



My

---

# Tech Home Lab

*Richardo J. Hinds*

# TABLE OF CONTENTS

---

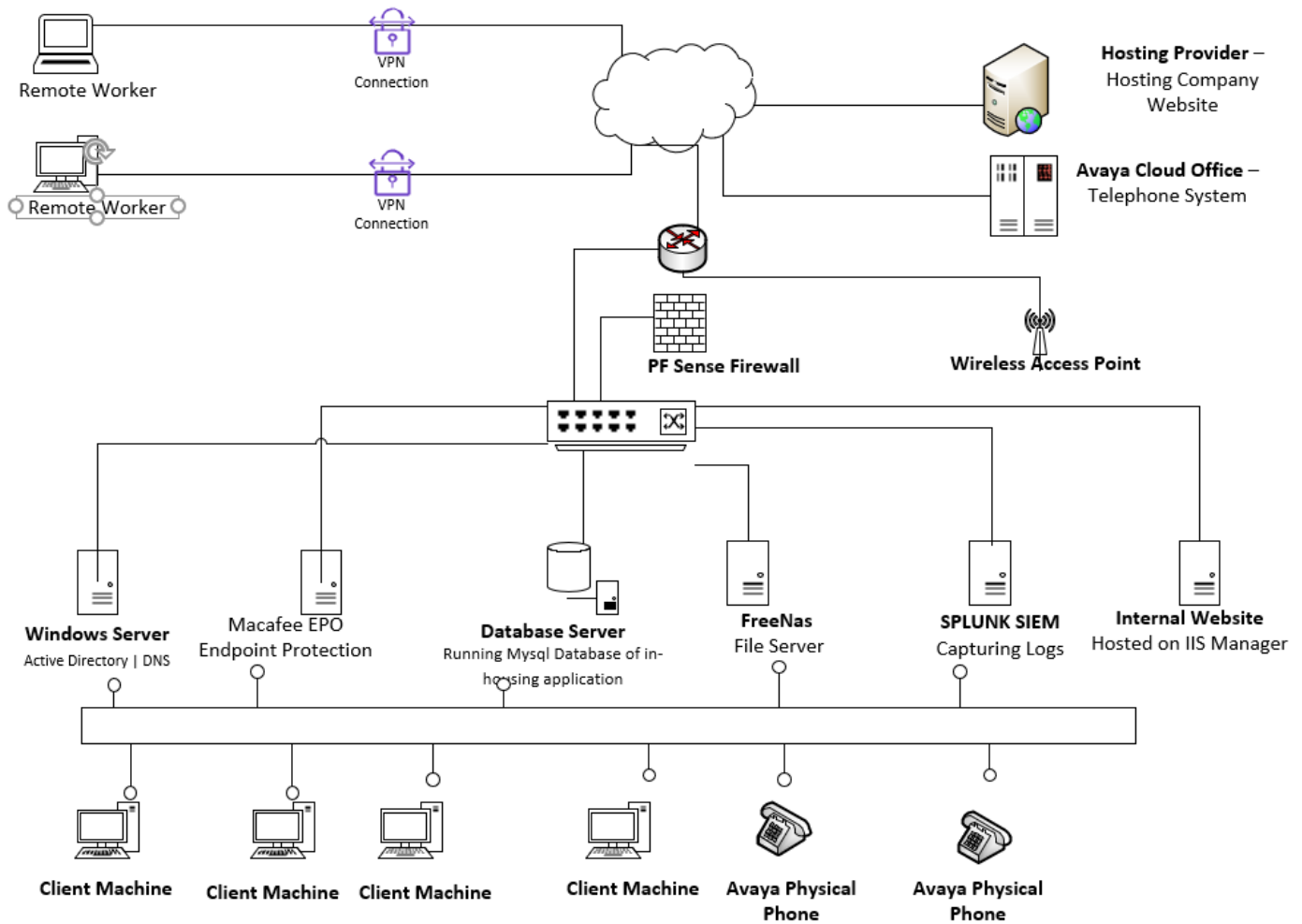
|   |    |
|---|----|
| Summary Of the Lab .....                                | 3  |
| Networking Diagram .....                                | 4  |
| Active Directory and Administration .....               | 5  |
| Remote Server Administration Tools (RSAT).....          | 7  |
| Group Policy.....                                       | 8  |
| Tech Ticketing System .....                             | 9  |
| Drive Encryption .....                                  | 10 |
| Merging two Partitions .....                            | 10 |
| Truenas File Server.....                                | 11 |
| Applying Content Filtering Using Pf Sense Firewall..... | 11 |
| Macafee Endpoints .....                                 | 12 |
| Macafee Endpoints .....                                 | 13 |
| Microsoft 365 .....                                     | 14 |
| Software Inventory Using Spiceworks.....                | 15 |
| Inventory Management - Spiceworks.....                  | 16 |
| VPN – Remote Access .....                               | 16 |
| Hosting Website on IIS Manager .....                    | 17 |

