# Policy Implementation Lab

Joshua Main-Smith

2020-11-22

## Contents

# Policy Implementation

## Introduction

After attending the United States Government Configuration Baseline (US-GCB) for Microsoft content seminar, Richard LeGrand of DASWebs Inc. relayed important security policies that needed to be implemented. These policies were

1. Limit private information from being sent to Microsoft

2. Deny user based security change within Explorer

3. Disable Cross-Site Scripting

4. Proper signature download verification via Internet Explorer

These changes are to be made in the Domain-Controller, which is running Microsoft Windows Server 2008 R2 Standard. An outline of DASWeb Inc. infrastructure can be seen in the image below.
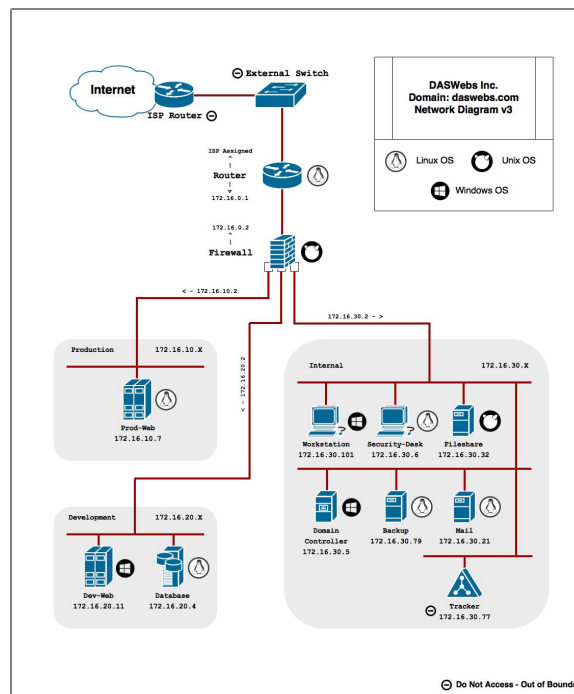


## Disable Microsoft Customer Experience Improvement

To disable Microsoft Customer Experience Improvement (CEIP), we opened **Group Policy Management** (GPM) by navigating to **Start** >**Administrative**

**Tools** >**Group Policy Management**. Under GPM, we then opened the editor under **Forest: ad.daswebs.com** >**Domains** >**ad.daswebs.com** then right-click **DasGroup** and select **Edit**. The CEIP policy is located under **Computer Configuration** >**Policies** >**Administrative Templates: Policy definitions** >**System** >**Internet Communication Management** >**Internet Communication Settings**. Double-click **Turn off Windows Customer Experience Improvement Program** and select **Enabled** and **Apply** under the window that pops up.
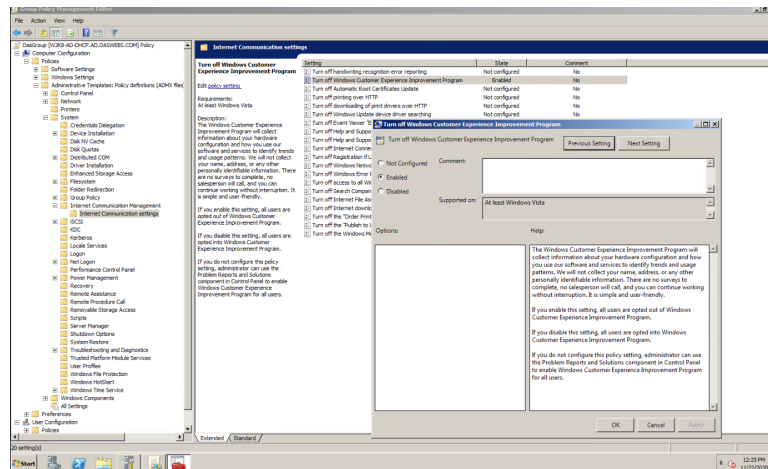


## Disable Security Tab

To prevent users from changing the security settings within windows explorer we can disable access to the security tab all together. To do this, we opened to the **Group Policy Management Editor** then navigated to **User Configuration** >**Policies** >**Administrative Templates: Policy definitions** >**Windows Components** >**Windows Explorer** then double-click on **Remove Security tab**. Under the window that pops up, toggle **Enabled** and click **Apply**.
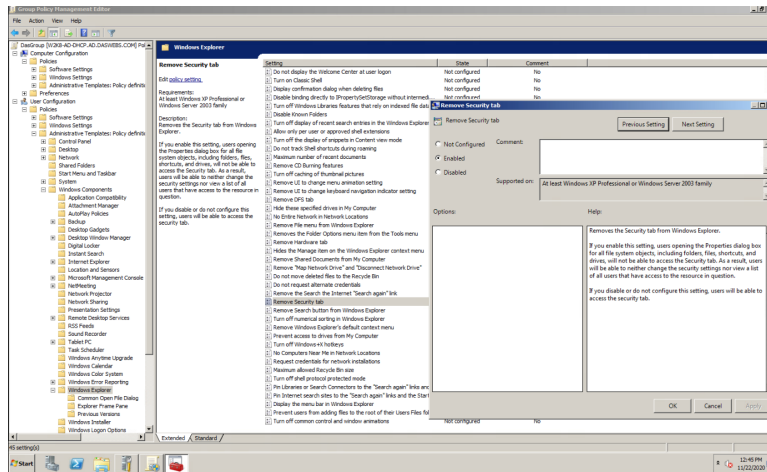
## Disable Cross-Site Scripting Improvement

To disable Cross-Site Scripting (XSS), open the **Group Policy Management Editor** and navigate to **Computer Configuration >Policies Administrative Templates: Policy definitions >Windows Components >Internet Explorer >Internet Control Panel >Security Page >Internet Zone** then double-click **Turn on Cross-Site Scripting (XSS) Filter**. Under the window that pops up, toggle **Enabled** and select **Enable** for the drop-down menu, then click **Apply**.
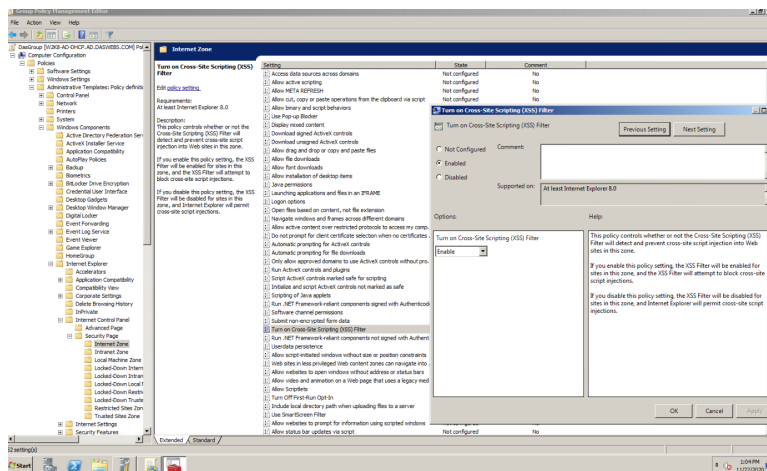


## Disable Downloads Without Correct Signatures for Files

To only allow programs with correct signature to download via Internet Explorer, open **Group Policy Management Editor** and navigate to **Computer**

**Configuration >Policies Administrative Templates: Policy definitions >Windows Components >Internet Explorer >Internet Control Panel >Advanced Page** then double-click **Check for signatures on downloaded programs**. Under the window that pops up, toggle **Enabled** and click **Apply**.