

Policy Enforcement using Baselines

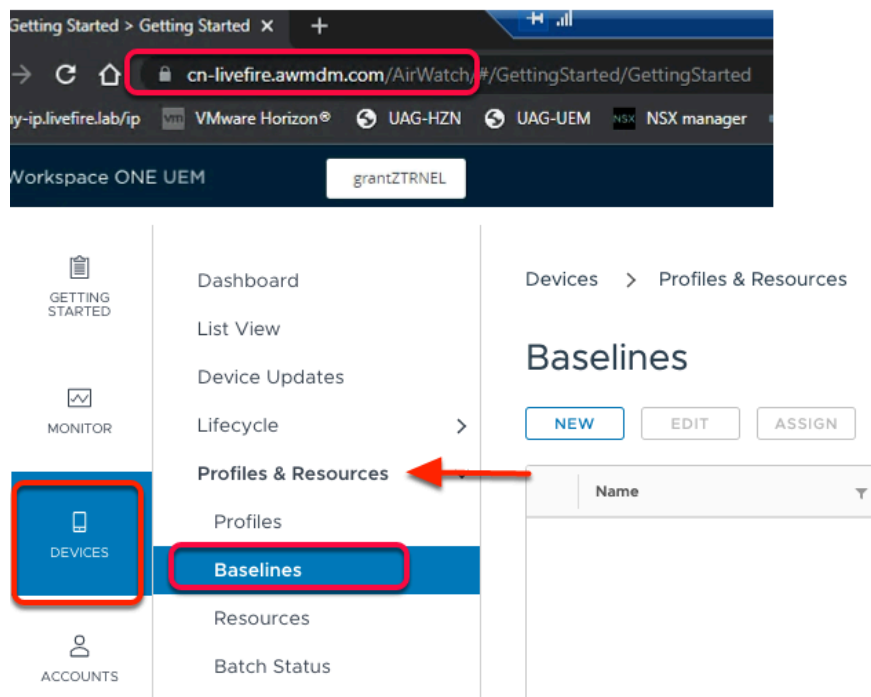
Baselines are industry-recommended settings to simplify security on your devices using Workspace ONE UEM. These one stop configurations significantly reduce the time it takes to set up and secure Windows devices.

In this section you will:

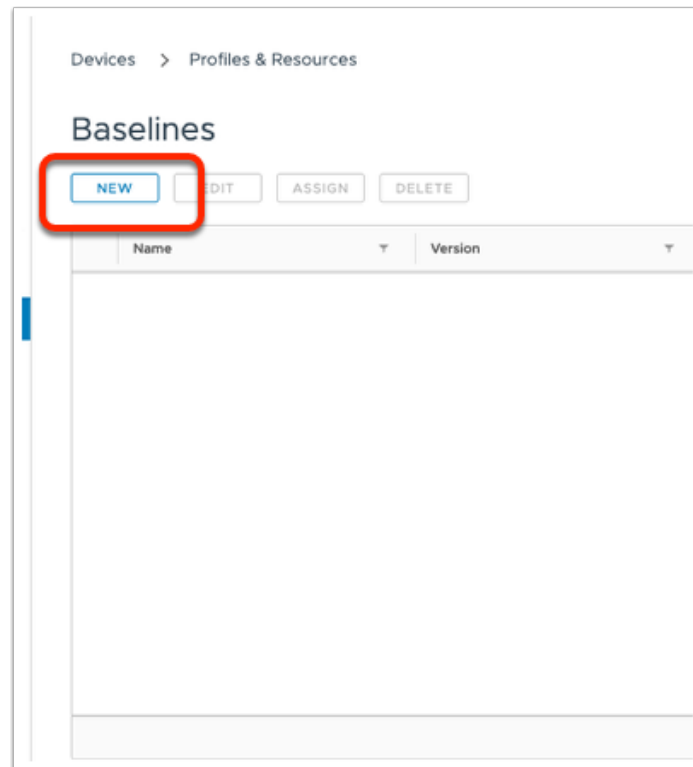
1. Create a Windows 10 Security baseline and add additional policies.
2. Test on your Windows VM machine.
3. Clean up

Lets get started!

Part 1: Create a Baseline



1. On the **MainConsole Machine**,
 1. Open **Google Chrome** browser
 2. Navigate to your Workspace ONE UEM console i.e. **cn-livewire.awmdm.com**
 3. Navigate to **Devices > Profiles & Resources > Baselines**.



2. Under **Baselines**, click on **NEW**.

A screenshot of a 'New Baseline' dialog box. On the left, there is a sidebar with five tabs: '1 General', '2 Choose Baseline', '3 Customize', '4 Add Policy', and '5 Summary'. The '1 General' tab is selected and highlighted with a red arrow. The main area of the dialog is titled 'General' and contains the following fields: 'Baseline Name' with the value 'Livefire Test', 'Description' with the value 'Livefire test baseline', and 'Managed By' with the value 'RohitM'. At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'.

3. Under **General** tab,
- Enter a **Baseline Name** as **LivefireTest**
 - Enter a **Description** as **Livefire Test Baseline**.
 - In the bottom right corner, select **NEXT**