## Summary Of the Lab

### Technologies / Tools

| Technology / Tools                        | Category   | Purpose   |
|---|--|---|
| Remote server Administration Tools (RSAT) | <b>Administrating Active directory from Client Machine</b> | <b>Access the Server to perform IT administration</b>   |
| Veem backup & Replication                 | <b>Backup Tool</b>   | <b>Backup endpoints</b>   |
| TrueNas                                   | <b>File Server</b>   | <b>File Server that will be used to stroe the organization's data. Access Control List gives certain users certain access to access and modify files.</b> |
| Spiceworks                                | <b>Tech Ticketing System</b>                               | <b>A customized spice work has been created to use as the Tech Ticketing System accessible to all clients</b>   |
| Avaya Cloud Office                        | <b>Phone System</b>  | <b>This is a cloud-based Technology telephony system</b>  |
| Macafee EPO                               | <b>Endpoint Protection</b>                                 | <b>Antivirus Tools that manage and protects endpoints from virus and Malware</b>  |
| SoftEther VPN                             | <b>VPN</b>   | <b>Allow Remote workers to access internal database and network resources on the network</b>  |
| Bitlocker Encryption                      | <b>Drives Encryption</b>                                   | <b>Encrypting client drive.</b>   |
| IIS Manager on Windows Server 2016        | <b>Website Hosting</b>                                     | <b>Host a website via IIS Manager. This website is only accessible to remote users accessing the VPN.</b>   |

