|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| **Lab Report** |
| COURSE: Cyber 262  LAB: Deploying Endpoint Protection  Submitted BY: Jack Morgan  Date: 01/31/2022  Instructor: Hozza |
| *By submitting this report, I certify that this is my work and was not copied from other sources. Any use of public materials is cited.* |

Table of Contents

[INTRODUCTION 3](#_Toc50470226)

[SCREEN CAPTURES 4](#_Toc50470227)

[REFLECTION 8](#_Toc50470228)

# INTRODUCTION

In this lab we will be learning how to administer and deploy endpoint protection on practice labs. From what we learned during this week of classes, we will most likely be administering protection such as firewalls, antimalware software and creating backups of our existing system states. In addition to administration, we will be learning how to update antimalware on our systems and how to manage everything we input. These are crucial skills to understand in cyber security to understand protection and keep our information safe. This is a key skill that all employers will want their employees to know, and this is a great way to start our learnings.

# SCREEN CAPTURES

***Figure (1):*** *Ex1 – Task 1 – Step 11: Proof that Endpoint Site System Role was added to the Primary Site*

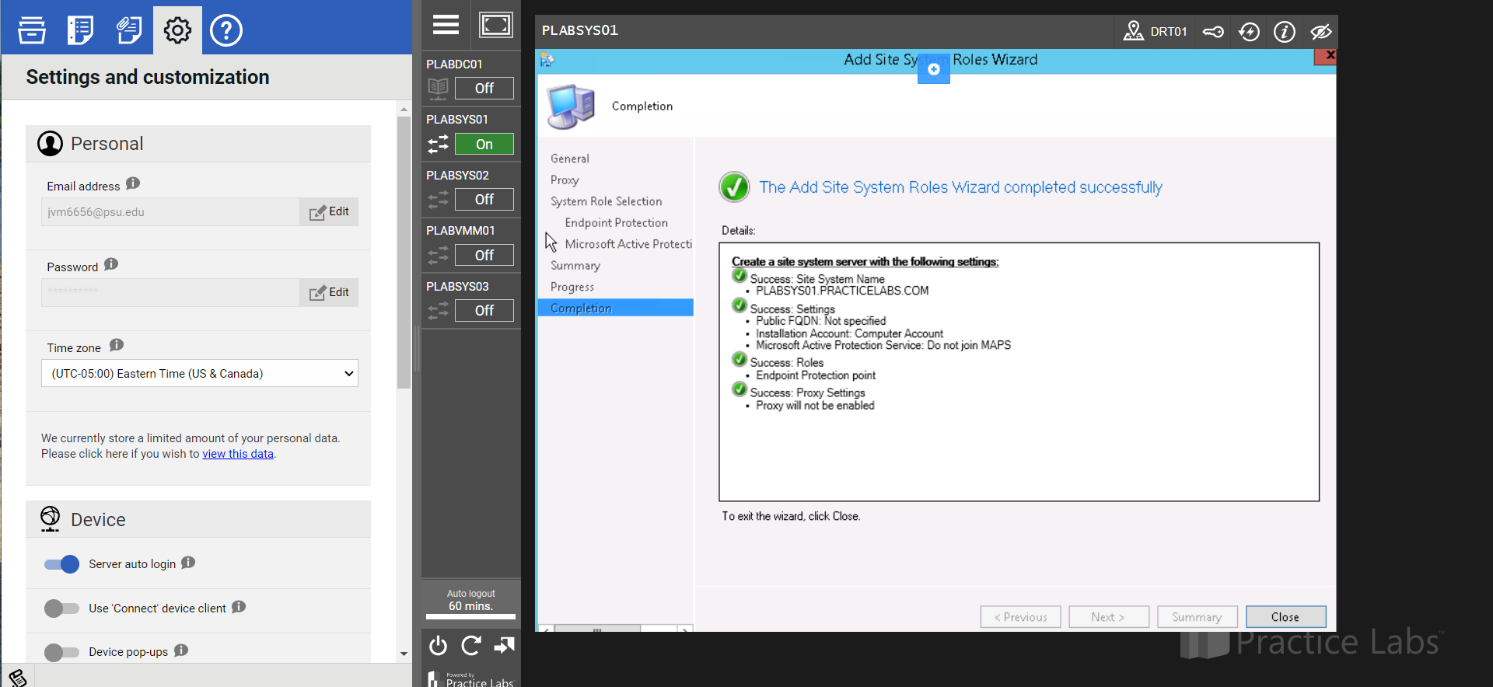
**

Figure : Shows proof that the Endpoint Site System Role is added after going through all of the system settings.

