# Lab: Configuring security in Windows Server

## Scenario

Contoso Pharmaceuticals is a medical research company with about 5,000 employees worldwide. They have specific needs for ensuring that medical records and data remain private. The company has a headquarters location and multiple worldwide sites. Contoso has recently deployed a Windows Server and Windows client infrastructure. You have been asked to implement improvements in the server security configuration.

## Objectives

After completing this lab, you will be able to:

* Configure Windows Defender Credential Guard.
* Locate problematic user accounts.
* Implement and verify LAPS (Local Administrator Password Solution)

## Estimate time: 40 minutes

## Lab setup

Virtual machines: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-SVR1**, and **WS-011T00A-SEA-ADM1** User name: Contoso\Administrator Password: Pa55w.rd

## Exercise 1: Configuring Windows Defender Credential Guard

### Scenario

You decide to implement Windows Defender Credential Guard on the servers and administrative workstations to protect against Pass-the-Hash and Pass-the-Ticket credential thefts. You will use Group Policy to enable Credential Guard on your existing servers. For all new servers, you will use the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool to enable Credential Guard before the new servers are domain joined.

In this lab, you will set up the Group Policy and run the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool on an existing server.

**Note**: In the lab environment, Credential Guard will not run VMs because they don't meet the requirements. You can still create the GPO (Group Policy Objects) and run the tool.

The main tasks for this exercise are to:

1. Enable Windows Defender Credential Guard using Group Policy.
2. Enable Windows Defender Credential Guard using the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool.

### Task 1: Enable Windows Defender Credential Guard using Group Policy

1. Sign-in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start**, and then enter **Group Policy Management**.
3. Select **Group Policy Management**.
4. In the Group Policy Management Console, expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**, right-click or access the context menu for the **IT** OU (Organizational Unit), and then select **Create a GPO in this domain, and Link it here**.
5. In the **New GPO** dialog box, in the **Name** text box, enter **CredentialGuard\_GPO**, and then select **OK**.
6. In the **Group Policy Management** window, under **IT**, right-click or access the context menu for **CredentialGuard\_GPO**, and then select **Edit**.
7. In the Group Policy Management Editor, navigate to **Computer Configuration\Policies\Administrative Templates\System\Device Guard**.
8. Select **Turn On Virtualization Based Security**, and then select the **policy setting** link.
9. Select **Enabled**.
10. In the **Select Platform Security Level** drop-down list, select **Secure Boot and DMA Protection**.
11. In the **Credential Guard Configuration** drop-down list, select **Enabled with UEFI lock**.
12. In the **Secure Launch Configuration** drop-down list, select **Enabled**, and then select **OK**.
13. Close the Group Policy Management Editor.
14. Close the Group Policy Management Console.

### Task 2: Enable Windows Defender Credential Guard using the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool

1. On **SEA-ADM1**, select **Start**, and then enter **Powershell**.
2. Right-click or access the context menu for **Windows PowerShell**, and then select **Run as administrator**.
3. Navigate to **c:\labfiles\Mod08**.
4. Enter the following command:

* DG\_Readiness\_Tool.ps1 -Enable -AutoReboot

1. Your virtual machine will restart after the tool has completed running.
2. When the virtual machine restarts, reenter the credentials for **Contoso\Administrator**.

### Results

After completing this exercise, you will have:

1. Used Group Policy to implement Windows Defender Credential Guard on all computers in your organization.
2. Enabled Windows Defender Credential guard immediately on your local computer.

## Exercise 2: Locating problematic accounts

### Scenario

You want to check whether your organization has user accounts with passwords that are configured not to expire and remediate this setting. You also want to check which accounts haven’t signed in for 90 of days or more and disable them.

The main tasks for this exercise are to:

1. Locate and reconfigure accounts with passwords that don’t expire.
2. Locate and disable accounts to which no sign-ins have occurred for at least 90 days.

### Task 1: Locate and reconfigure accounts with passwords that don’t expire

1. Sign in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Open Windows PowerShell.
3. Enter the following command:

* Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $true}

1. Review the list of user accounts returned.
2. Enter the following command:

* Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $true} | Set-ADUser -PasswordNeverExpires $false

1. Rerun the command from step 3 and notice that no users are returned.

### Task 2: Locate and disable accounts to which no sign-ins have occurred for at least 90 days

1. Enter the following commands:

* $days = (Get-Date).Adddays(-90)  
  Get-ADUser -Filter {LastLogonTimeStamp -lt $days -and enabled -eq $true} -Properties LastLogonTimeStamp

1. In the lab environment, no accounts will be returned.
2. Enter the following command:

* Get-ADUser -Filter {LastLogonTimeStamp -lt $days -and enabled -eq $true} -Properties LastLogonTimeStamp | Disable-ADAccount

1. No results will be returned in the lab environment.

## Exercise 3: Implementing LAPS

### Scenario

At present, the same local administrator account password is used across all servers and workstations at Contoso. To remedy this problem, you will configure and deploy LAPs.