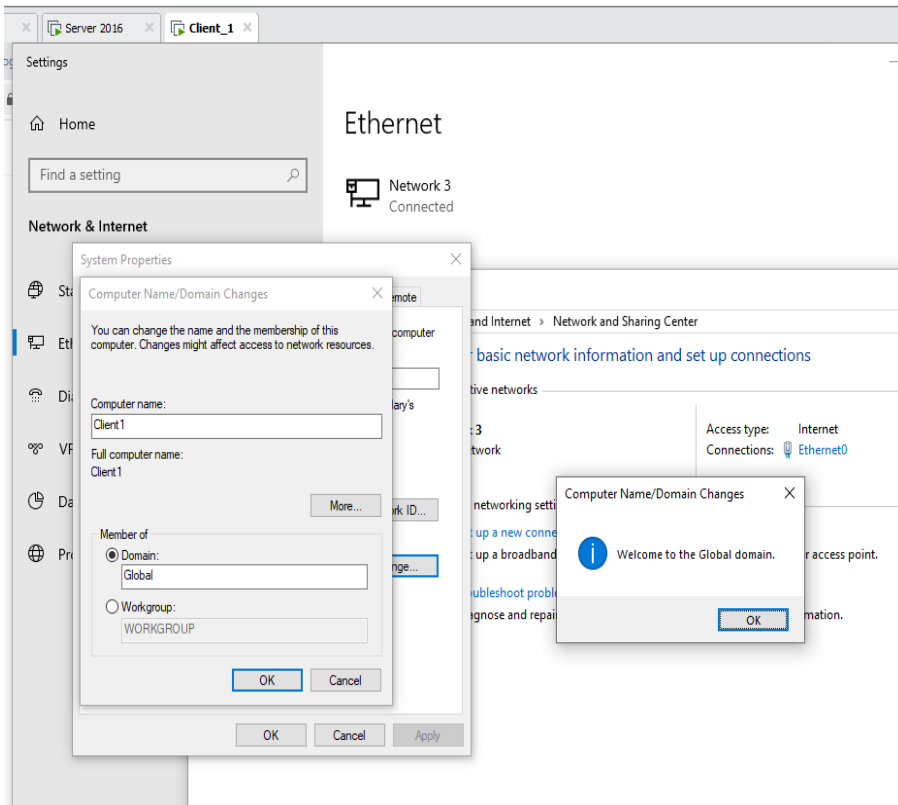
# Networking Diagram



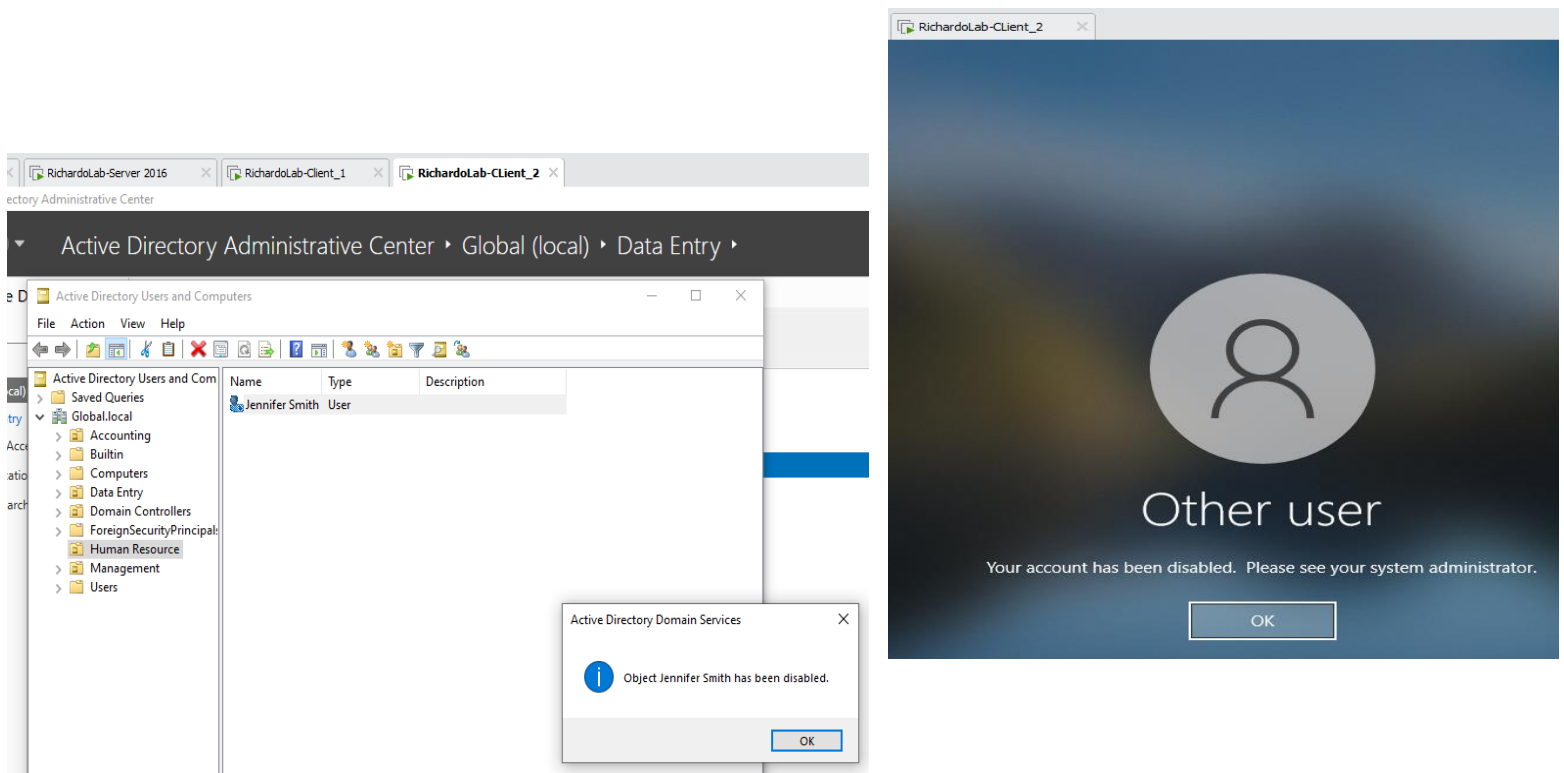
|                        |                    |
|------------------------|--------------------|
| <b>Maxine Campbell</b> | <b>192.168.1.2</b> |
| <b>Steve Campbell</b>  | <b>192.168.1.3</b> |
| <b>Jennifer Smith</b>  | <b>192.168.1.4</b> |
| <b>Matthew Samuels</b> | <b>192.168.1.5</b> |
| <b>Sarah Paul</b>      | <b>192.168.1.6</b> |
| <b>John Paul</b>       | <b>192.168.1.7</b> |

