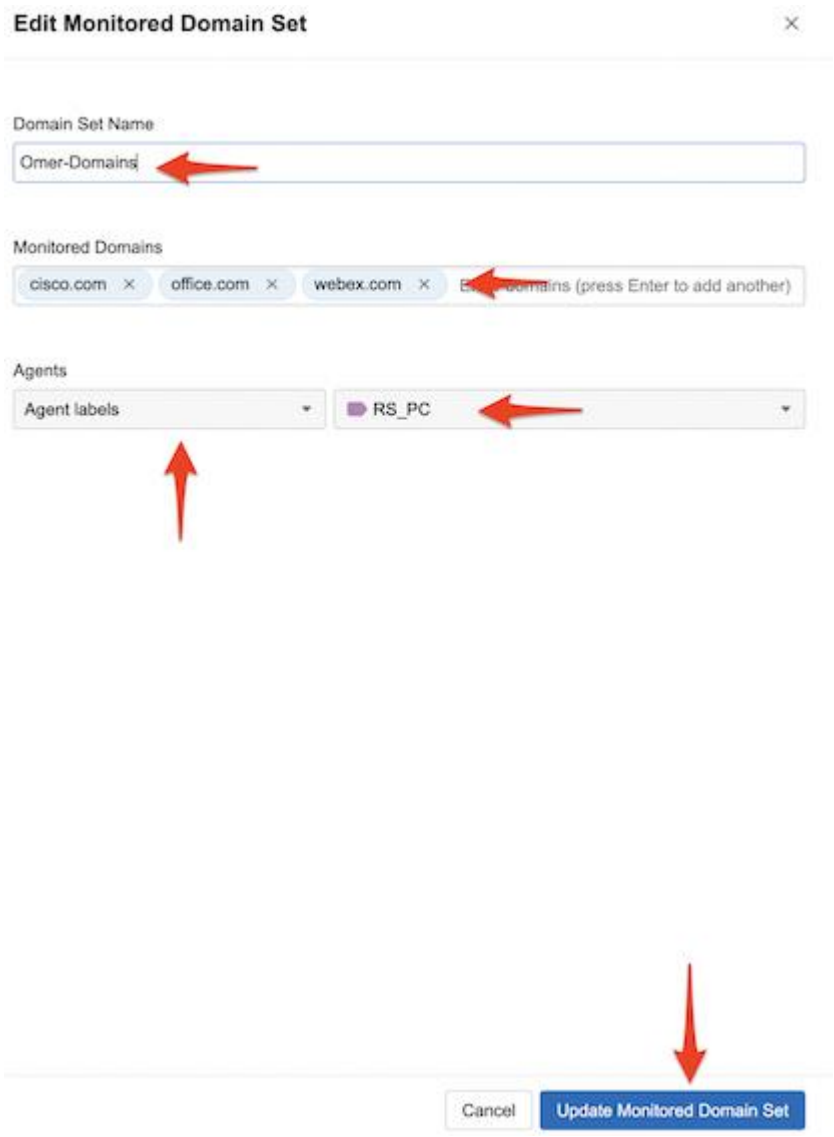
1.6.4 Set up Browser Sessions for your ThousandEyes EPA

Set up domains to be monitored when the browser on the Windows VM accesses them (Note: Only Chrome, Edge or IE 11+ browsers are supported). Typically these consist of the domains that are critical for your users and businses operations. You'll see shortly how powerful this can for troubleshooting users issues.

Navigate to **Endpoint Agents > Monitoring Settings > Browser Sessions**. For more information on Browser Session monitoring click here.

Click **Add New Monitored Domain Set**

- Domain Set Name: Set a unique name
- Monitored Domains: office.com, webex.com, cisco.com (feel free to add in other domains)
- Agents: Agent Labels and select your agent label that you created earlier
- Click **Add New Monitored Domain Set**

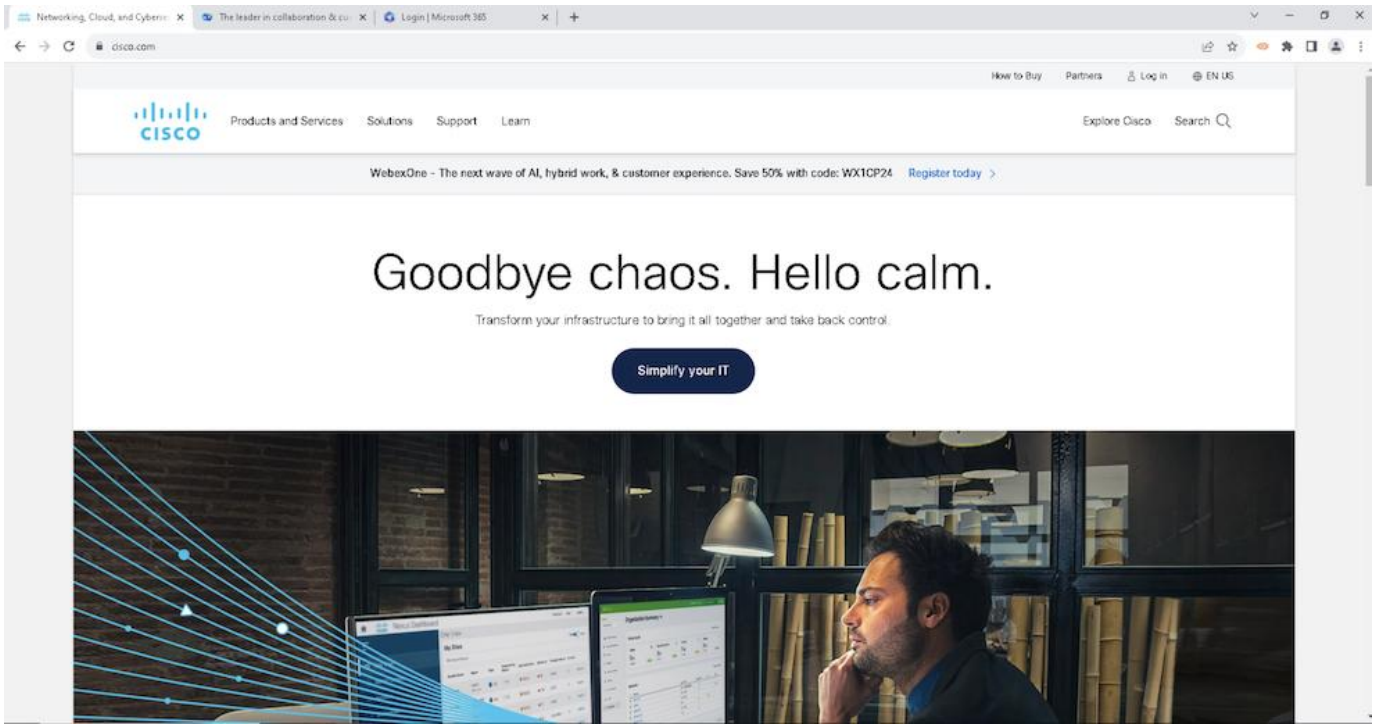


1.6.5 Automated Sessions Tests (AST) for your ThousandEyes EPA

1.6.6 Navigate back to your VM

Open the Chrome Browser and navigate to the domains you set for browser sessions. Open a tab and bring up a site in each tab:

- https://cisco.com
- https://webex.com
- https://office.com



Click refresh on each tab a few times to create some extra sessions. Do this for a few minutes randomly to generate web browser traffic which we will analyze later. If you need to test out having browser traffic randomly generated to a site or set of sites a great chrome plug in to use is Auto Refresh Plus. We won't go into configuring or installing it for this lab.

You should have some good data captured with the Webex session running in the background on the VM being catpured with the Webex AST, the scheduled tests runing in background providing a baseline and then the browser sessions. Time to move onto Task 6 and start analyzing the data!