***Question:*** *Ex 1 – Task 1 – Step 11: Describe in your own words what purposes Microsofts System Center serves in an enterprise? Please include a how it helps organizations manage endpoints and enforce policies.*

Microsofts System Center serves an enterprise by enabling the management, deployment and security of virtualization and devices across an enterprises’ network. This allows for a single entity to be able to control the most important aspects of a system including an enterprises security. In addition to these endpoint protection systems, this could also include protections such as firewalls that can prevent employees from accidentally accessing malware or releasing crucial information.

***Figure (2):*** *Ex 1 – Task 2 – Step 8: Proof that Step 8 showing all alerts and Repeated Malware Detection was added to all alerts.*

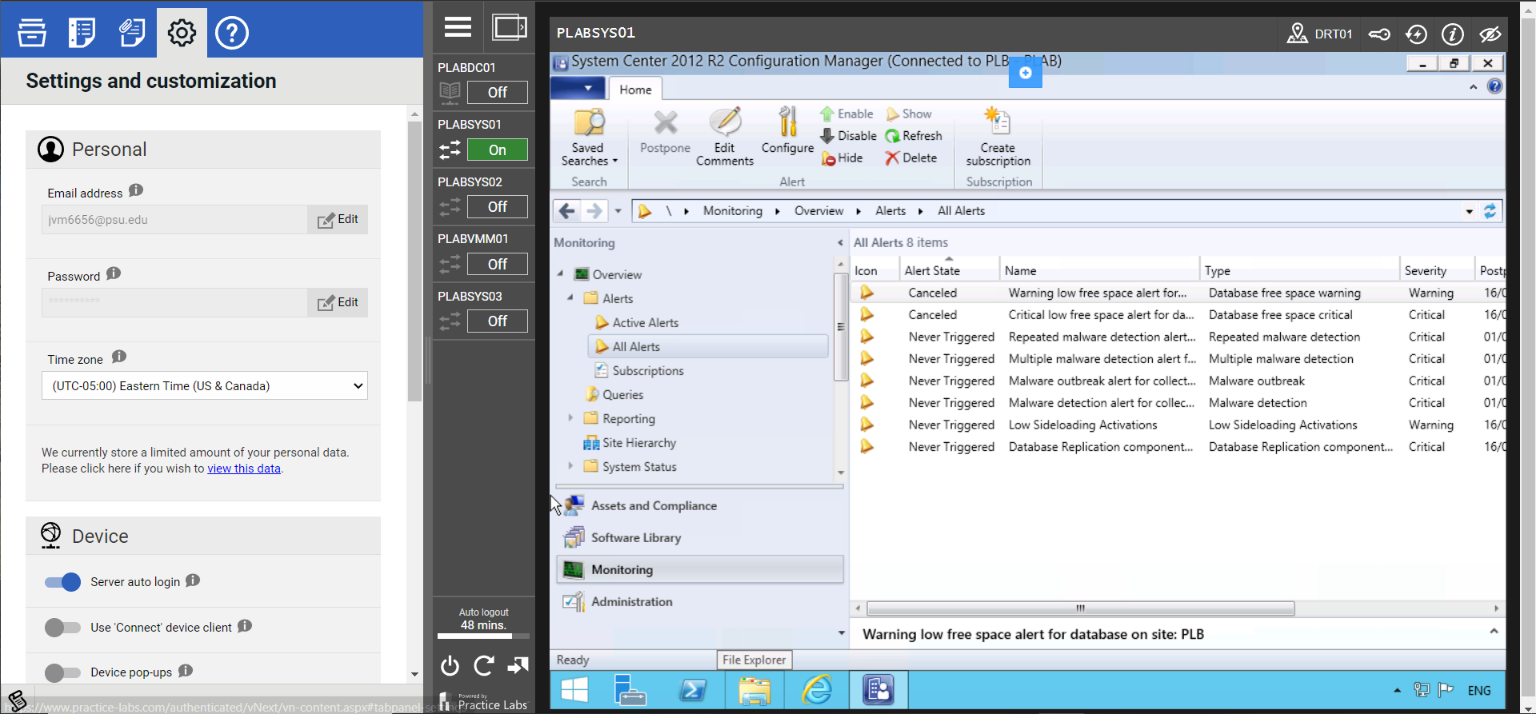
**

Figure : Shows proof that all the alerts and repeated malware detection was added