# Active Directory and Administration

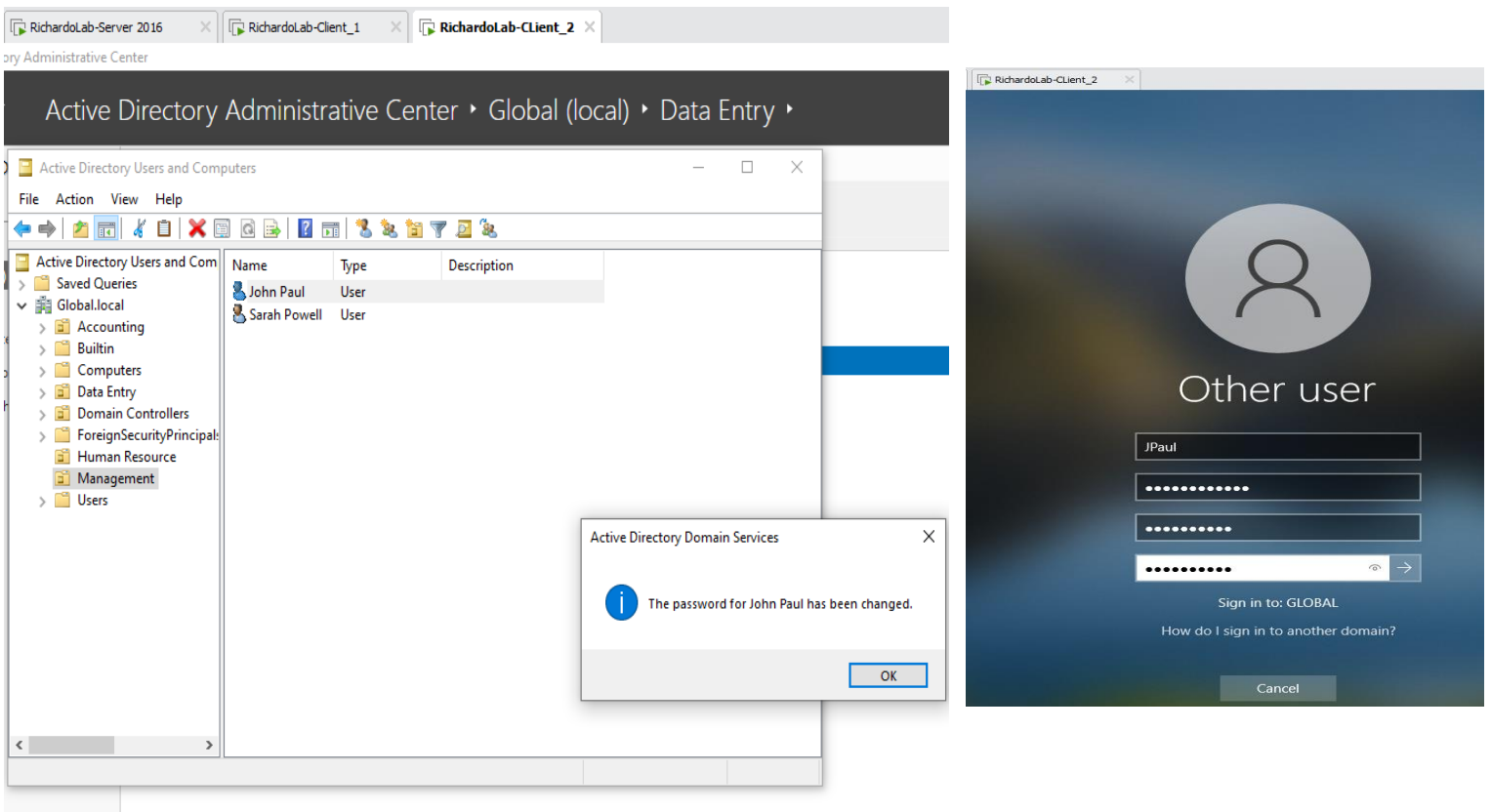