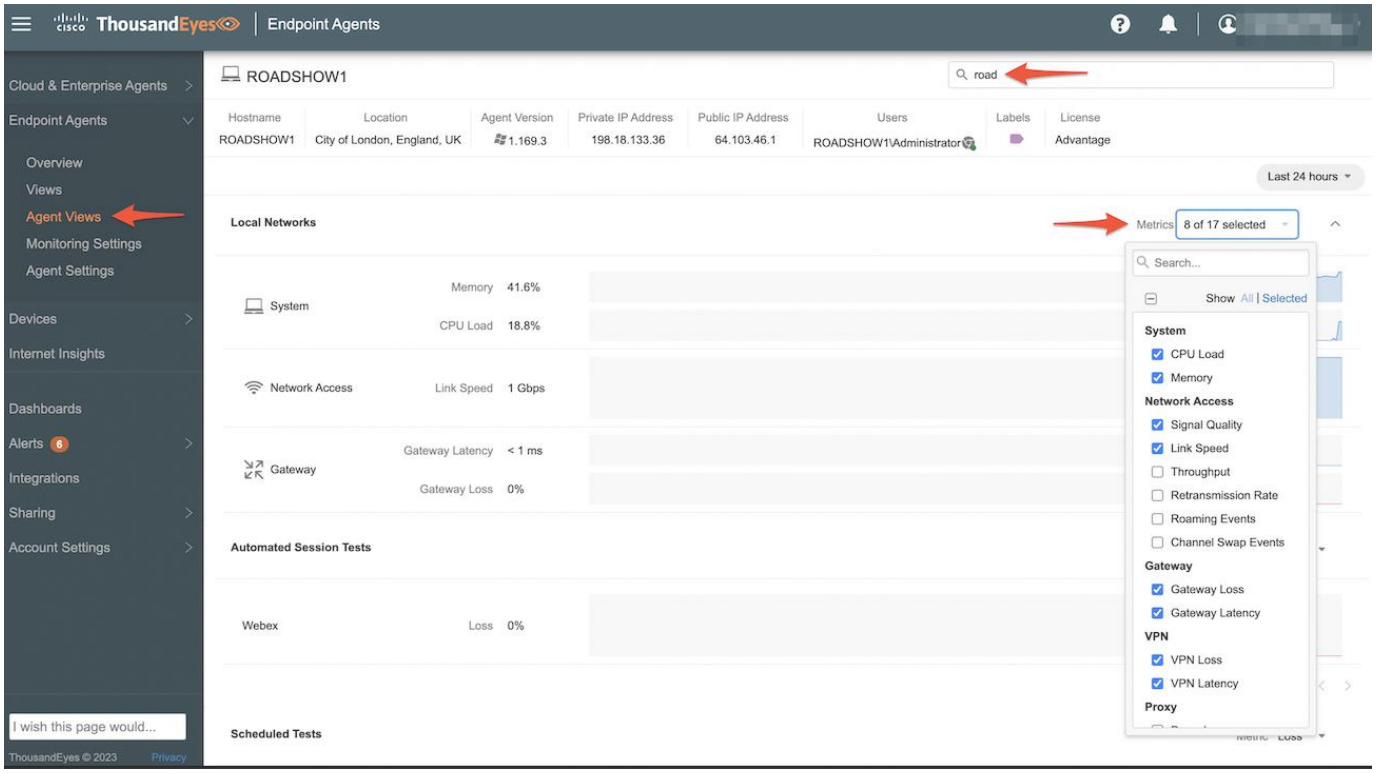
1.7 Analyzing ThousandEyes EPA Data

Typically when a user experiences an issue they will either suffer in silence, wait for the issue to go away and when it crops up again get frustrated and call in for help. Sometimes while they are working with support or the helpdesk the issue resolves itself. This makes it really difficult to troubleshoot issues if they aren't presistent. ThousandEyes stores 30 days of data so you have the abilty to go back in time and see what was occuring or see if this issue has been occuring and the user just didn't call into support.

If you are troubleshooting a issue and want to quickly see all the test data for a users system **Agent Views** provides the perfect visualization.

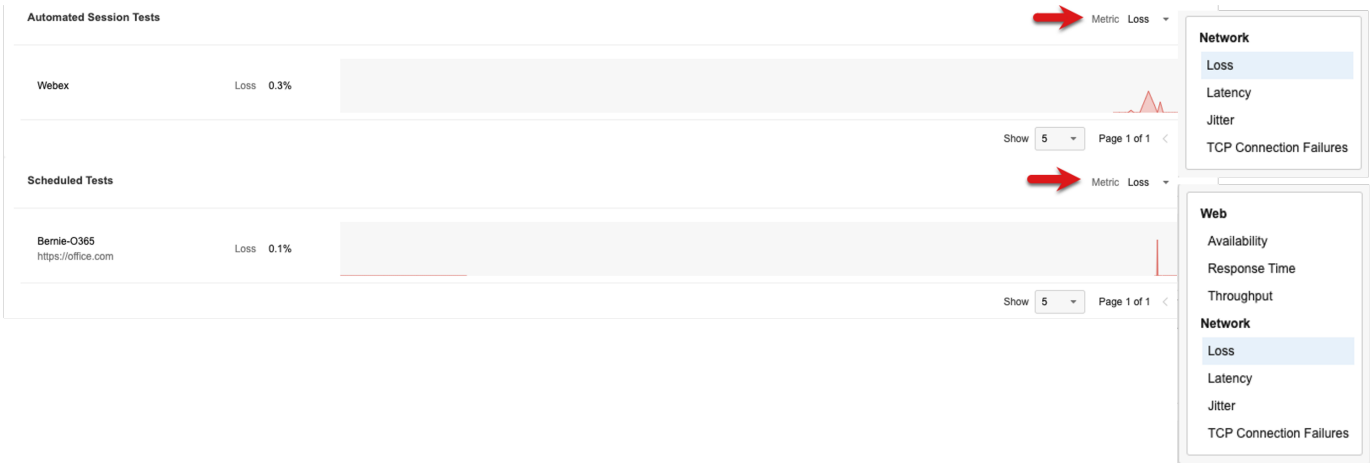
Navigate to VM session and browse to ThousandEyes portal. Open **Endpoint Agents > Agent Views** (be sure to use the incognito browser). Use the search box to find your agent which will be what you named your VM. Then you can begin to explore the metrics and tests. The top section contains your system's performance metrics.

- Use the Metrics pull down to view the different system metrics



The middle section shows Automated Session Tests (ASTs) and Scheduled Tests (up to 10 max).

- Use the pull down to view the different web and network metrics.

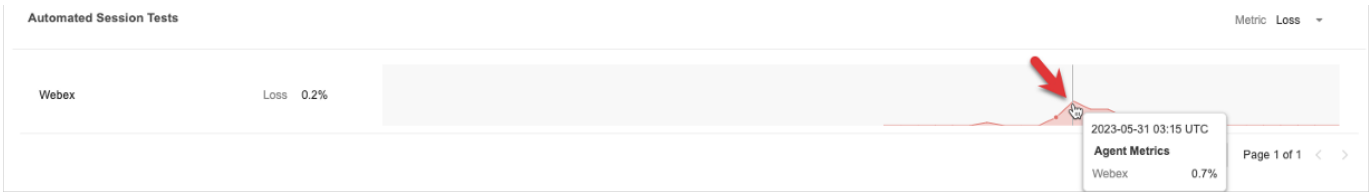


The bottom section shows browser sessions. If you don't see anything you might need to refresh the tabs in your VM's browser a few extra times or refresh the Agent Views page.

- Use the pull down to view the different browser and network metrics.

1.7.1 Drill into a Automated Session Test

Now that you've explored the Agent Views page click on the AST metric to dive into the detailed view associated with the Webex Test. If you don't have any network loss try changing the metric to latency.



You will now see a filtered view for your agent showing the network path which is dynamically created based on the endpoints your Webex session is connected to while the Webex session is running.

Here's an example view. I used the upper right **Save and Share** feature to create a snapshot that anyone can view for a full year! This can be very helpful as it can be attached to tickets, shared with the end user, anoter team or a service provider. They will see what you see making it simple to collaborate and reduce any finger pointing. (think back to the last slide in the ThousandEyes Overview).

- Open the snapshot in another browser tab
- You can mouse over the nodes for extra information
- Try changing the metric and drag over and navigate the time bar to see how the test changes

From this same view you can change the grouping to show IP Addresses and adjust the number of hops to get more a granular hop by hop network path.

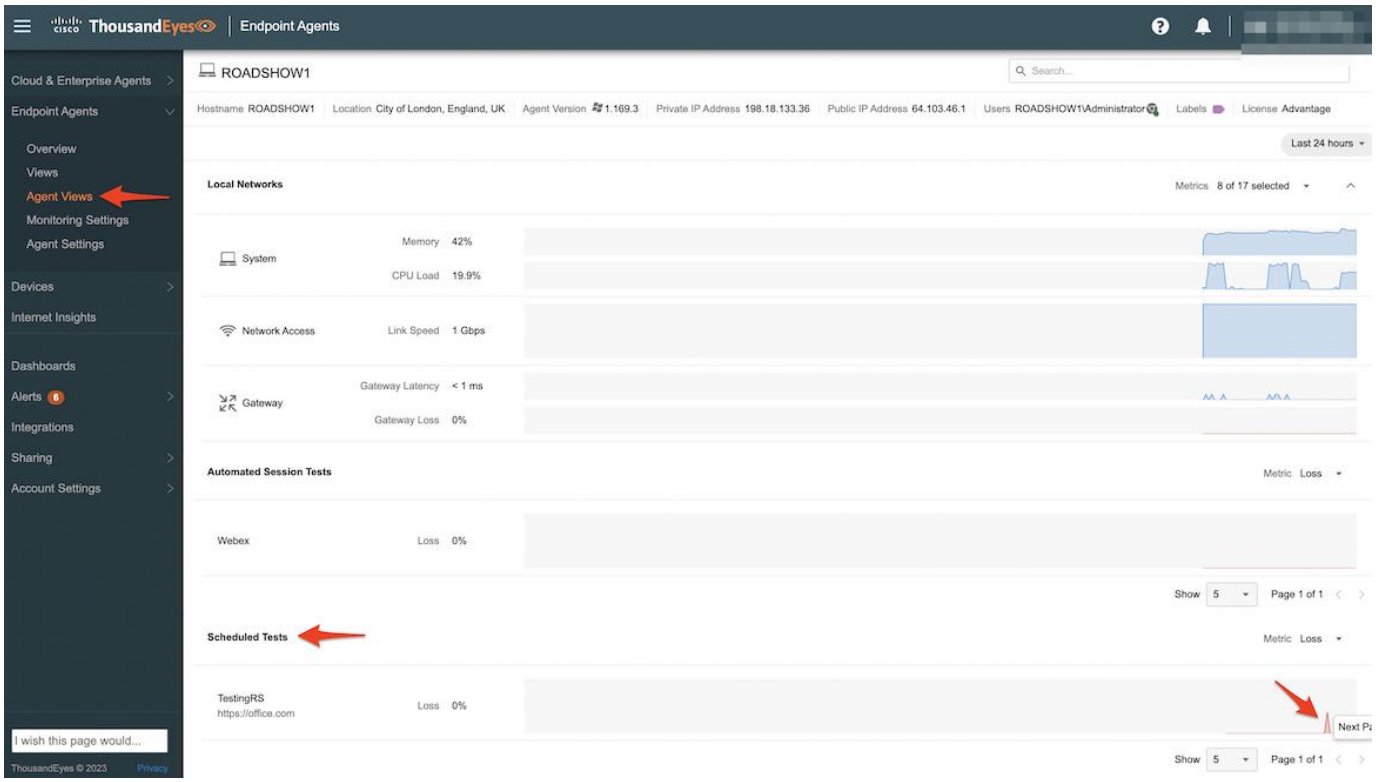
- You can mouse over the nodes and links for extra information.
- You can also adjust the link delay. In the below screenshot used 10ms. You can also click on the 8 links to see all links highlighted that are over 10ms.