The main tasks for this exercise are:

1. Prepare OU and computer accounts for LAPS.
2. Prepare AD DS (Active Directory) for LAPS.
3. Deploy LAPS client-side extension.
4. Verify LAPS.

### Task 1: Prepare OU and computer accounts for LAPS

1. Sign in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Open Windows PowerShell.
3. Enter the following commands:

* New-ADOrganizationalUnit -Name "Seattle\_Servers"  
  Get-ADComputer SEA-SVR1 | Move-ADObject –TargetPath "OU=Seattle\_Servers,DC=Contoso,DC=com"

1. Enter the following command:

* Msiexec /I C:\Labfiles\Mod08\LAPS.x64.msi

1. When the **Local Administrator Password Solution Setup Wizard** opens, select **Next**.
2. Select **I accept the terms in the License Agreement**, and then select **Next**.
3. Under **Custom Setup**, in the drop-down menu next to **Management Tools**, select **Entire feature will be installed on the local hard drive**.
4. Select **Next**, select **Install**, and then select **Finish**.

### Task 2: Prepare AD DS for LAPS

1. In Windows PowerShell, enter the following commands:

* Import-Module admpwd.ps  
  Update-AdmPwdADSchema  
  Set-AdmPwdComputerSelfPermission -Identity "Seattle\_Servers"

1. Select **Start**, and then enter **Group Policy**.
2. Select **Group Policy Management**.
3. In the Group Policy Management Console, expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**, right-click or access the context menu for the **Seattle\_Servers** OU, and then select **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** dialog box, in the **Name** text box, enter **LAPS\_GPO**, and then select **OK**.
5. In the **Group Policy Management** window, under **Seattle\_Servers**, right-click or access the context menu for **LAPS\_GPO**, and then select **Edit**.
6. In the **Group Policy Management Editor** window, under **Computer Configuration**, expand the **Policies** node, expand the **Administrative Templates** node, and then select **LAPS**.
7. Select the **Enable local admin password management** policy, and then select the **policy settings** link.
8. In the **Enable local admin password management** window, select **Enabled**, and then select **OK**.
9. Select the **Password Settings** policy, and then select the **policy settings** link.
10. In the **Password Settings** policy dialog box, select **Enabled**, and then configure **Password Length** to **20**.
11. Verify that the **Password Age (Days)** is configured to **30**, and then select **OK**.
12. Close the Group Policy Management Editor.

### Task 3: Deploy LAPS client-side extension

1. Switch to **SEA-SVR1**, using **Contoso\Administrator** with the password **Pa55w.rd**.

**Note**: You will be prompted to change your password, due to the previous exercise. Use the new password in place of the documented password throughout the remainder of the lab.

1. Enter the following command:

* Msiexec /I \\SEA-ADM1\c$\Labfiles\Mod08\LAPS.x64.msi

1. When the **Local Administrator Password Solution Setup Wizard** opens, select **Next**.
2. Select **I accept the terms in the License Agreement**, and then select **Next**.
3. Select **Next** again, and then select **Install**.
4. Select **Finish**.
5. Enter the following command:

* gpupdate /force

### Task 4: Verify LAPS

1. Switch to **SEA-ADM1**.
2. Select **Start**, select **LAPS**, and then select **LAPS UI**.
3. In the **LAPS UI** dialog box, in the **ComputerName** text box, enter **SEA-SVR1**, and then select **Search**.
4. Review the **Password** and the **Password expires** values, and then select **Exit**.
5. In the Windows PowerShell window, enter the following command:

* Get-ADComputer SEA-SVR1 -Properties ms-Mcs-AdmPwd

1. Review the password assigned to SEA-SVR1.
2. Close the gridview window.

### Results

After completing this lab, you will have:

* Prepared an OU and computer accounts for LAPs.
* Prepared your AD DS for LAPS.
* Deployed LAPS client-side extension.
* Verified that you implemented LAPS successfully.

©2019 Microsoft Corporation. All rights reserved. The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are ***not*** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.