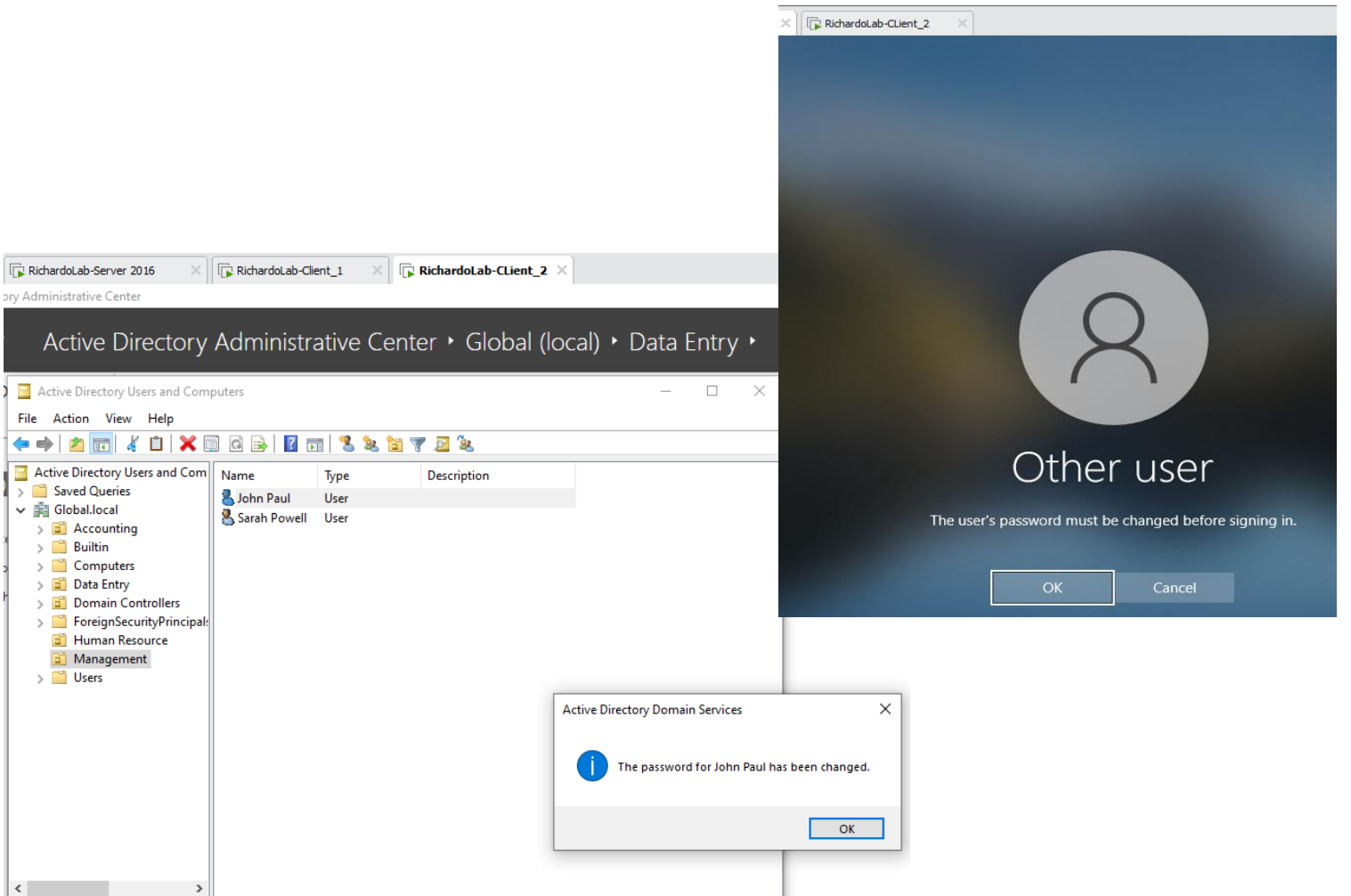
## Joining machine to the Domain



