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-livefire.awmdm.com
- 3. Navigate to **Devices > Profiles & Resources > Baselines.**

	Devices > Profiles & Resources	i	
	Baselines		
C	NEW EDIT ASSIGN	DELETE	
	Name	T Version	Ψ
٩.			

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

New Baseline	General		×
1 General	Give the baseline a friendly name	and description.	
2 Choose Baseline	Baseline Name *	Livefire Test	
3 Customize	Description	Livefire test baseline	
4 Add Policy			
5 Summary			.6
	Managed By	RohitM	
		CANCEL	σ

3. Under General tab,

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

1 General		
2 Choose Baseline	Windows 10 Security Baseline (j)	
3 Customize	Windows	
4 Add Policy		
5 Summary		J
	0	
	Custom Baseline ①	

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.



- 6. 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.

Customize

You can review or customize the policies from Windows 10 Security Baseline 2004 to meet your net



7. 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**

Network security: Minimum session security for NTLN	И :
✓ User Rights Assignment	
Access this computer from the network	
Deny access to this computer from the network	
✓ System Services	
	×
ty Baseline 2004 to meet your needs.	
Deny access to this computer from the net () Not Configured	
Allowed to den	
CANCEL PREVIOUS NEXT	

- 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**.

Version 1809 Versi	
User Prevent access to registry editin	
Enabled ~	User Configura
Disable regedit from running silently?	Yes Templates/Sys
	Disables the W
	Disables the W
	Disables the W If you enable the start Regedit.e
	Disables the W If you enable th start Regedit.e that a policy se
	Disables the W If you enable th start Regedit.e that a policy se If you disable t

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		\times
Optionally add policies fro	m the catalog.	
Version 2004 V	Q Allow log on through Remote Desktop Services	
	Allow log on through Remote Desktop Services	
✓ User Prevent ac	Computer Configuration//Security Settings/Local Policies/User Rights Assignment	

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

✓ Machine Allow log on through	Remote Desktop Services 🛈
Enabled ~	
Allowed to log on locally	вном

13. Under the **ADD Policy** area,

• Change the field under Allow log on through Remote Desktop Services from Not configured to Enabled.

Add Policy

 \times

Optionally add policies fro	om the catalog.
Version 2004 V	O, Allow remote server management through WinRM
	Allow remote server management through WinRM
> User Prevent ad	Computer Configuration//Windows Components/Windows Remote Management (WinRM)/WinRM Service

14. Next, under ADD Policy area

- In the Search, type Allow remote server management through WinRM
- Select Allow remote server management through WinRM

➤ Machine Allow remote server management	nt through WinRM (i)
Enabled ~	
IPv4 filter:	*
IPv6 filter:	•
Syntax:	
Type "*" to allow messages from any IP address, or le	ave the
ŵ 🚽	
CANCEL PREVIOUS NEXT	

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	Summary	×
1 General		
2 Choose Baseline	Vame: Windows to security Baseline	
3 Customize	Customization 0	
4 Add Policy	Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment/Deny log on through Remote Desktop Services	Not Configured
5 Summary	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

Assignments Exclusions	eline will be removed from the excluded
Assignments	
w	
All Employee Owned Devic	es(grantZTRNEL)
W10Client01a(grantZTRNEL	.)
W10Ext01a(grantZTRNEL)	7
	No Smart Group(s) s