***Figure (3):*** *Ex 2 – Task 1 – Step 27: Proof from step 27 showing System Center 2012 R2 Configuration Manager, Automatic Deployment Rules.*

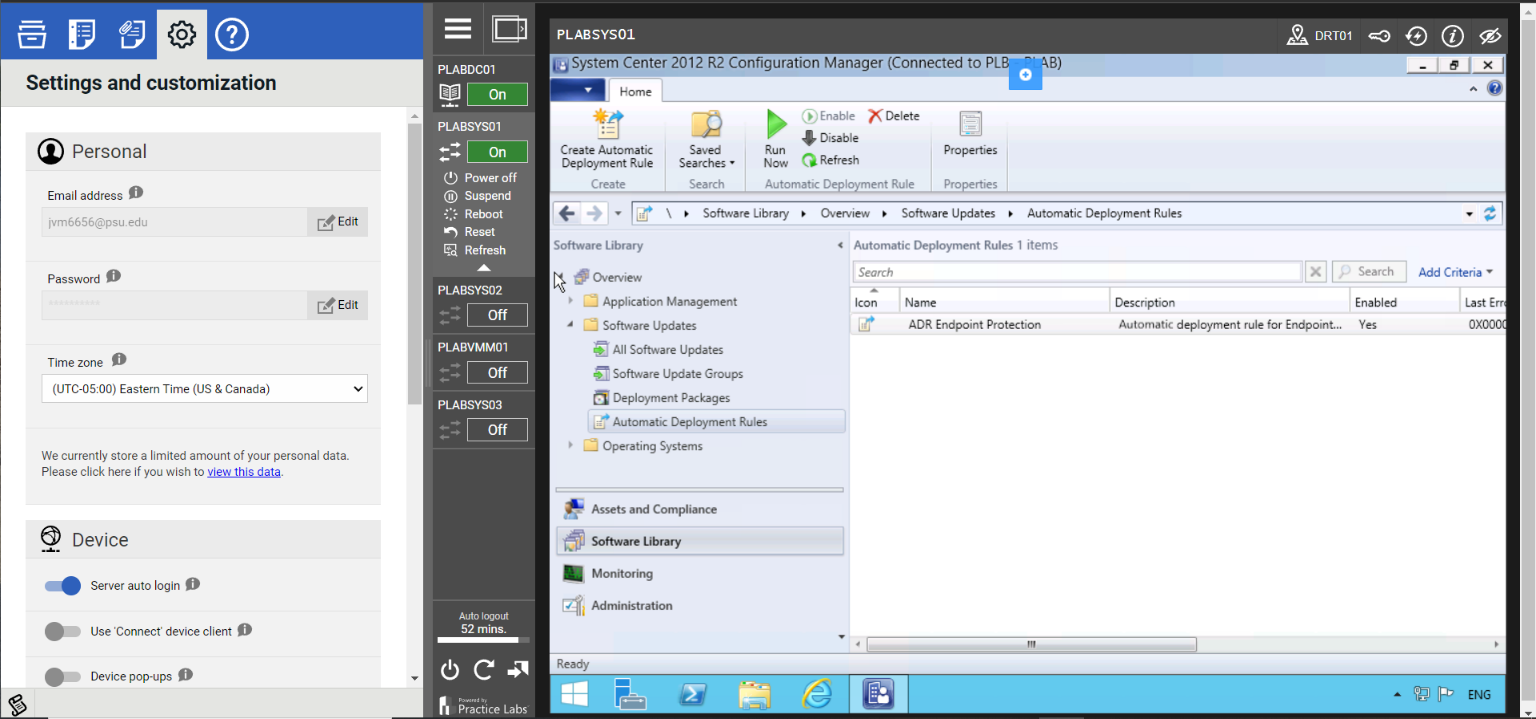
**

Figure : After finishing Automatic Deployment Rules, we can see the existing changes under the description of teh ADR Endpoint Protection

***Figure (4):*** *Ex 3 – Task 1 – Step 15: Under Assets and Compliance there is a drop down for Compliance Settings. Review one compliance setting and explain how they can help secure an organizations endpoints. For example, User data and profiles.*

Company Resource Access: Under this company resource access tab, users have the option to manage profiels for certificates, VPNs and Wi-fi. In these setting options we can manage existing profiles or add new profiles in order to manage existing or new profiles in an administration. This is also an example of authoritative control, where one user can control all the existing profiles in a network.