Edit Baseline

- 1 General
- 2 Choose Baseline**
- 3 Customize
- 4 Add Policy
- 5 Summary

Choose Baseline

Select a preconfigured baseline and version

☒ **Windows 10 Security Baseline** ⓘ

Windows

Version 2004 ▾

☐ **Custom Baseline** ⓘ

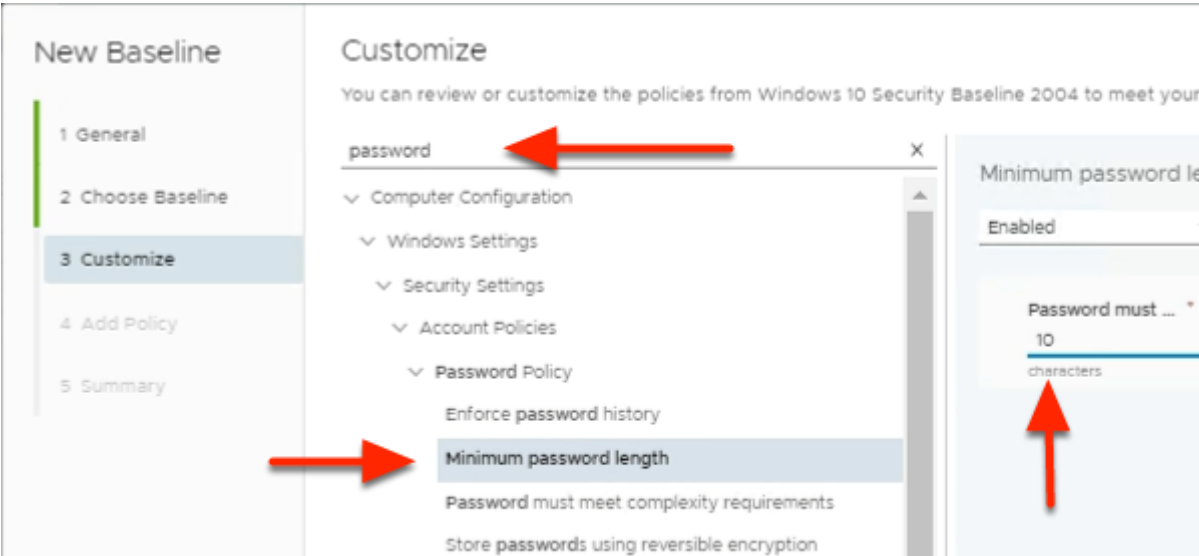
CANCEL **PREVIOUS** **NEXT**

4. Under **Choose Baseline**,
- Select **Windows 10 Security Baseline**
 - From the **Version** Drop down, select the latest version **2004**.
 - Select **NEXT**.

NOTE: you have 3 options to select from. We are selecting Windows 10 Security Baseline for this demo. Below is a description of the different options you can choose from,

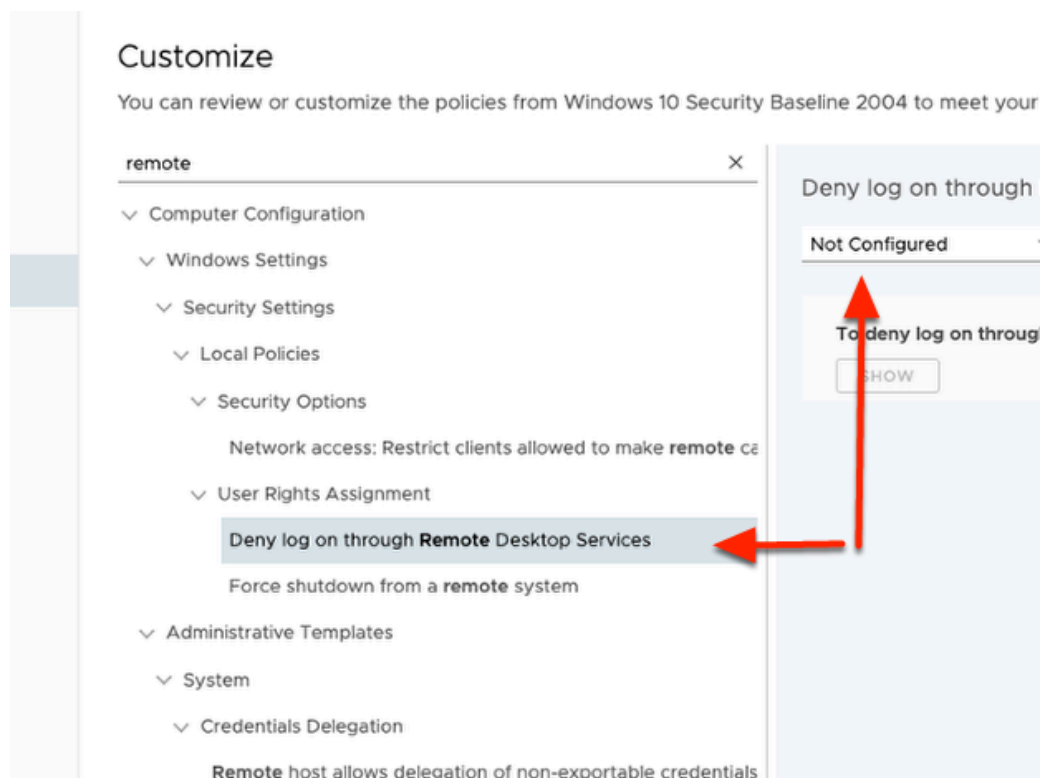
Setting	Description
CIS Windows 10 Benchmarks	This baseline applies the configuration settings recommended by CIS Benchmarks. L1 & L2 are two levels of CIS benchmarks. L2 being the most restrictive. Selecting L2 will block Workspace ONE Intelligence HUB from the device by default. Exclusion needs to be made to whitelist WS1 Intelligent HUB if L2 is selected.
Windows 10 Security Baseline	This baseline applies the configuration settings recommended by Microsoft. Select the OS version and benchmark level to apply.

Setting	Description
Custom Baseline	Allows you to upload your local policies which cannot be configured using microsoft CSPs.