17. In Assign Baseline,

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

Part 2: Test on your Windows VM machine

grantZTRNEL					Add ~	α¢	i ☆	0	grantfle
Devices > Profiles & Resources									
Baselines									
NEW COPY EDIT	ASSIGN DELETE						_		
Name	T Version	Υ Template	Y Managed By	Υ ÅD	signments		v	inctail Stat	tus
 LivefretEST 	1	MSFT 2004	grantZTRNEL	. 1				View	
							_		_
	grantZTRNEL Devices > Profiles & Resources Baselines NEW COPY EDIT Name O LivefroTEST	grantZTRNEL Devices > Profiles & Resources Baselines NEW COPY EDIT ASSIGN DELETE Name Y Version UvefraTEST 1	grantZTRNEL Devices > Profiles & Resources Baselines NEW COPY EDIT ASSIGN DELETE Name Y Version Y Template UvefreTEST 1 MSFT 2004	grantZTRNEL Devices > Profiles & Resources Baselines NEW COPY EDIT ASSIGN DELETE Name Y Version Y Template Y Manged By LivefireTEST 1 MSFT 2004 grantZTRNEL	grantZTRNEL Devices > Profiles & Resources Baselines NEW COPY EDIT ASSIGN DELETE Name Y Version Y Template Y Managed By Y Assign LivefineTEST 1 MSFT 2004 grantZTRNEL 1	grantZTRNEL Add ~ Devices > Profiles & Resources Baselines NEW COPY EDIT ASSIGN DELETE Name Y Version Y Tempiate Y Assignments UnverseTEST 1 MSFT 2004 grantZTRNEL 1	grantZTRNEL Add v Q Q Devices > Profiles & Resources Baselines NEW COPY EDIT ASSIGN DELETE Name Y Version Y Template Y LivefireTEST 1 MSFT 2004 grantZTRNEL 1	grantZTRNEL Add v Q <th>grantZTRNEL Add ∨ Q</th>	grantZTRNEL Add ∨ Q

1 Installed O Not Installed	Install Status
	View
1 Assigned	

- 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**.

	۲	Friendly Name	т	User	т	Platform	OS	Τ	Updated	Τ
Installed		livefireuser Desktop Windows Desktop 10.0.18	1363 b 9f	livefireuser		Windows Desktop	10.0.18363		6/6/2020, 03:0	D3 AM
									ite	1151-10

2. In the View Devices - Baselines area

• If the baseline is installed, you can verify this under status.

	Friendly Name y	Compliance	Y User	Ψ	Platform	Updated T
 Pending Reboot v1 	Userl Desktop Window VMware Virtual Platfori	Not Available	euc-liv	efire.com\	Windows Des 10.0.18362	5/15/202

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



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

Windows Security	×
Enter your credentials	
These credentials will be used to	connect to 172.16.30.29.
euc-livefire\administrator	
Password	
Remember me	
More choices	
ОК	Cancel

- 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.

Settings	– 🗆 X
ப் Home	Other users
Find a setting ρ	Workplace or school users
Accounts	+ Add a workplace or school user
RE Your info	Other users
🖾 Email & accounts	
🔍 Sign-in options	+ Add someone else to this PC
Access work or school	8 student Administrator - Local account
R_{\star} Other users	
⊖ Sync your settings	Set up a kiosk
	Assigned access Set up this device as a kiosk – this could be a digital sign, interactive display or public browser, among other things.
	Do you have a question?

8. Under Other Users,

• Select on Add someone else to this PC.

Microsoft account		×
	Microsoft	
	How will this person sign in?	
	Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.	
Series 1	Email or phone	
ſ	I don't have this person's sign-in information	
	Cancel Next	
	Terms of Use	Privacy & Cookies

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

Microsoft account		×
	Microsoft Create account someone@example.com Use a phone number instead Get a new email address	
(Add a user without a Microsoft account	
	Back Next	
	Terms of Use	Privacy & Cookies

- 10. On the Create account window
 - Select Add a user without a Microsoft account.
 - Select Next

Make it secure.		
••••		
••••		
The password you typed doesn't me complexity requirements set by the network or group. Get the requirem administrator, then type a new pass	eet the password administrator for your ents from your word.	
In case you forget your password		
What was your first pet's name?	<u> </u>	
test		
test What is the name of the city where	e you were born?	

- 11. In the Microsoft account window
 - Fill in the information with dummy values.

I 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, !, \$, #, %)

Settings	– 🗆 X
û Home	Other users
Find a setting ρ	Workplace or school users
Accounts	+ Add a workplace or school user
R⊟ Your info	Other users
🖾 Email & accounts	Add someone else to this PC
🔍 Sign-in options	+ Add someone else to this i c
료 Access work or school	livefiretest Local account
A_{\star} Other users	8 student Administrator - Local account
${\mathcal C}$ Sync your settings	-
	Set up a kiosk
	Assigned access Set up this device as a kiosk – this could be a digital sign, interactive display or public browser, among other things.

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.