***Figure (5):*** *Ex 4 – Task 1 – Step 9: Proof that Step 9 showing the results when clicking your ‘deploments’ tab. We want to see All Systems as endpoints.*

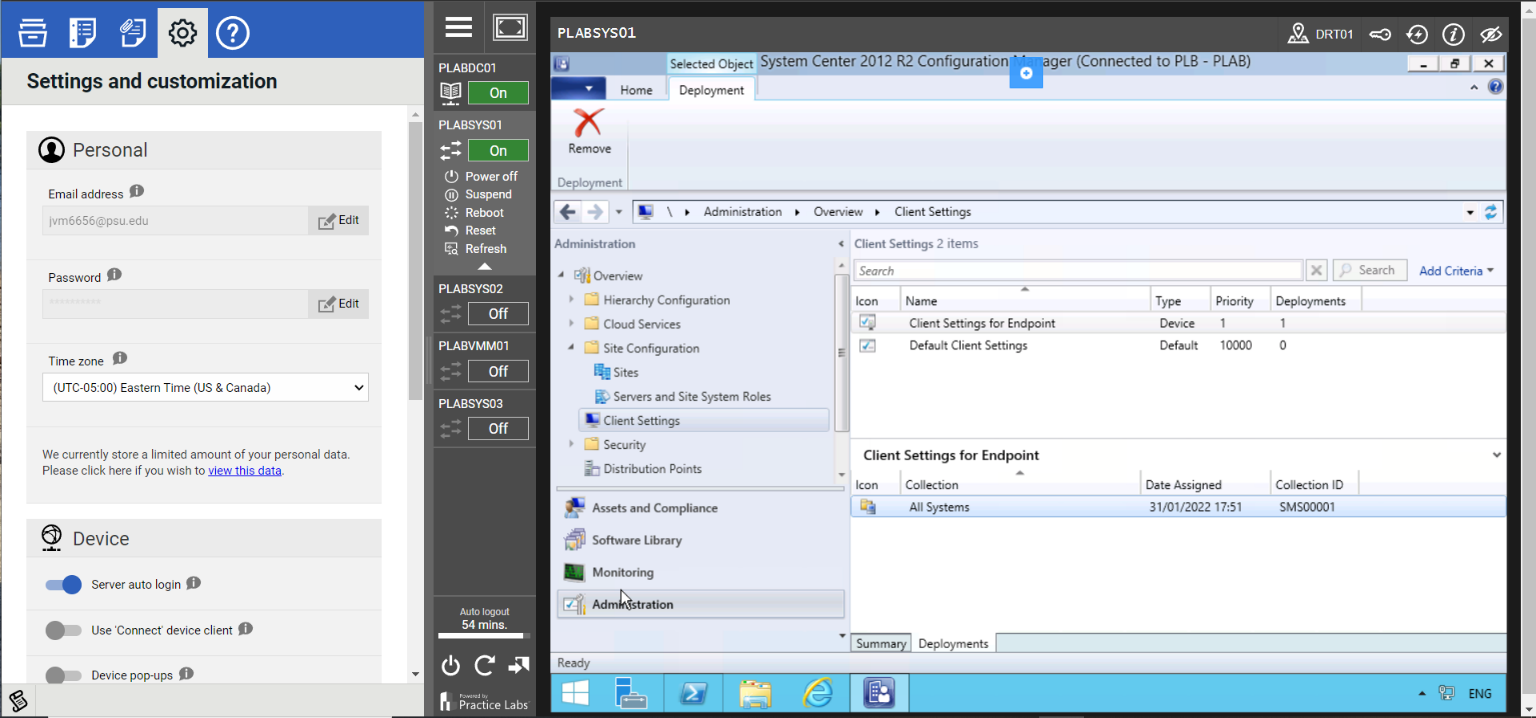
**

Figure : After making all of the changes to the endpoint system we can see that it says All Systems under the client settings as we expected.