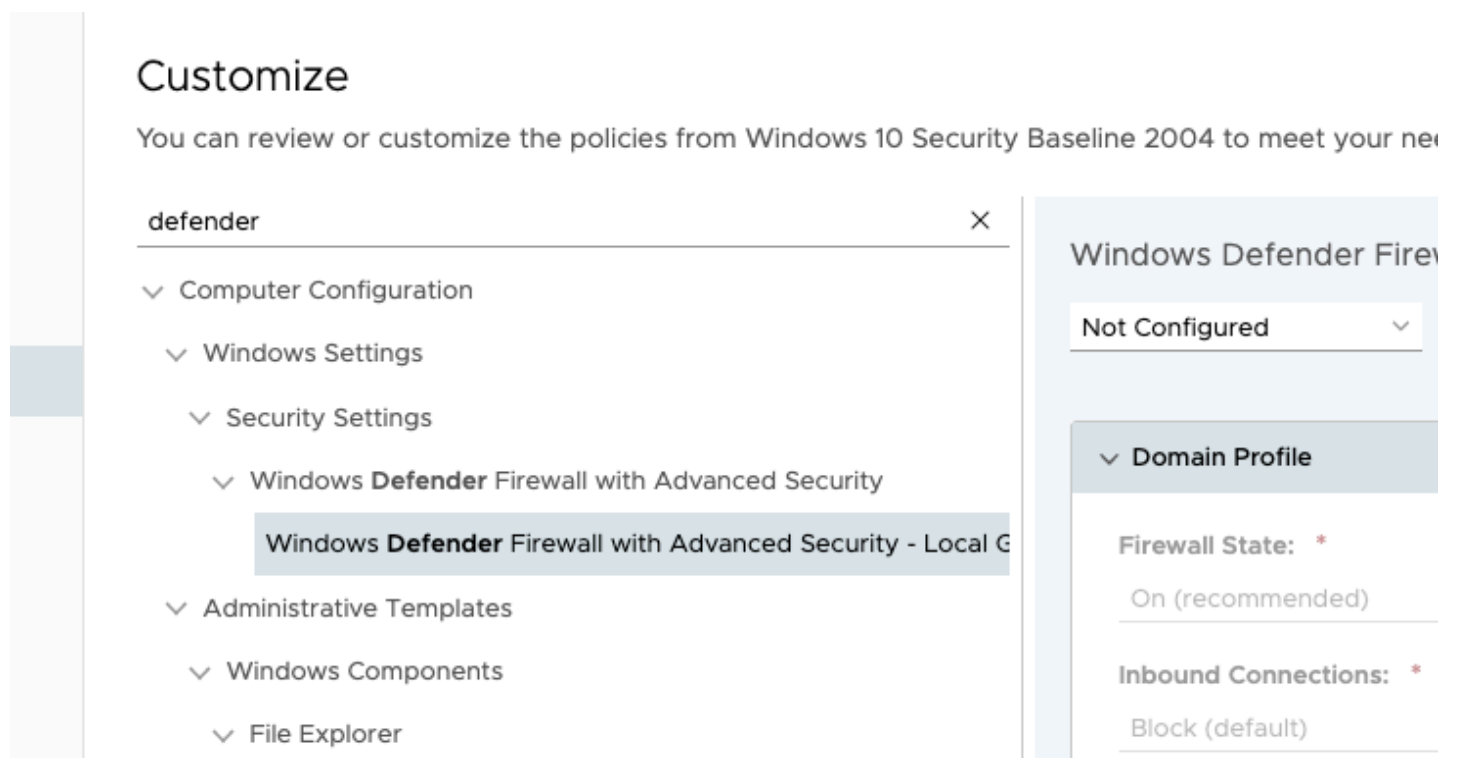


5. Under **Customize**,
1. In the **Filter**, search for **Password**.
 2. Click on **Minimum Password Length** in the results below.
 3. Change the Password must be at least to **10**

💡 **NOTE:** Password Complexity is enabled by default. You can customize the Baselines to further meet your organizations security policies.

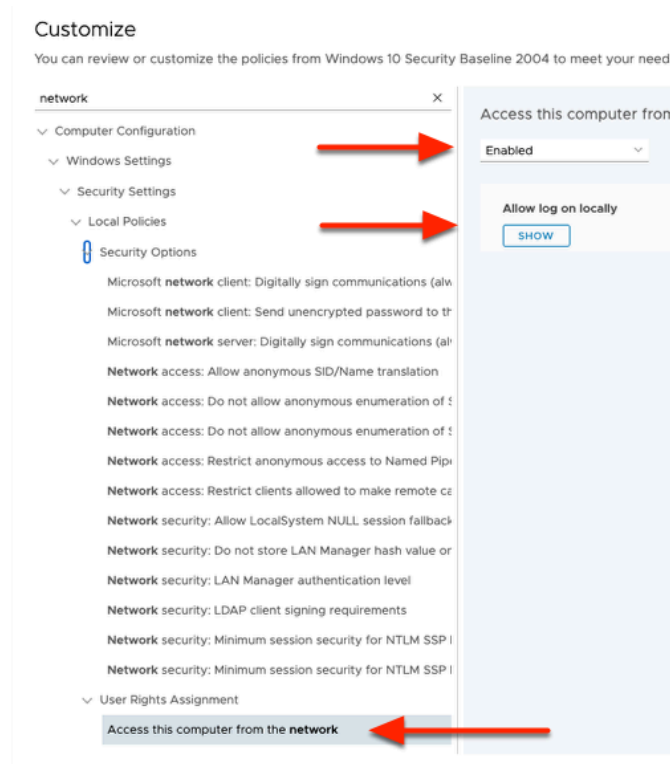


- Under **Customize**,
 - In the **Filter** type **REMOTE**
 - Select on '**Deny log on through remote desktop services**'
 - From the drop down on the right, Change from Enabled to **Not Configured**.



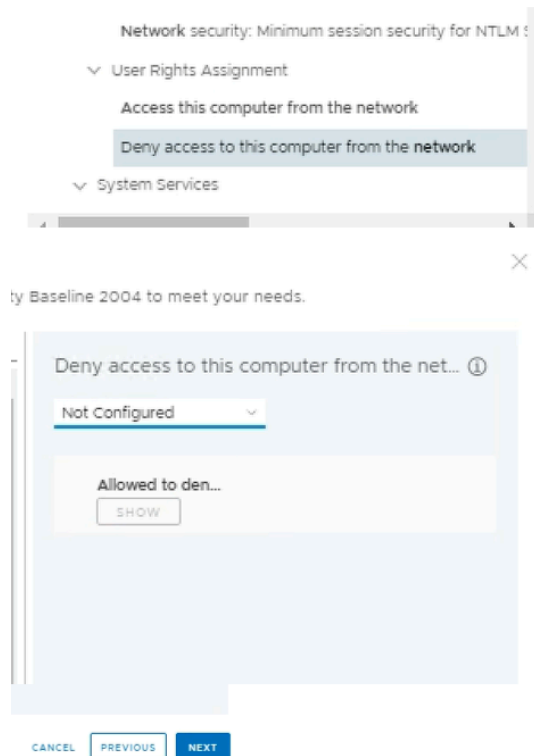
- Under **Customize**,

- In the **Filter** type **Defender**
- Select on '**Windows Defender Firewall with Advanced Security - Local Group Policy Object**'
- From the drop down on the right, Change from **Enabled** to **Not Configured**.



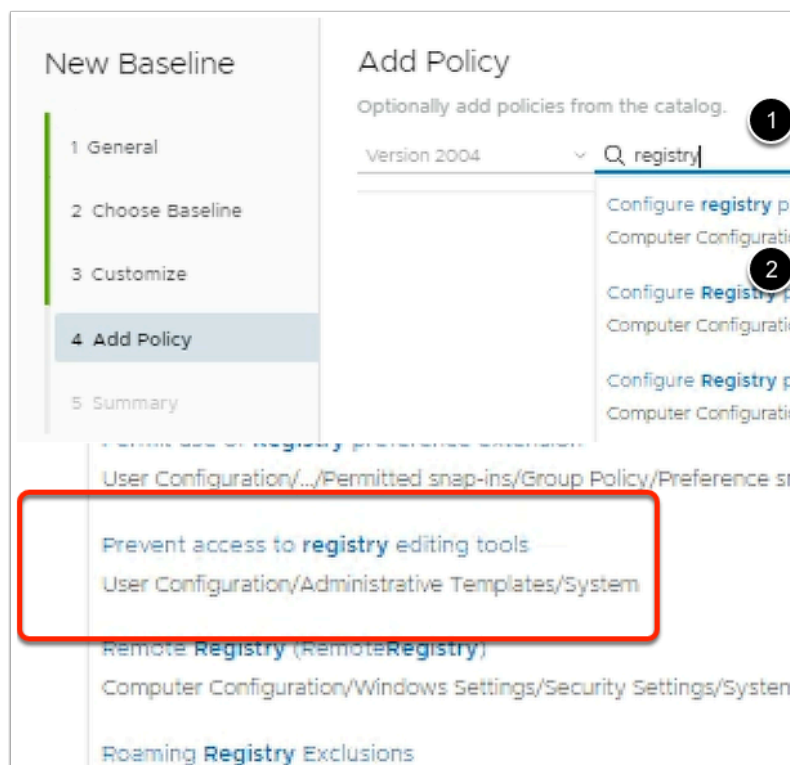
8. Under **Customize**,

- In the **Filter** type **Network**
- Click on **Access this computer from the network**
 - From the drop down on the right, ensure its **Enabled**