Feel free to navigate back to your Automated Session Test view showing your agent and click around to expermiement with how to see similar data.

1.7.2 Drill into Scheduled Tests

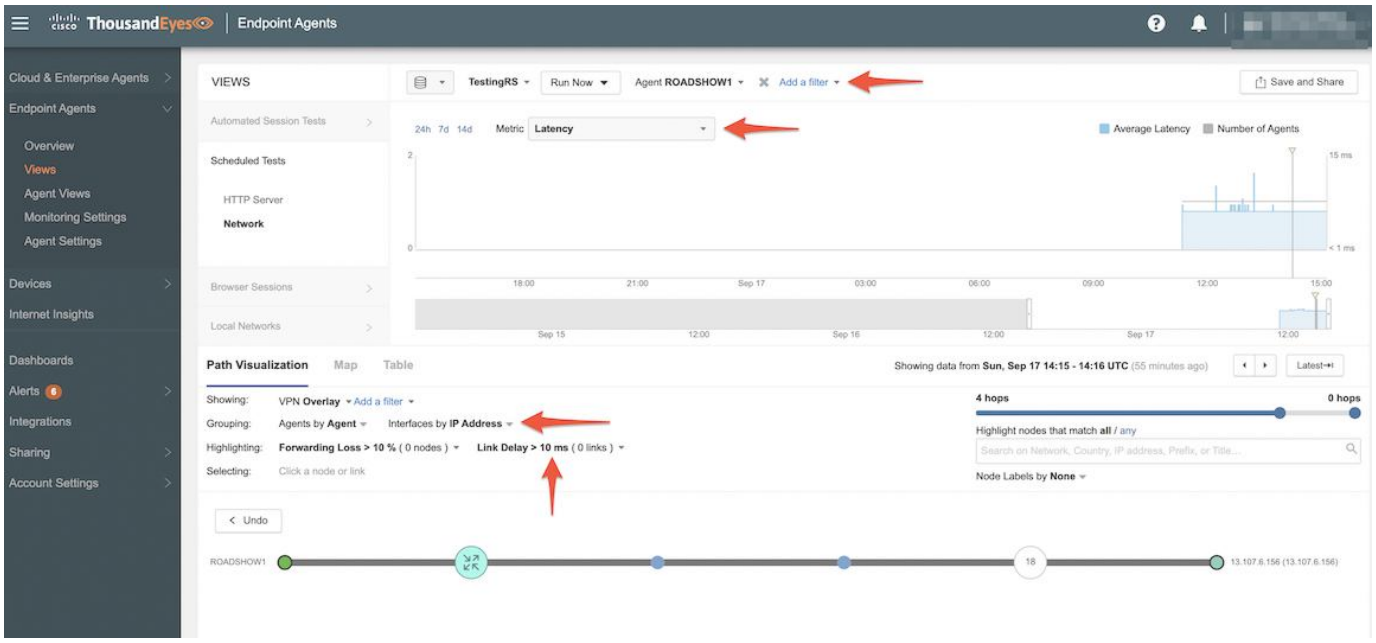
Scheduled tests provide a consistent baseline. Whenever an Endpoint Agent is online the test runs at the specified interval. Navigate back to **Agent Views** and search and select your agent.

- Click **Agent Views** and use the search box to find your agent.
- Click into the scheduled test to drill into a filtered view. (If you set up other scheduled tests feel free to use one of them instead)



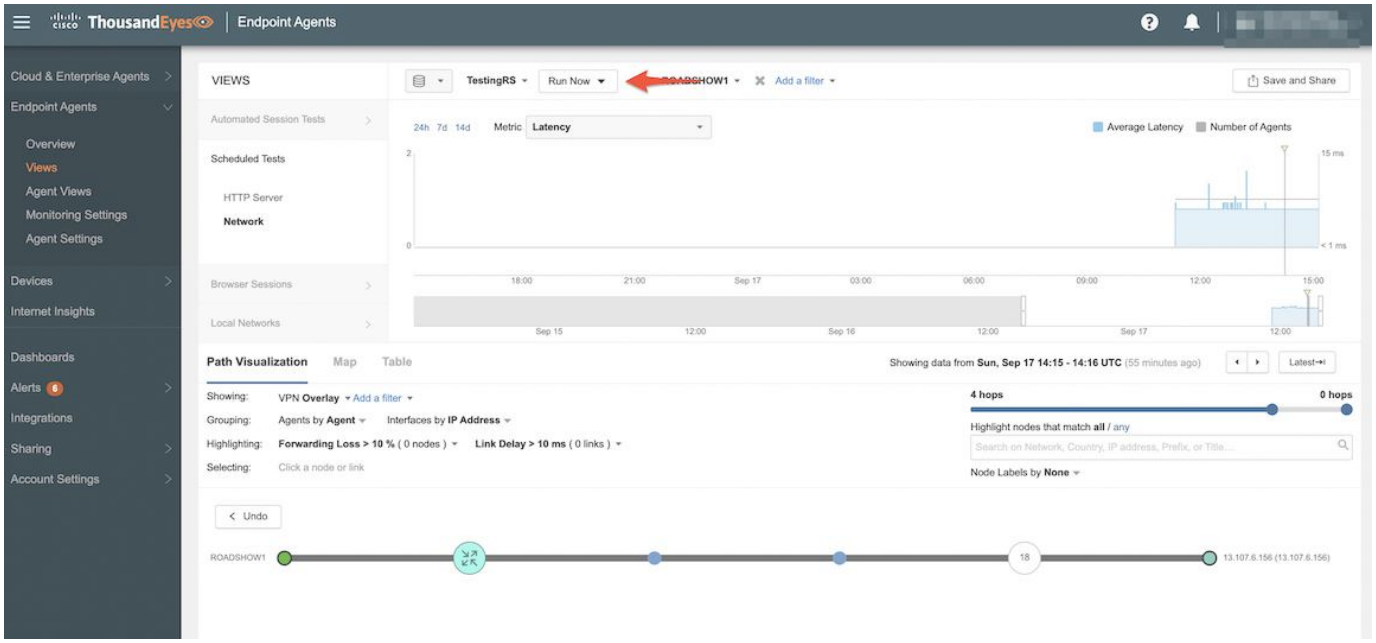
Now you're in a filtered test view. Note the filters at the top of the screen showing the test and your agent. See the below screen shot as an example.

- Adjust the metric to latency and change the grouping to IP Address
- Adjust the hops to max using the slider
- Set the link delay to 10ms and then click on the links to highlight them in the network path



If you wanted to see all agents that are runnig the scheduled test you could just remove the agent filter (this won't work in this lab as we have only one agent). This would be a great way to figure out if an issue is effecting multiple users or start to isolate the users that are having issues as they might all be in the same building or connecting through the same router that is causing congestion, latency or loss. You can also right click on the agent to pull up the traceroute which is run every time the test is executed.

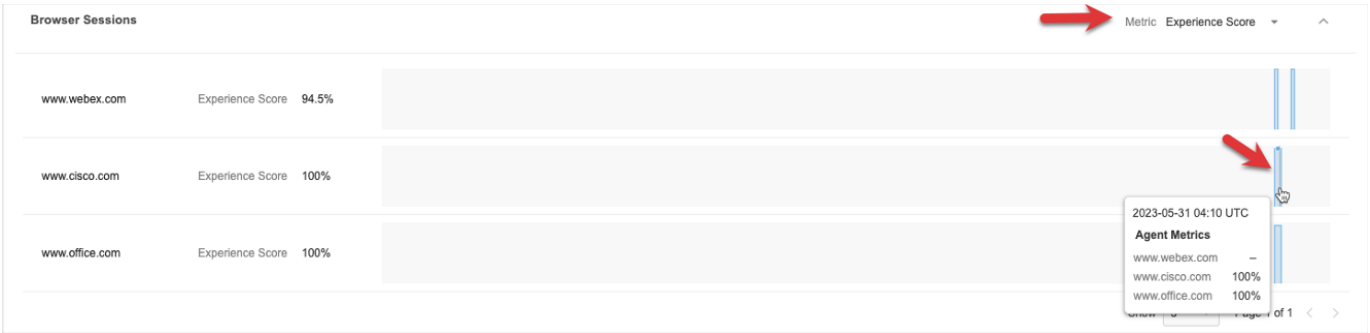
Another powerful feature is the **Run Now** option for when you are actively troubleshooting and need test results right away or you can make changes and run it. Feel free to test it out.