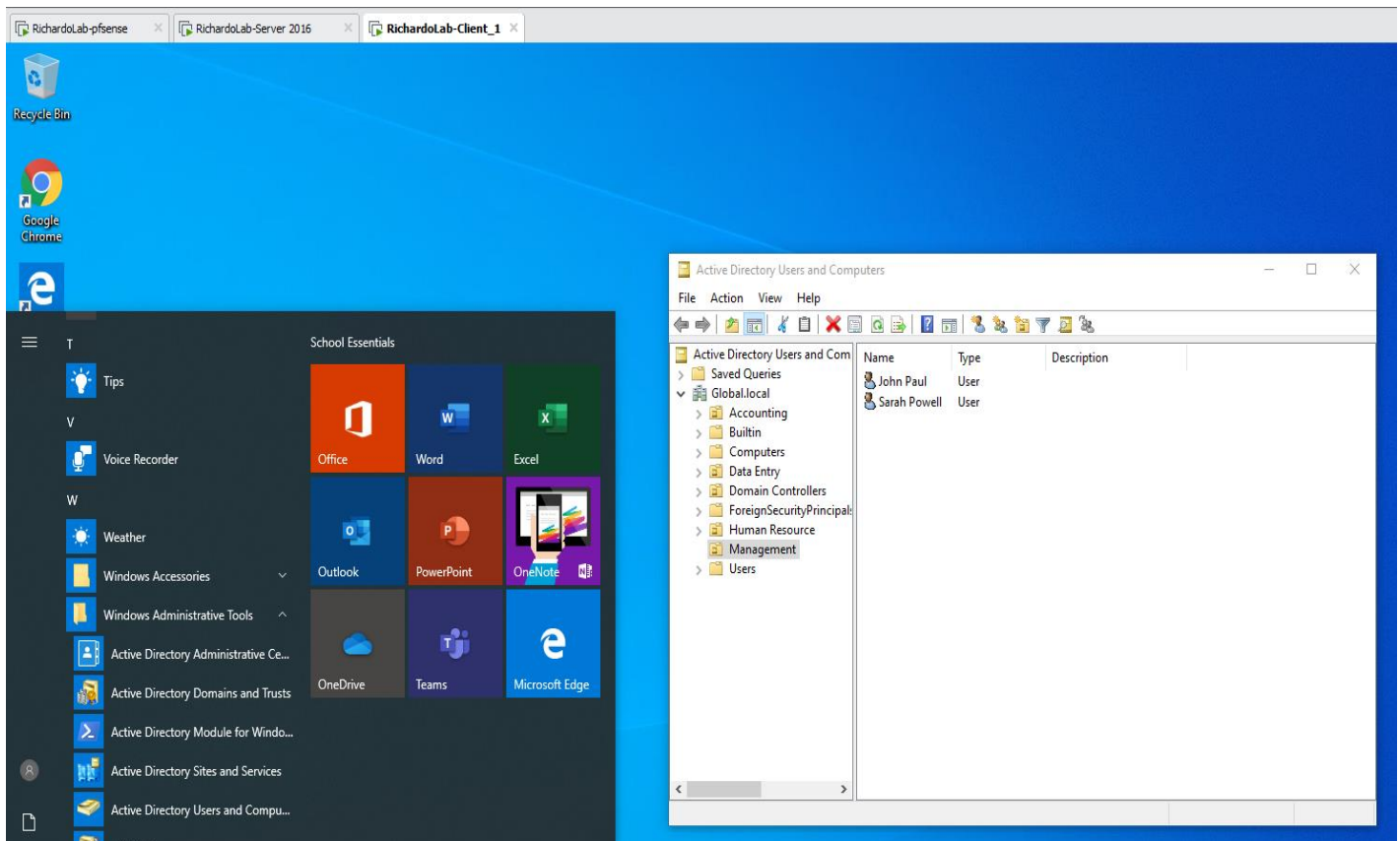
## Disabling an User



# Reseting user Password

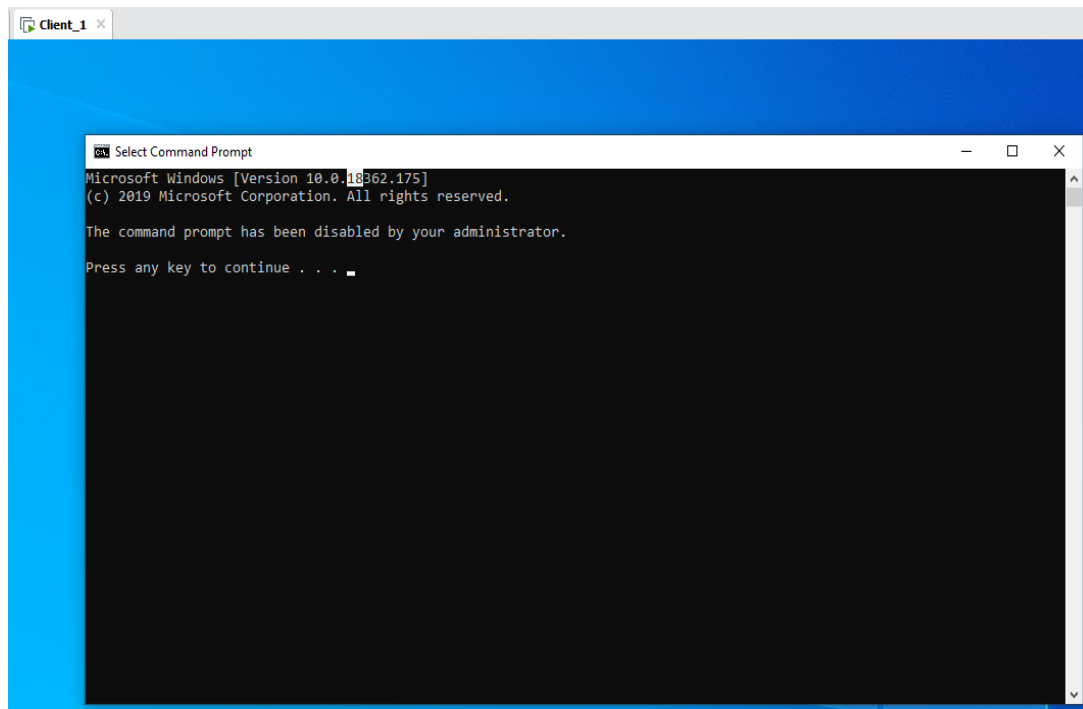


# Remote Server Administration Tools (RSAT)



*Performing Active Directory Administration From Clients Machines*

# Group Policy



*Preventing client users from accessing the command line.*



# Tech Ticketing System

Client View - <https://hindslab.on.spiceworks.com/portal>

Tech Support View

## Welcome to Hinds Tech Zone Lab Helpdesk

**Submit a help desk ticket**

Simply create a ticket below. A technician will respond promptly to your issue. You may also send tickets directly to [help@hindslab.on.spiceworks.com](mailto:help@hindslab.on.spiceworks.com)