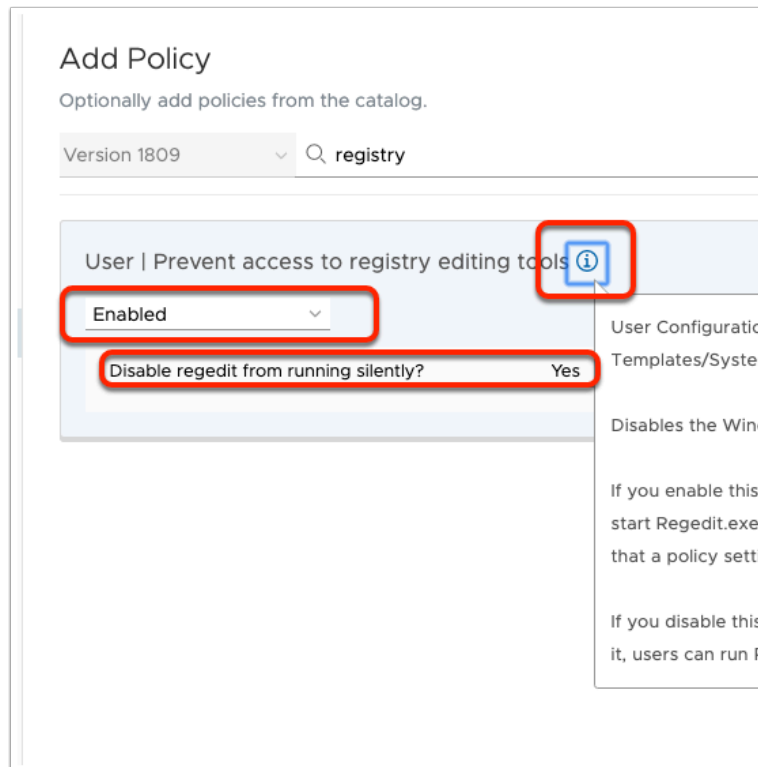
9. Under the same Network filter,

- Select **Deny access to this computer from the network**
 - To the right, from the drop down on the right, change from **Enabled** to **Not Configured**.
- In the bottom right corner, select **NEXT**.



10. In the **Add Policy** area ,

- (This section allows you to include any additional policies you need as part of the configuration)
 - To the right, In the **search** field, type **registry**
 - Select **ENTER**.
 - From the list of results,
 - Scroll down and select **Prevent access to registry editing tools**.

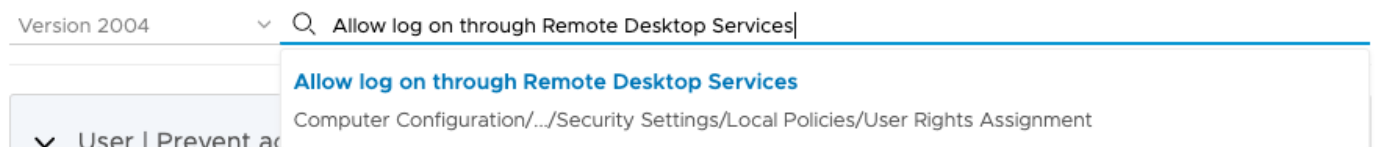


11. In the **Add Policy** area, und

- Change the **Policy** from **Not Configured** to **Enabled** using the drop down.
- Confirm the **Disable regedit from running silently** is set to **YES**.
 - Select the more information icon **i**.
 - **Confirm** the policy action for the additional policy created.

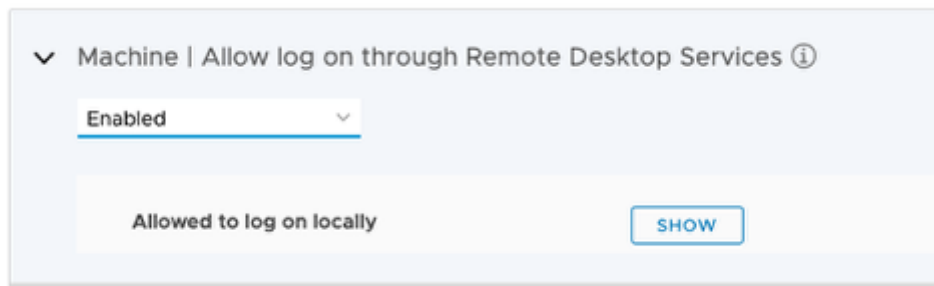
Add Policy

Optionally add policies from the catalog.



12. Under **ADD Policy** area,

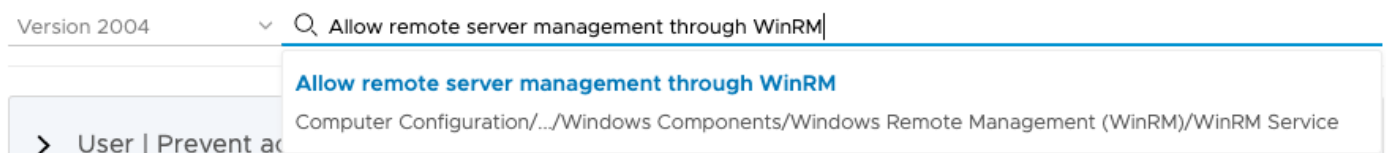
- In the **Search** area , type **Allow log on through Remote Desktop Services**
- Select **Allow log on through Remote Desktop Services**