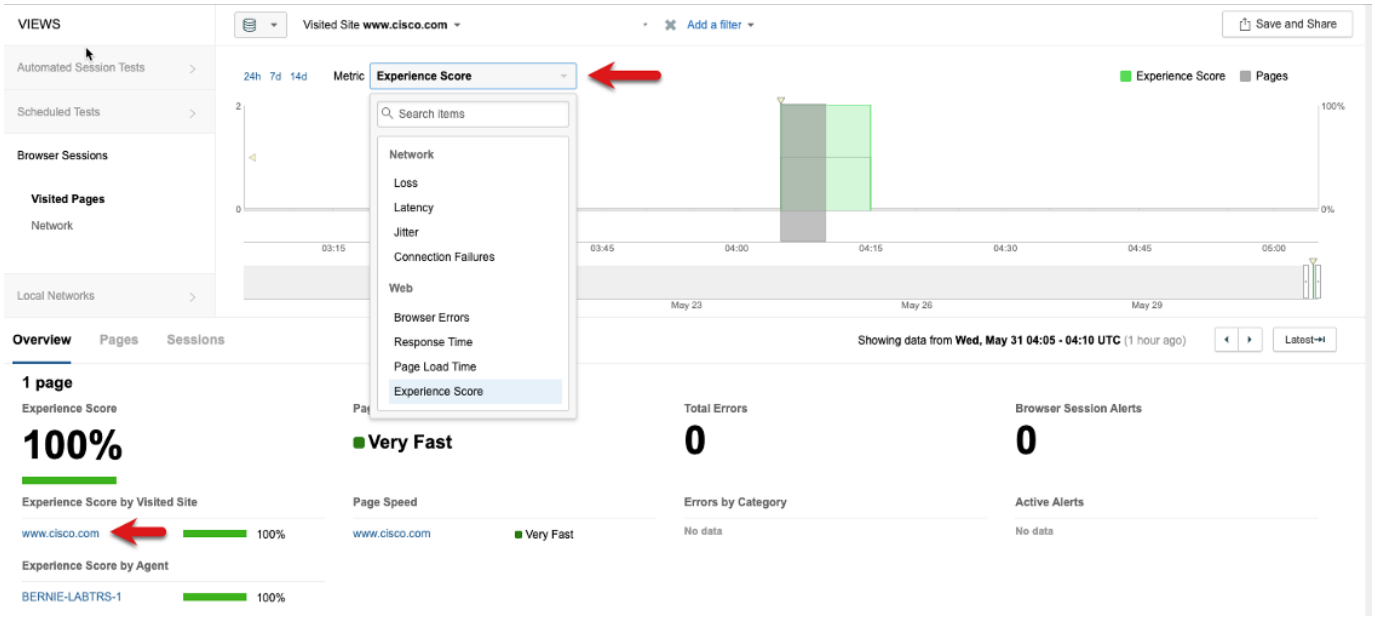
Note: It might take a few minutes for the test to complete and then be processed for visualization. So you may want to kick it off and then continue on with the lab and come back to the tab in a few minutes.

1.7.3 Drill into Browser Sessions

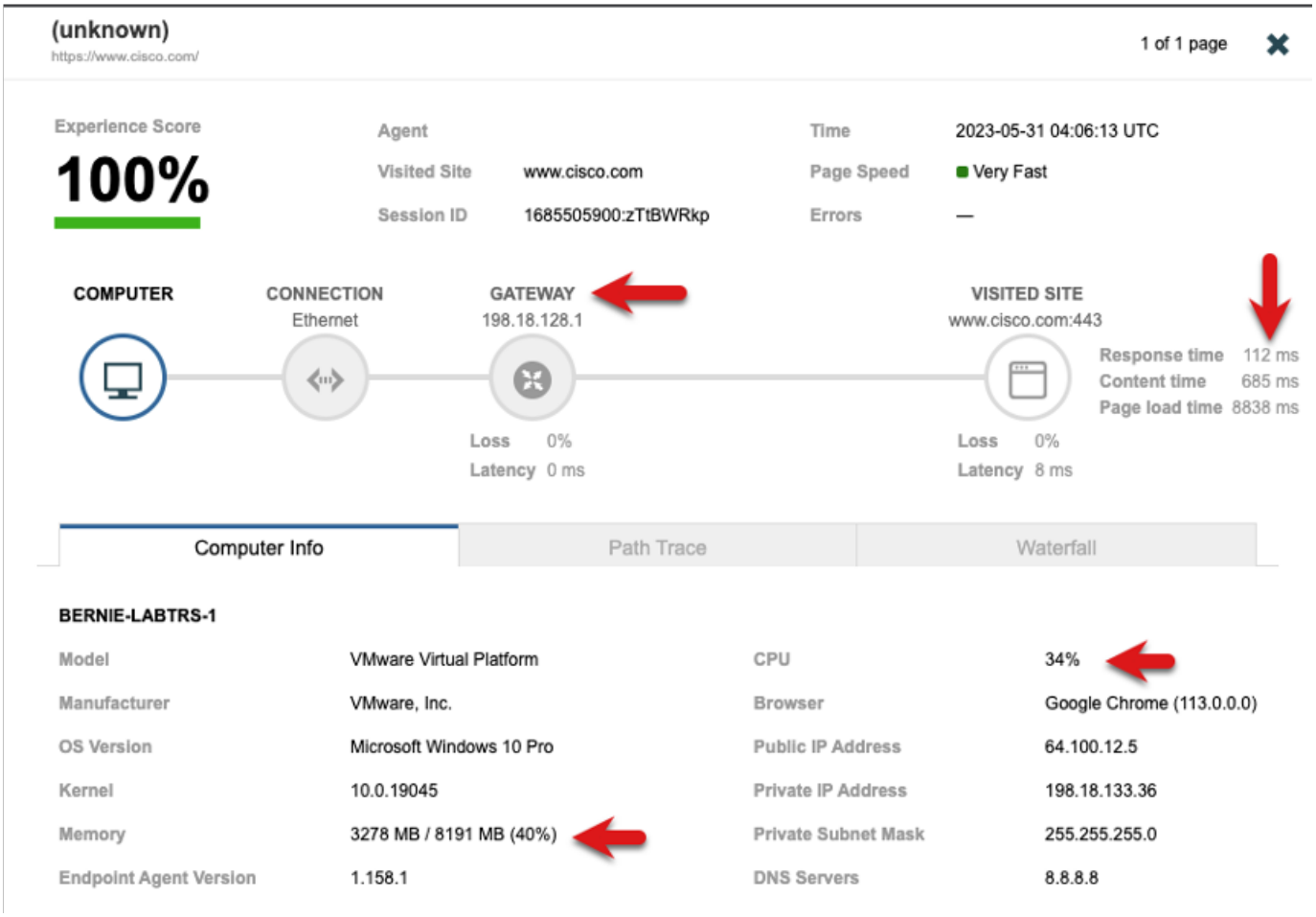
Browser Sessions are generated using the browser plugin and will monitor the user experience and network path for your monitored domain set. The experience score is a calculated metric to help gauge the end users web performance. You can change the metric based on what you are wanting to use for troubleshooting. Navigate back to **Agent Views** and search and select your agent. Click on the **www.cisco.com** session to drill into a filtered view. Note if your browser sessions aren't showing up, verify your agent is associated with the agent label and then make sure to go back to the browser and refresh the tabs.

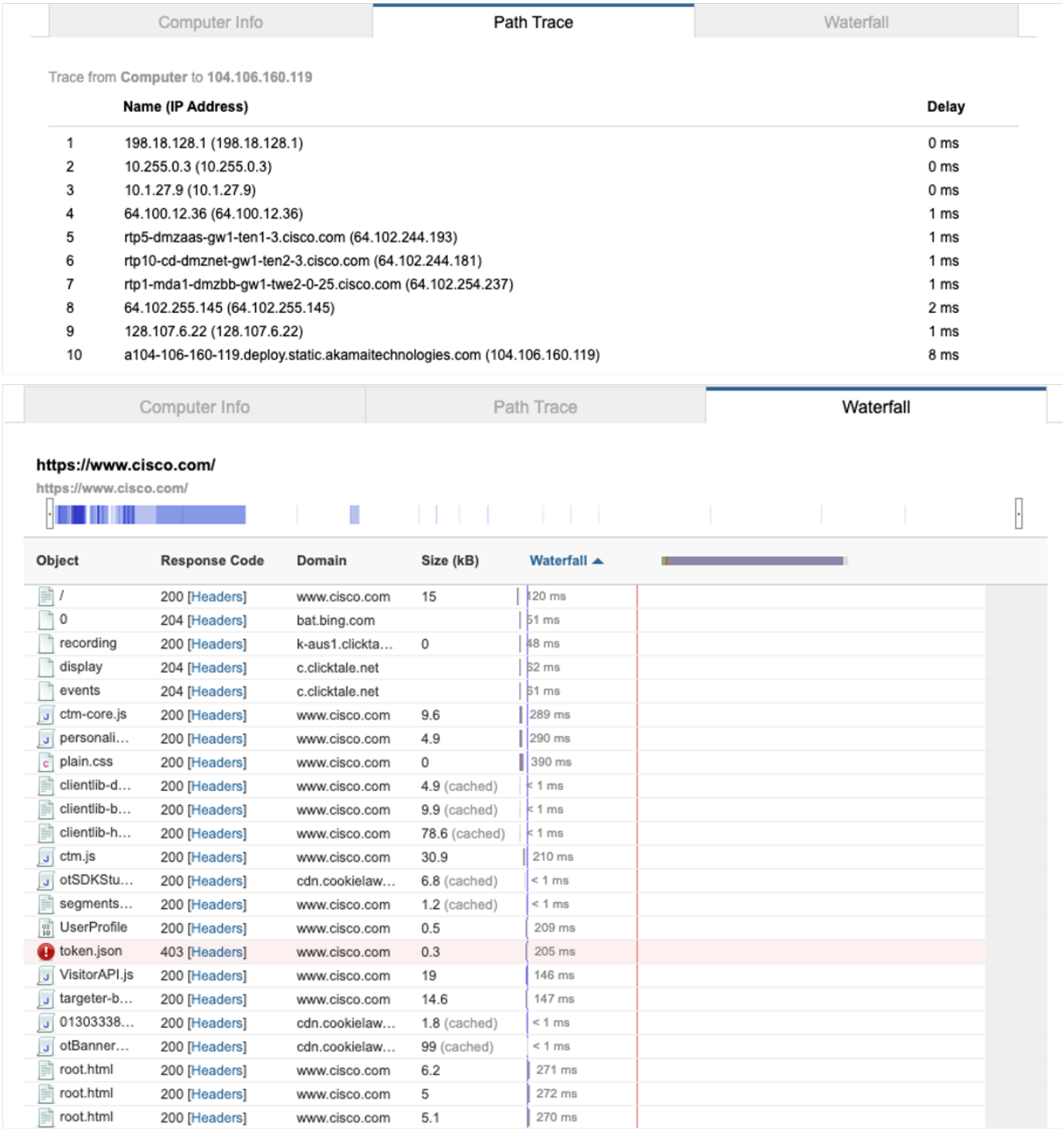


The browser session view shows the visited pages and experience score. See the below screenshot for an example. Note the filter for the Visited Site and Agent which was automatically applied based on the browser session test you clicked from the **Agent View**.