***Figure (6):*** *Ex 5 – Task 2 – Step 2: Your screen shot should show the Green Checkmark and that your PC is being monitored and protected. Real-time protection and virus and spyware definitions may not be up to date due to the lab machines internet connectivity.*

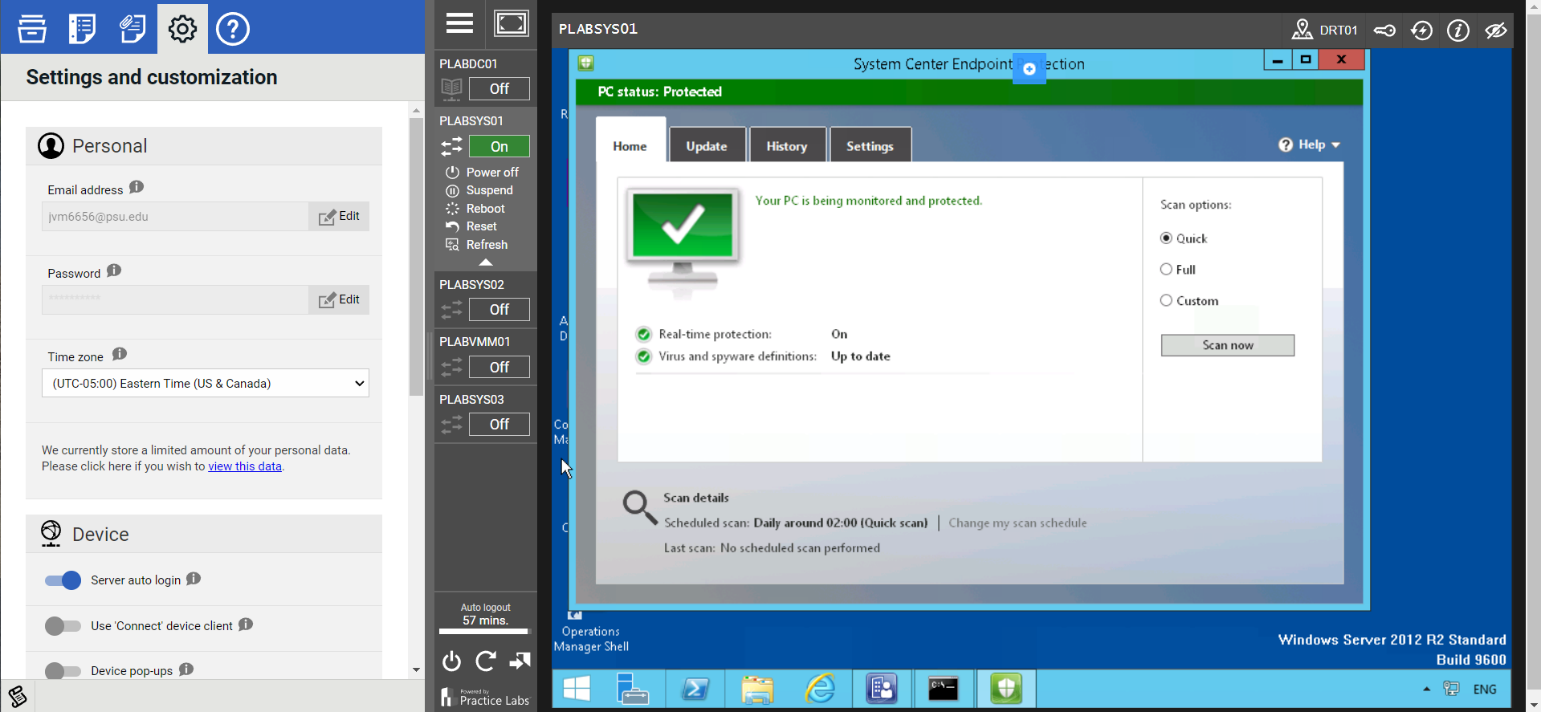
**

Figure : After finishing all the required changes, we can see that the changes were successfully made and administered and that the virus and spyware definitions are up to date as expected.

***Question:*** *Ex 5 – Task 2 – Step 2: Describe in your own words* ***why*** *you would build a “reference” computer and image it?*

Our reasoning for building a reference computer and imaging it is so that we can create a “standard” configuration that we can always refer to. This also allows administration to push out all settings and changes to other systems based of of the “standard.”

# REFLECTION

During this lab we learned crucial skills that will helps us down the line in our Cyber Security careers. By learning how to deploy endpoint protection this early on, we will eventually be able to expand upon this knowledge and perform stronger endpoint protection such as secure firewalls that will allow us to better protect our data, information, and personnel. After performing this lab, we can see how our learnings in class can connect to what we did during this lab. For example, we made changes to security systems that would fit under authoritative controls. The manager or employee in charge of these systems must know how to make these changes in order to protect an administrations data and personnel.