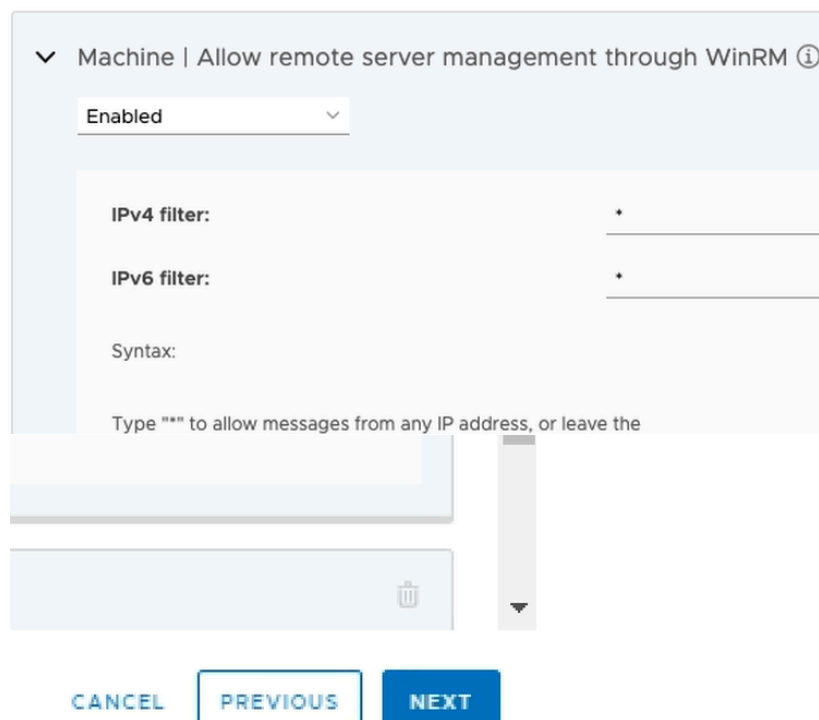
13. Under the **ADD Policy** area,
 - Change the field under **Allow log on through Remote Desktop Services** from **Not configured** to **Enabled**.

Add Policy

Optionally add policies from the catalog.



14. Next, under **ADD Policy area**
 - In the **Search**, type **Allow remote server management through WinRM**
 - Select **Allow remote server management through WinRM**



15. Under **Allow remote server management through WinRM**,

- From the drop down, change from **Not Configured** to **Enabled**.
- Under **IPv4 & IPv6 filter**, enter * (see the screenshot for reference)
- Select **NEXT**.

Edit Baseline

- 1 General
- 2 Choose Baseline
- 3 Customize
- 4 Add Policy
- 5 Summary

Summary

Baseline

Name: Windows 10 Security Baseline
Version: 2004

Customization

Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment/Deny log on through Remote Desktop Services	Not Configured
Computer Configuration/Windows Settings/Security Settings/Windows Defender Firewall with Advanced Security/Windows Defender Firewall with Advanced Security - Local Group Policy Object	Not Configured
Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options/Network access: Restrict clients allowed to make remote calls to SAM	Not Configured
Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment/Deny access to this computer from the network	Not Configured
> Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment/Access this computer from the network	Enabled

Added Policies

> User Configuration/Administrative Templates/System/Prevent access to registry editing tools	Enabled
> Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment/Allow log on through Remote Desktop Services	Enabled
> Computer Configuration/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service/Allow remote server management through WinRM	Enabled

CANCEL

PREVIOUS

SAVE AND PUBLISH

16. Under **Summary**,
- **Verify** the **customization & added** policies to your baseline.
 - Select **SAVE & ASSIGN**

Assign Baseline

Select the Smart Group(s) to assign the baseline. Select Exclusions to exclude a published baseline, the baseline will be removed from the excluded devices.

Assignments Exclusions

W

- All Employee Owned Devices(grantZTRNEL)
- W10Client01a(grantZTRNEL)
- W10Ext01a(grantZTRNEL)

No Smart Group(s) selected

CANCEL **PUBLISH**

17. In **Assign Baseline**,
- In the search area, type **W**
 - Select **W10Client01a**.
 - Select **PUBLISH**.

Part 2: Test on your Windows VM machine

grantZTRNEL

Add ▾ 🔍 🔔 ⭐ ? grantZTRNEL

Devices > Profiles & Resources

Baselines

NEW COPY EDIT ASSIGN DELETE

	Name	Version	Template	Managed By	Assignments	Install Status
<input type="radio"/>	Livetest	1	MSFT 2004	grantZTRNEL	1	View

1 Installed
0 Not Installed
1 Assigned

Install Status

View

1. In the Baselines area
 - Confirm the Baseline is created.
 - Under **Install Status** select **VIEW**
 - Select the **Count** (in this case **1**) for your baseline **Livefire Test**.


View Devices - Baselines

Last Update: 6/6/2020, 03:32 AM

Status	Friendly Name	User	Platform	OS	Updated
✓ Installed	livefireuser Desktop Windows Desktop 10.0.18363 b 9f	livefireuser	Windows Desktop	10.0.18363	6/6/2020, 03:03 AM

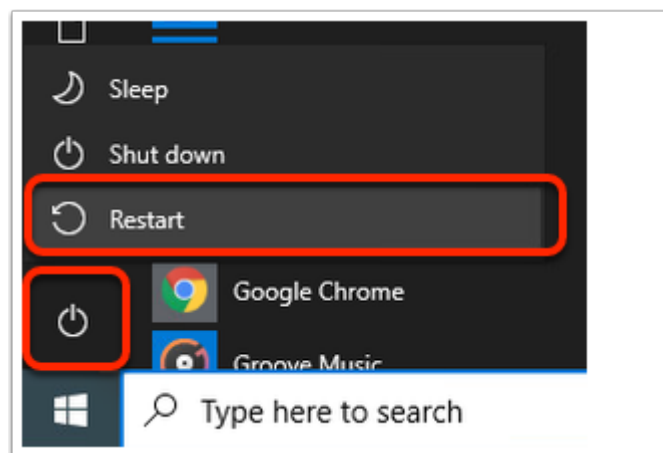
Items 1 - 1 of 1

2. In the **View Devices - Baselines** area
 - If the baseline is installed, you can verify this under status.

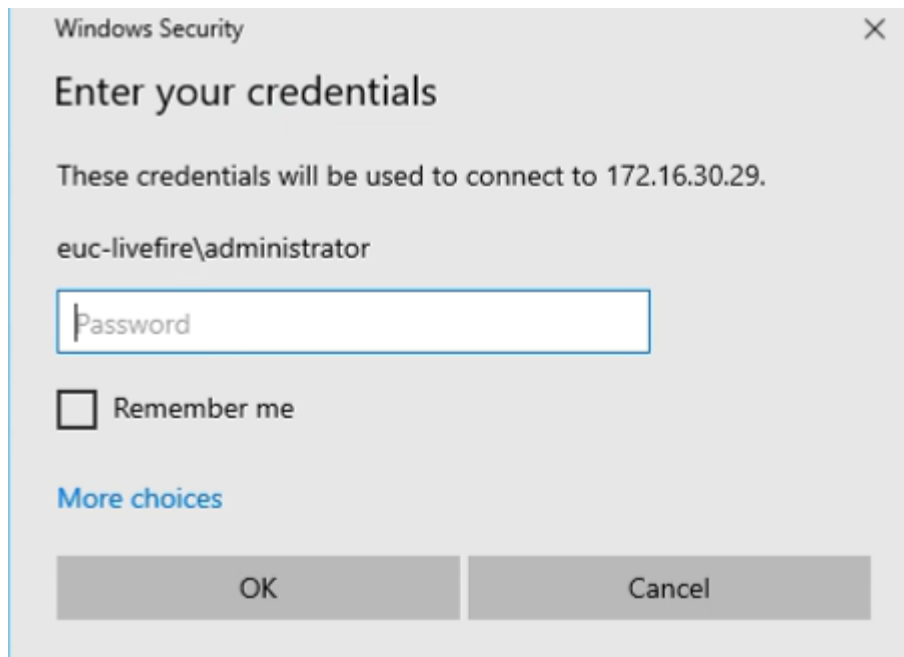
Status	Friendly Name	Compliance	User	Platform	Updated
<div>  Pending Reboot v1 </div>	User1 Desktop Window VMware Virtual Platform	Not Available	euc-livewire.com\...	Windows Des 10.0.18362	5/15/202...