You can easily explore the other metrics from the session. Click on the web site to bring up the session, system and network details and review the tabs for the path trace and waterfall details. Additional metric will be pulled in based on how the Enpoint Agent is connected to the network like wireless, vpn or proxy.





Computer Info | Path Trace | Waterfall

Trace from **Computer** to **104.106.160.119**

	Name (IP Address)	Delay
1	198.18.128.1 (198.18.128.1)	0 ms
2	10.255.0.3 (10.255.0.3)	0 ms
3	10.1.27.9 (10.1.27.9)	0 ms
4	64.100.12.36 (64.100.12.36)	1 ms
5	rtp5-dmzaas-gw1-ten1-3.cisco.com (64.102.244.193)	1 ms
6	rtp10-cd-dmznet-gw1-ten2-3.cisco.com (64.102.244.181)	1 ms
7	rtp1-mda1-dmzbb-gw1-twe2-0-25.cisco.com (64.102.254.237)	1 ms
8	64.102.255.145 (64.102.255.145)	2 ms
9	128.107.6.22 (128.107.6.22)	1 ms
10	a104-106-160-119.deploy.static.akamaitechnologies.com (104.106.160.119)	8 ms

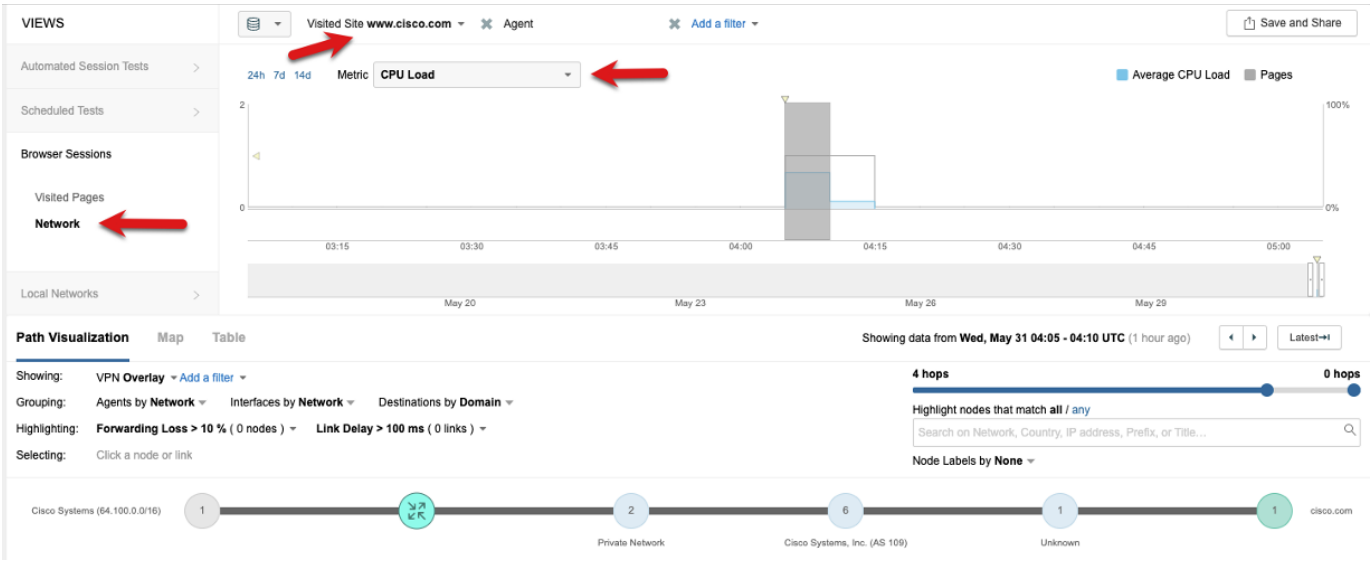
Computer Info | Path Trace | Waterfall

https://www.cisco.com/

https://www.cisco.com/

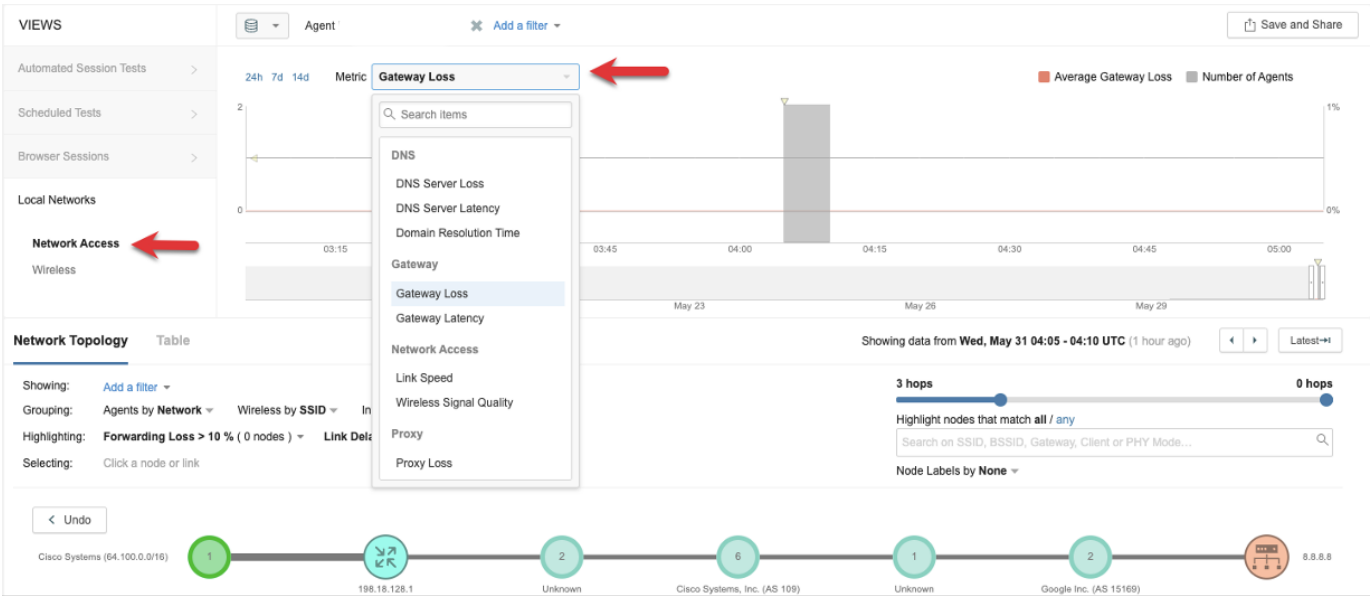
Object	Response Code	Domain	Size (kB)	Waterfall
/	200 [Headers]	www.cisco.com	15	120 ms
0	204 [Headers]	bat.bing.com		51 ms
recording	200 [Headers]	k-aus1.clickta…	0	48 ms
display	204 [Headers]	c.clicktale.net		62 ms
events	204 [Headers]	c.clicktale.net		61 ms
ctm-core.js	200 [Headers]	www.cisco.com	9.6	289 ms
personali…	200 [Headers]	www.cisco.com	4.9	290 ms
plain.css	200 [Headers]	www.cisco.com	0	390 ms
clientlib-d…	200 [Headers]	www.cisco.com	4.9 (cached)	< 1 ms
clientlib-b…	200 [Headers]	www.cisco.com	9.9 (cached)	< 1 ms
clientlib-h…	200 [Headers]	www.cisco.com	78.6 (cached)	< 1 ms
ctm.js	200 [Headers]	www.cisco.com	30.9	210 ms
otSDKStu…	200 [Headers]	cdn.cookielaw…	6.8 (cached)	< 1 ms
segments…	200 [Headers]	www.cisco.com	1.2 (cached)	< 1 ms
UserProfile	200 [Headers]	www.cisco.com	0.5	209 ms
token.json	403 [Headers]	www.cisco.com	0.3	205 ms
VisitorAPI.js	200 [Headers]	www.cisco.com	19	146 ms
targeter-b…	200 [Headers]	www.cisco.com	14.6	147 ms
01303338…	200 [Headers]	cdn.cookielaw…	1.8 (cached)	< 1 ms
otBanner…	200 [Headers]	cdn.cookielaw…	99 (cached)	< 1 ms
root.html	200 [Headers]	www.cisco.com	6.2	271 ms
root.html	200 [Headers]	www.cisco.com	5	272 ms
root.html	200 [Headers]	www.cisco.com	5.1	270 ms

ThousandEyes takes a layered approach with visualizing the data to help you isolate and troubleshoot issues. The Network Layer will show the network path filter on the browser session. Click on the Network Layer that is associated with the Browser Session. Explore the different metrics that are captured in context in time like CPU Load.



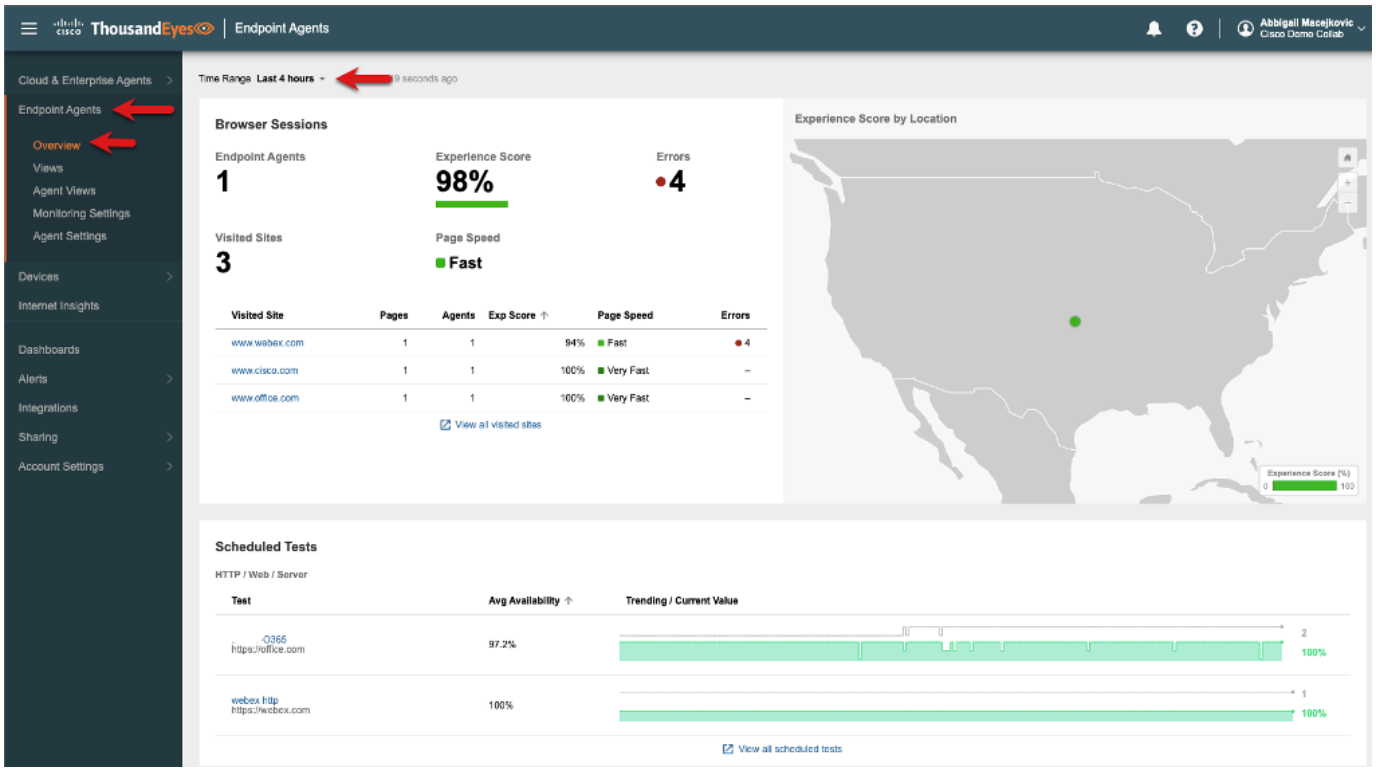
1.7.4 Local Network View

The Local Networks view will provide the local network and DNS information. This can be very helpful for finding bad DNS settings or Wi-Fi related issues. Click into the **Local Networks > Network Access** layer and make sure your agent is still in the agent filter or clear it out with the **X** to see all agents. Explore the different metrics as well using the pull down. If this was a production environment the filters could be used for isolation of issues.



1.7.5 Endpoint Agent Overview

This page provides a quick overall health view of your Endpoint Agents. Navigate to the **Endpoint Agents > Overview** to see all the stats from all the agents. Try adjusting the time range as well.

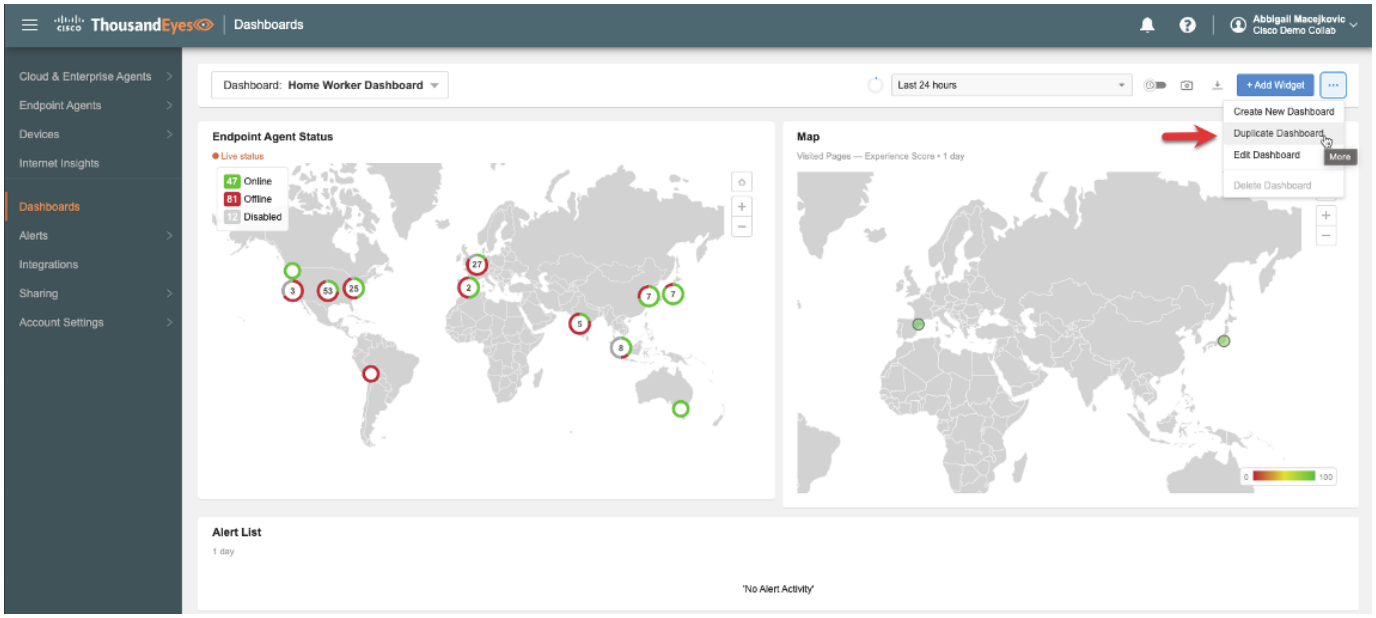


Now that you've learned about the metrics, tests and various way that ThousandEyes can help you troubleshoot, isolate and resolve end users issues you're one short step from the final stage of this learning jounery. The last step will be learning about some of the ways a dashboard can be used to visualize the endpoint agent data and shared with other stakeholders. Check out Task 7 to learn about Endpoint Agent data in Dashboards.

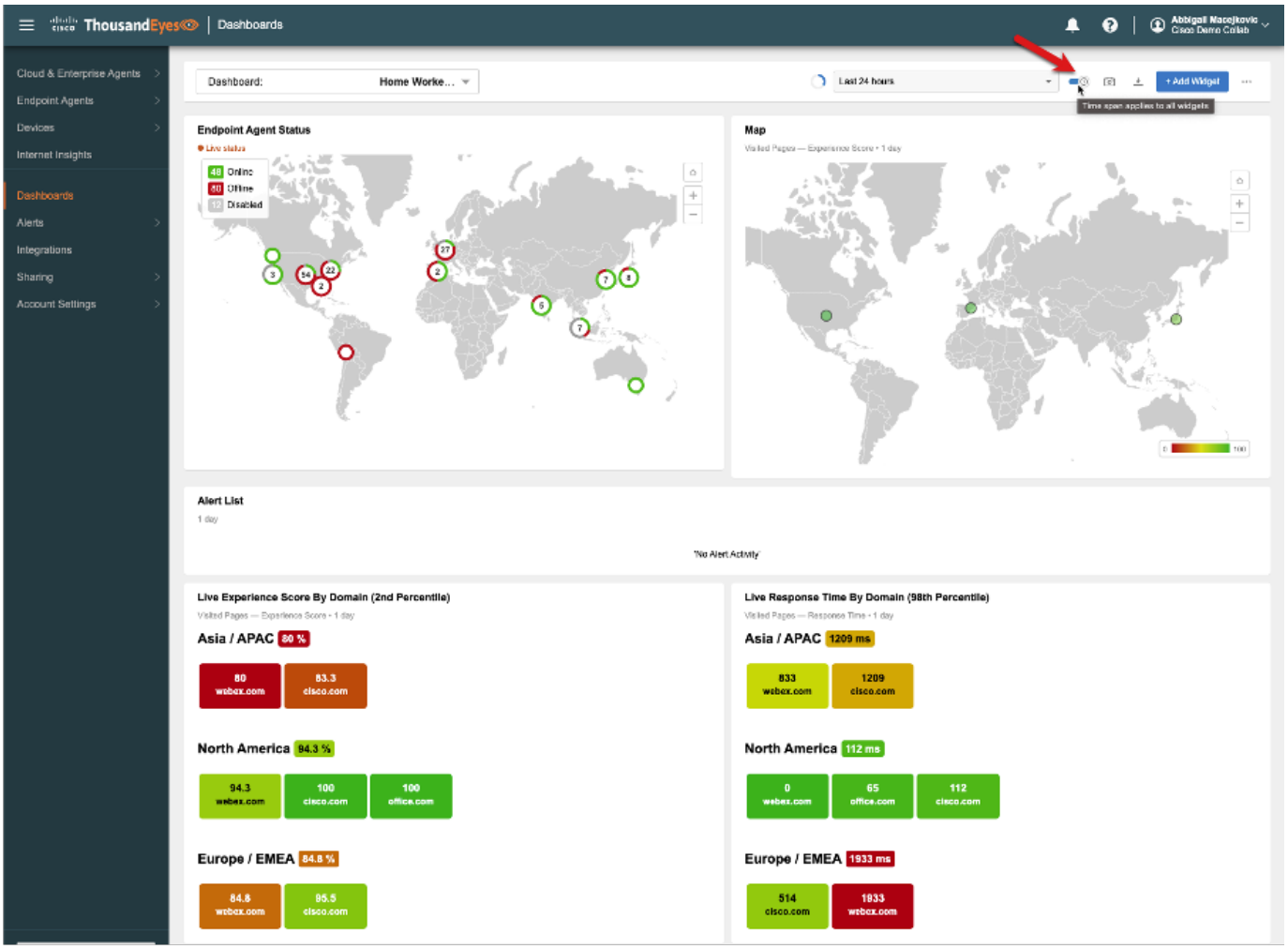
1.8 ThousandEyes Home Worker Dashboard (optional)

Dashboards provie a rich powerful way to visualize your ThousandEyes tests, quickly isolate issues, and see the health of your infrastructure and applications. Since we are focused on the Endpoint Agent we will use a dashboard that is based off this blog: Best Practcies to Create a "Remote Workforce" Dashboard.