Items 1 - 1 of 1

❗ NOTE: In either case, you must **restart** the device for the baseline to take effect.

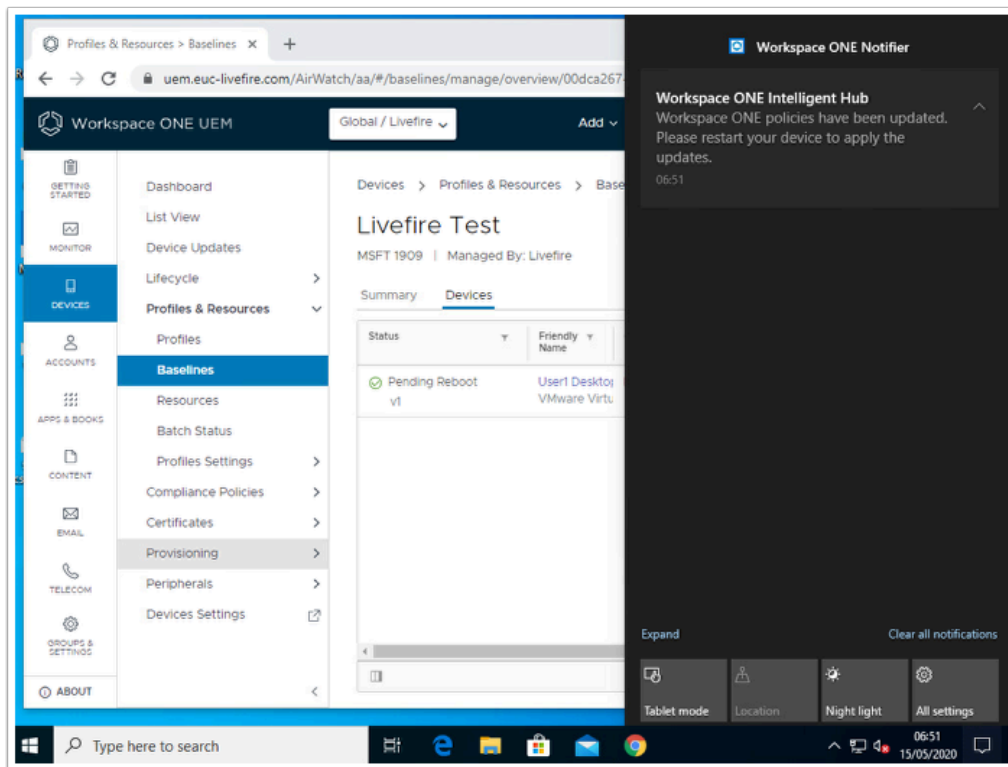


- On your W10Client01 Machine,
 - Select the **Start Menu > Power > Restart**. (NOTE: This will kill the RDP session)



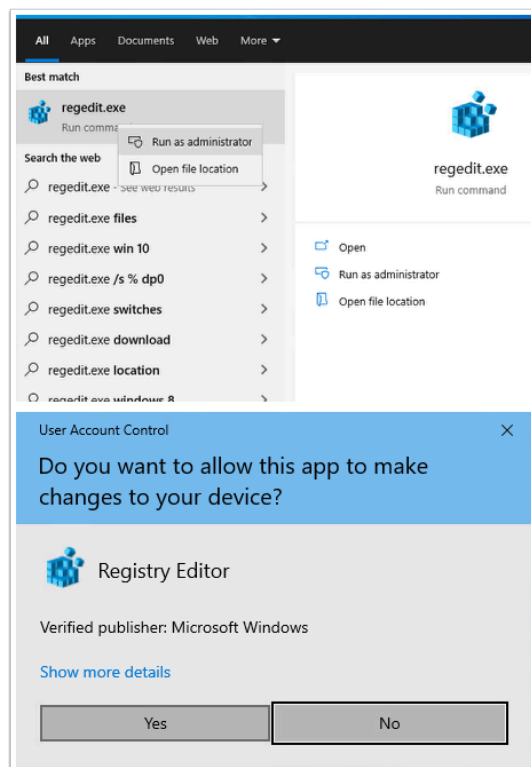
4. On your ControlCenter server
 - Open your **Remote Desktops** Folder
 - Select the **W10Client01.RDP** client.
 - In the Password area enter: **VMware1!**
 - Select **OK**

! NOTE: This is the same Virtual Machine you enrolled in to Workspace ONE UEM SaaS tenant.



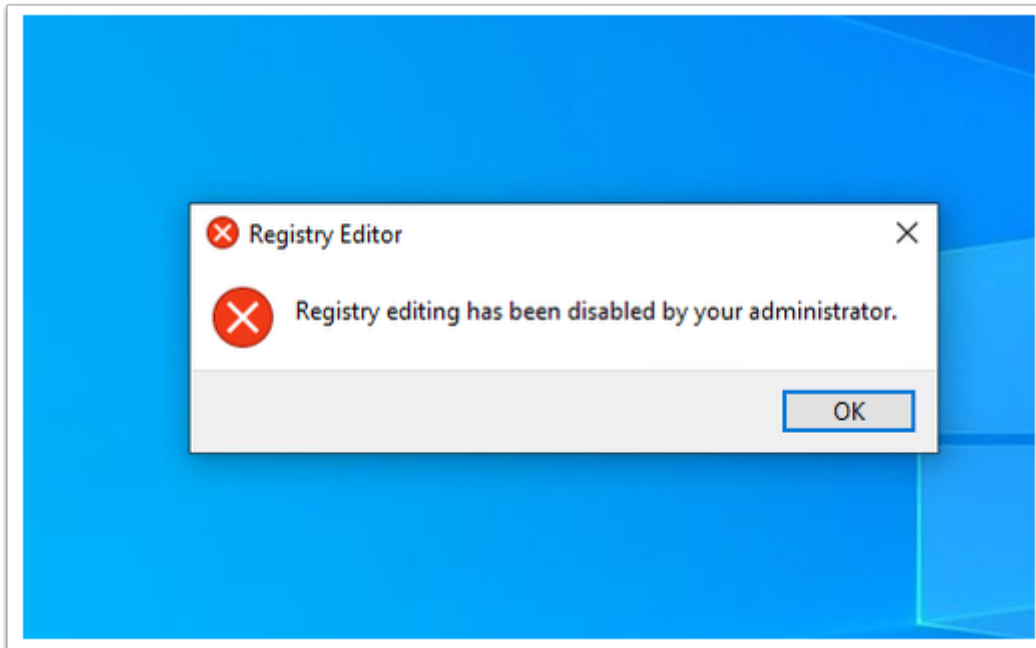
5. In the Workspace ONE UEM admin console