Navigate to **Dashboards**. Use the pull down to select the **Home Worker Dashboard** then select the **"…"** pull down to duplicate the dashboard. Name it your name-Roadshow Home Worker Dashboard as this will allow you to try out some of the widgets without effecting the original.

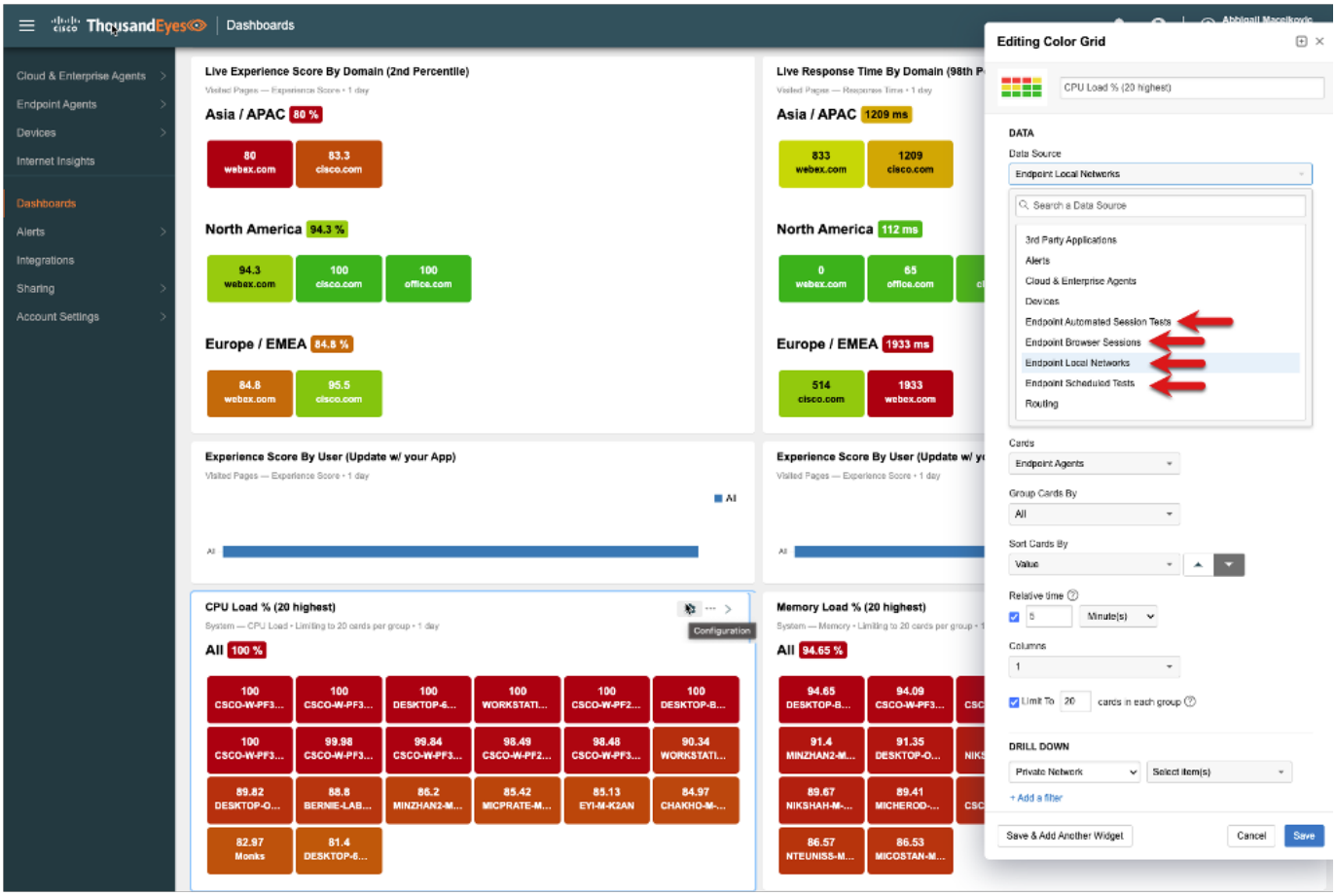


Test out the pull down for time and use the toggle to update all widgets. The snapshot feature will create a link for the dashboard. Additonally it can be scheduled to be emailed to team members or executives who may use for reports or meetings. Lastly the download options can create a pdf or csv file.

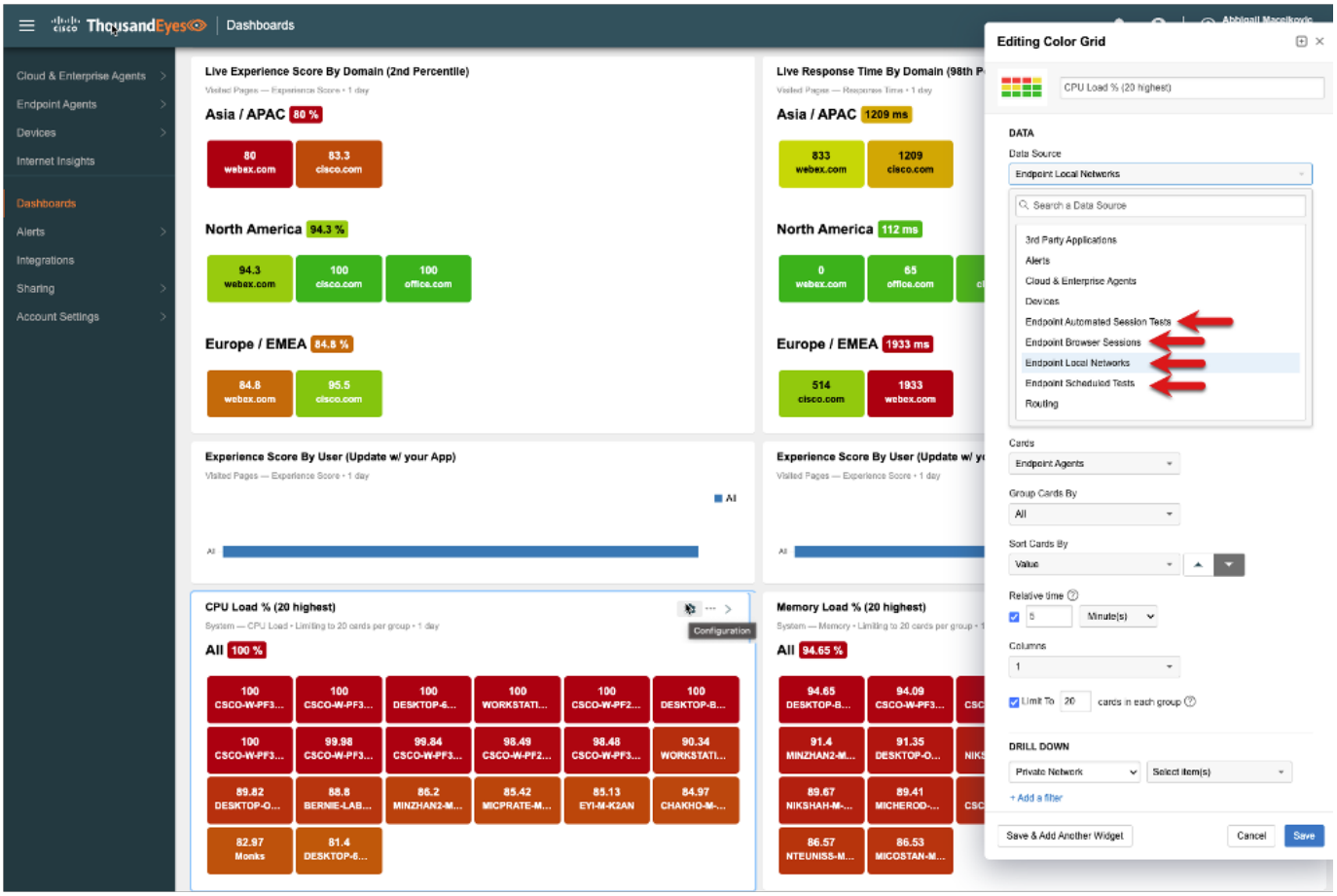


Each widget can be customized, or new widgets can be added based on your reporting requirements. Dashboards can be created to show Wi-Fi health of home vs. office, floor or building using the SSID or BSSID and labels. This makes it so your dashboard will be dynamic based on the time and how users are accessing the network and applications.

We'll use CPU color grid widget for this example. Click on the **settings** icon in the top right and click **Configuration** to see the Editing Color Grid pop out.



Changing the **Data Source** allows for different categories and Endpoint Agent metrics to be displayed in the widget. You can use the **"..."** to duplicate or delete the widget. Adjusting the **DESIGN** section will change the way the cards show up. The **Drill Down** is a great way to provide a filter for the metrics. For example if you were looking at **Visited Pages** for a category you could use it to filter down to the critical domain(s) you want the widget to display.



Feel free to modify, add widgets and make changes to your dashbord. Have fun with it and if you want to learn more about ThousandEyes dashboards check out our Getting Stared with Dashboards documenation.

Outside of the scope of this but a best practice recommendation is to set up alert rules with suitable conditions and assign those to your tests associated with your Endpoint Agents. This ensures you are notified of potential issues as soon as they occur, allowing for a swift resolution before user impact. For instance, if an Endpoint Agent detects a network connection issue, it can send an alert to your IT team. They can then investigate and resolve the issue before it starts affecting users. Alert rules can be configured to monitor performance metrics such as latency, packet loss, and jitter, or to flag when an application becomes unavailable or experiences degraded performance.

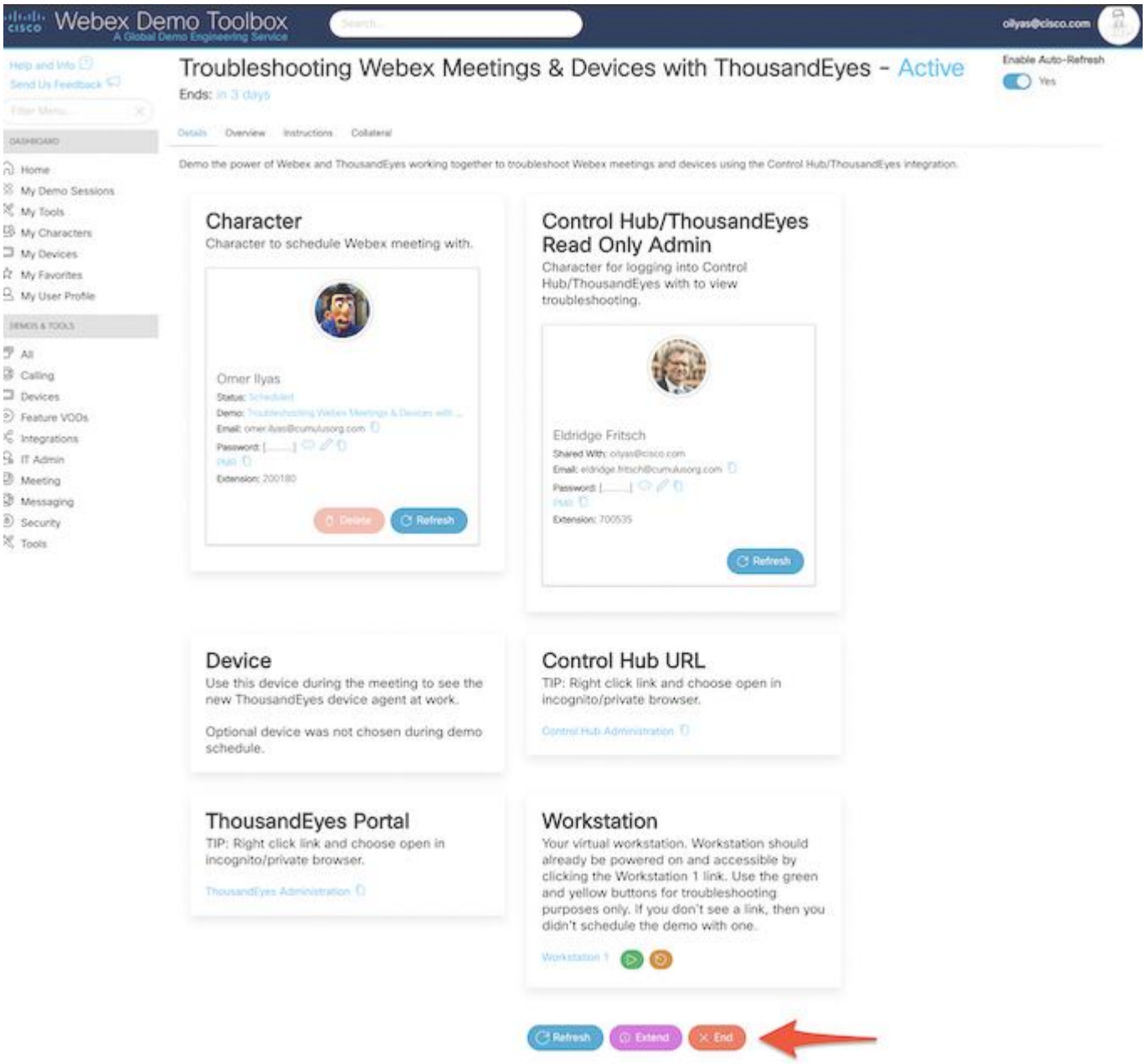
You can choose to receive these alerts when certain thresholds are exceeded and have them directed to a tool of your preference. ThousandEyes supports numerous integration options, including native integrations with Webex and ITSM tools such as ServiceNow and PagerDuty. Alternatively, you can choose from various custom webhook templates such as Webex, Slack, Microsoft Teams, or any third-party tool of your choice using the generic template. ThousandEyes integrations are powerful, delivering alerts directly into your existing workflow, thereby centralizing data and notifications from multiple sources into a single platform. For more information check out Getting Started with Alerts.

You've done an amazing job learning about how to deploy, configure and use the ThousandEyes Enpoint Agent to help you solve and isolate your end users issues providing you with actionable data and reducing your mean time to resolution (MTTR). Continue on to Logging Out and Ending the Lab Session

1.9 Logging Out and Ending the Lab Session

Close out of the Chrome Browser Close out Webex Close the Windows VM browser tab Log out of the ThousandEyes and close the incognito browser

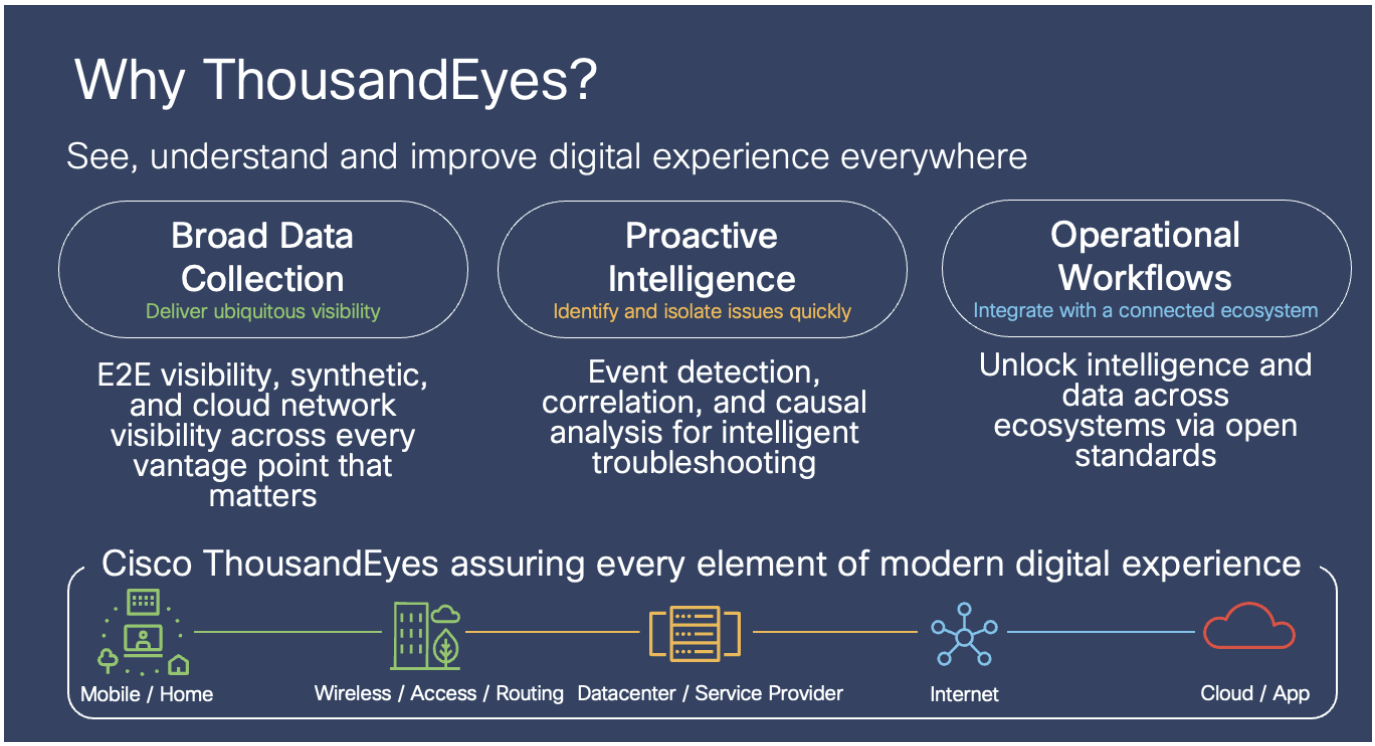
In the Webex Demo Toolbox browser tab scroll to the bottom and click **End**



Click **End Session** in the pop up to shutdown the lab and close the tab

Time to wrap things and with the Lab Conclusion.

1.10 Conclusion



Thank you for taking the time to learn about the ThousandEyes Endpoint Agent. Please **provide feedback** as I'm always looking at ways I can improve this content. If you have ideas where you think the ThosuandEyes Endpoint Agent could be improved please submit them as well so we can better help you solve your end users issues and provide you more time to do the things you enjoy.