- NOTE: This might take a few minutes. You can refresh the baseline page on Workspace ONE UEM to confirm the status has changed to installed to see this notification.
- However, once your desktop has restarted and you have logged in, you should proceed with the test in step 5

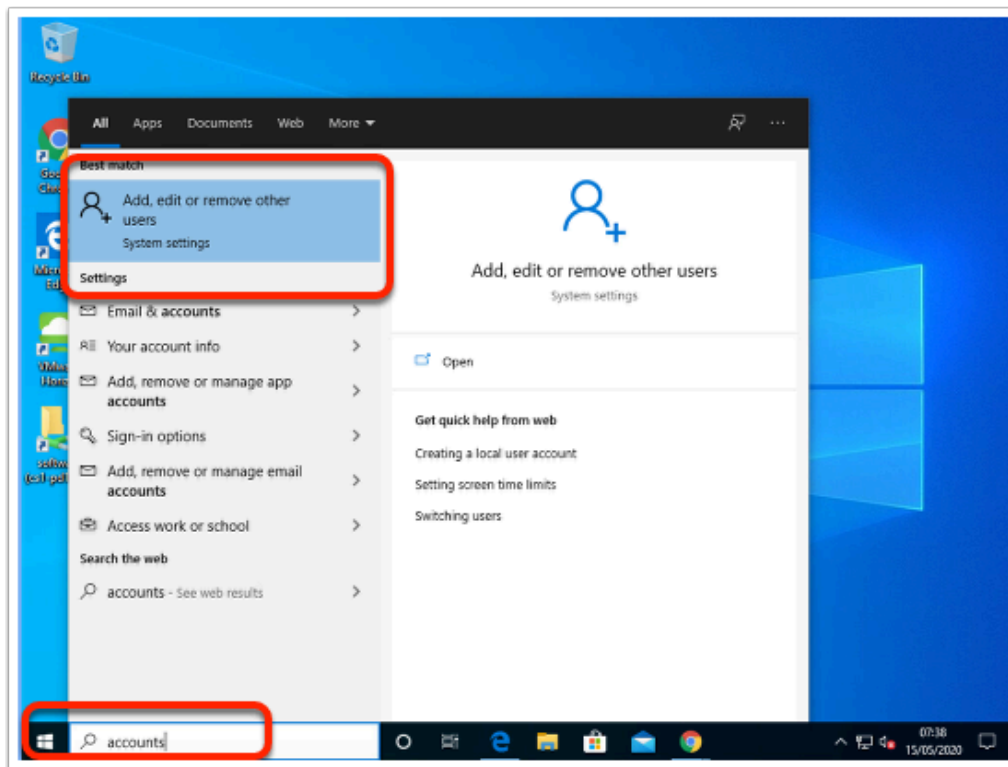


6. On your W10Client01 computer

- To **test** if the baseline policy is successfully applied,
 - Navigate to **Search bar**. Type **Regedit.exe**.
 - Right Click on the **Regedit.exe** result and Click **Run as administrator**.

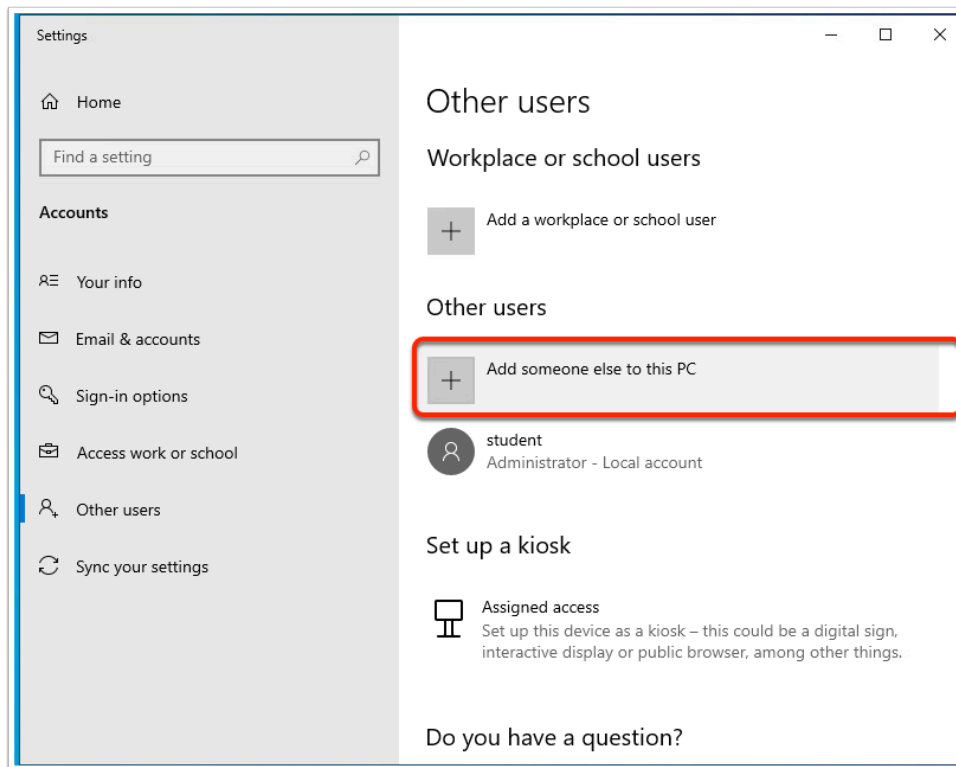


! Notice you will see this **error message: Registry editing has been disabled by your administrator.**

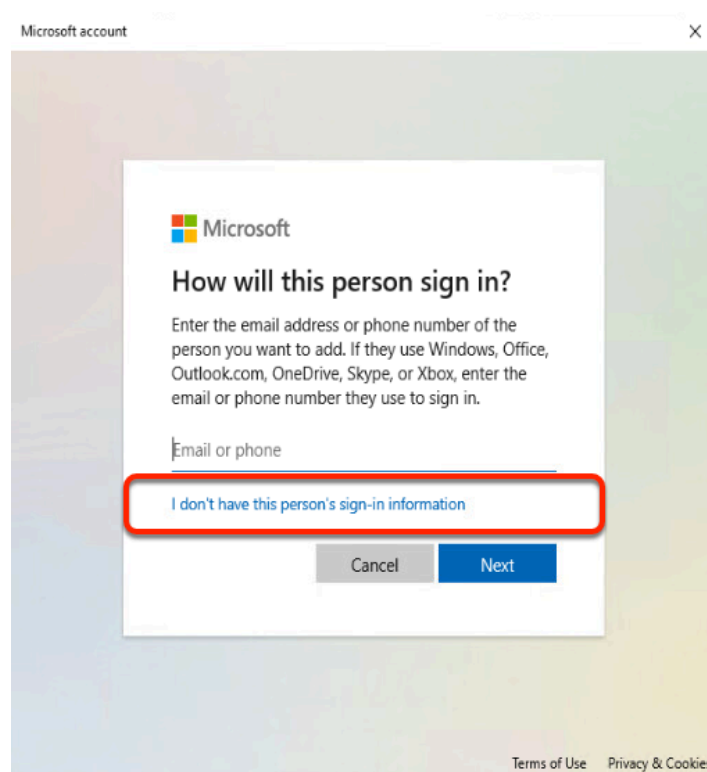


7. On your **W10Client01** computer

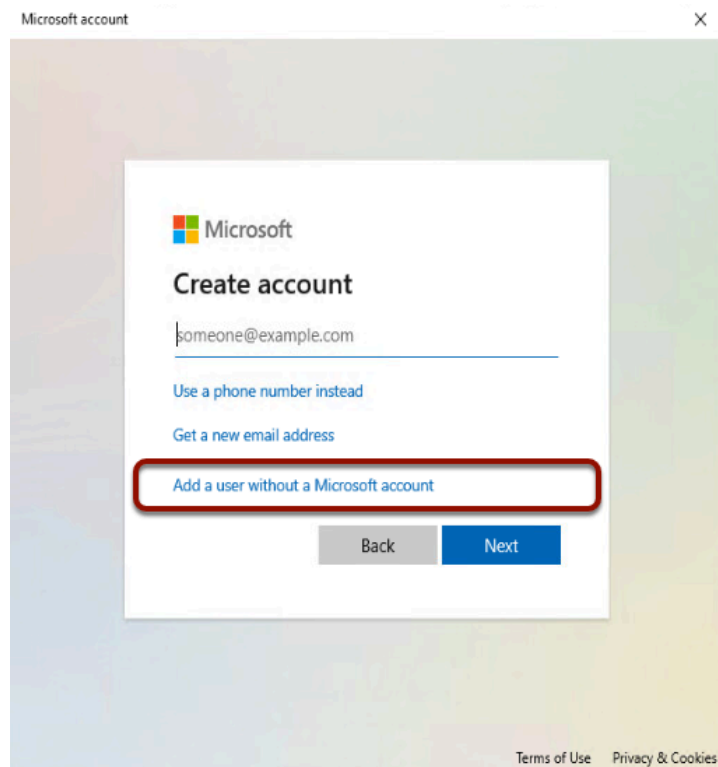
- In order to test the **Minimum Password Length policy** applied by your Baseline, we will add a user account on this machine with password less than 10 characters. To add a user account,
 - Search **Accounts** in search bar from your Windows **win10Client01** machine.
 - Select on **Add, edit or remove other users**.



8. Under **Other Users**,
- Select on **Add someone else to this PC**.



9. On the **How will this person sign in?** window
- Select **I don't have this person's sign in information**



10. On the Create account window

- Select **Add a user without a Microsoft account.**
- Select **Next**

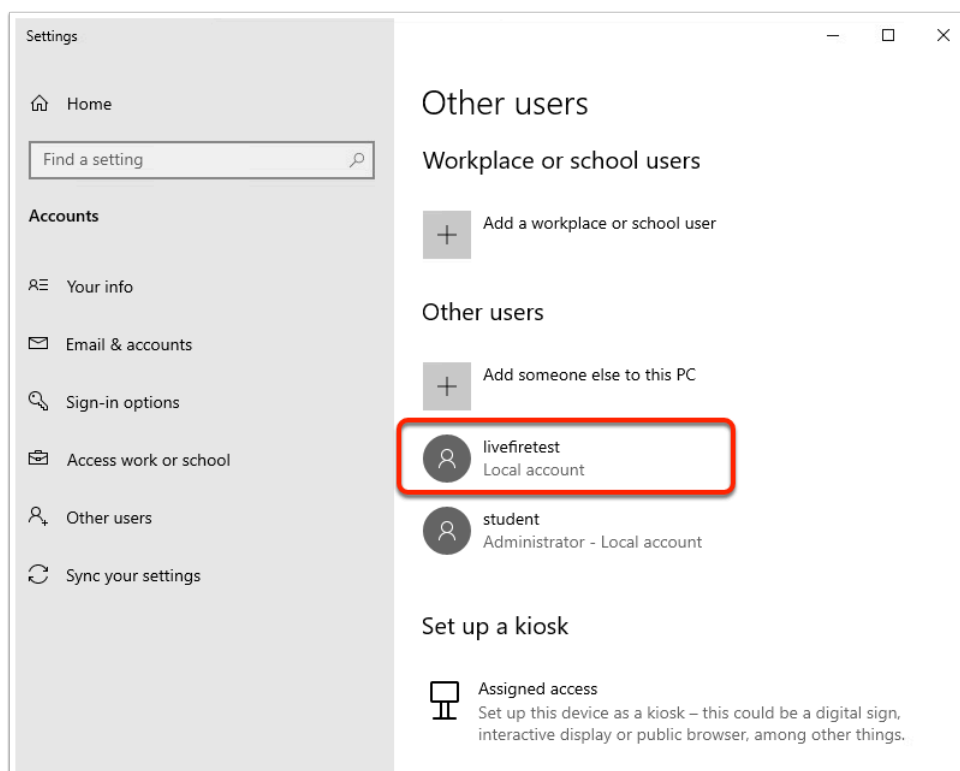
11. In the Microsoft account window

- Fill in the information with dummy values.

NOTE: For this test, use a password less than 10 characters in length.

Notice as per our Windows 10 security baseline, password should be greater than 10 characters and must meet the below complexity requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length Contain characters from three of the following four categories: English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, !, \$, #, %)



12. In the **Other users** window

- **Change** the password to meet your requirement of 10 characters and **save**.
- Notice the account is successfully created once you meet the password requirements.

You have completed this lab. This brings us to the end of labs for this week. Thank you again for the participation and hard work.