Contact Email (required)

Summary (required) 0 / 255

Description (required) 0 / 2000

Category (required)

Name (required) 0 / 255

**Submit**

The screenshot shows the Spiceworks Tech Support View interface. At the top, there's a navigation bar with 'spiceworks' logo and search bar. Below it, a 'Tickets' tab is active, displaying a table of open tickets. Ticket #7 is highlighted with a red circle. Below the table, the details for ticket #7 are shown, including the title 'End Users are able to use command prompt', the creator 'Portal Guest', and the description 'I saw an end user using command prompt. I'm kindly asking to block such capability. Only give permission to me and Sarah Powell'. The user email 'jpaul@global.com' is also circled in red.

| ID | SUMMARY                                  | ASSIGNEE | CREATOR      | ORGANIZATION    | PRIORITY | CATEGORY | DUE | UP |
|----|--|----------|--------------|-----------------|----------|----------|-----|----|
| 7  | End Users are able to use command prompt | Accept   | Portal Guest | Hinds Tech Zone | Medium   | Software |     | 10 |
| 6  | Software Installation                    | Accept   | Portal Guest | Hinds Tech Zone | Medium   | Software |     | 10 |

**#7** Submitted by Portal Guest on Wednesday, October 13th 2021 at 12:06 pm **Accept** **Close** **Mute** **Remote Session** **More**

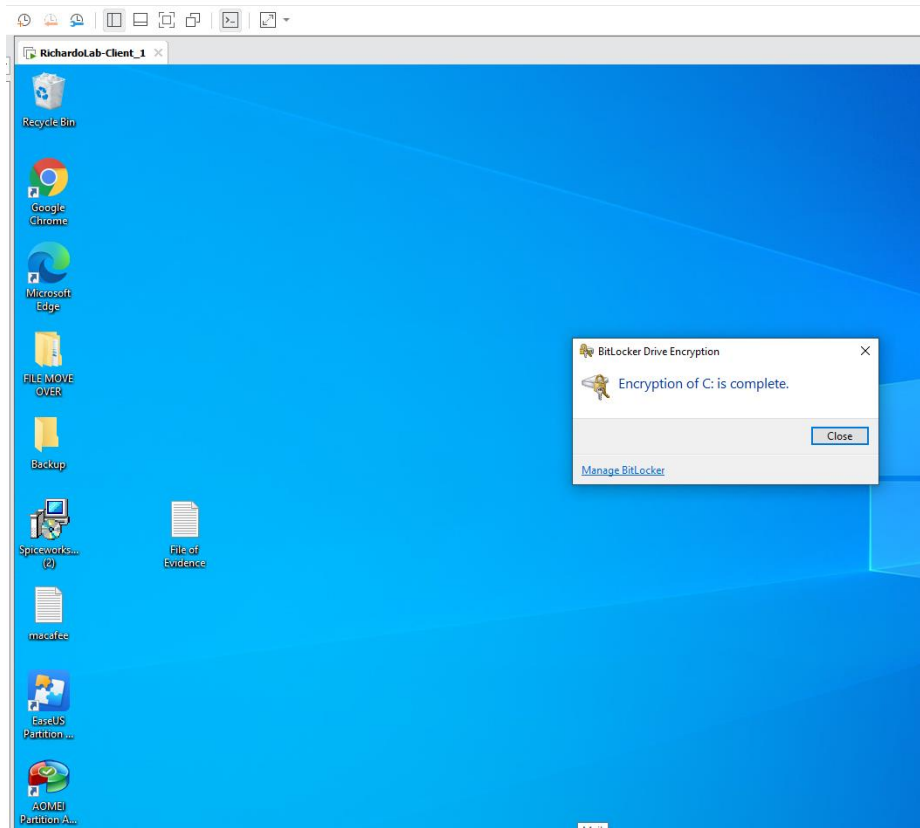
**HINDS TECH ZONE**

### End Users are able to use command prompt

Ticket created by an unauthenticated user: [jpaul@global.com](mailto:jpaul@global.com)

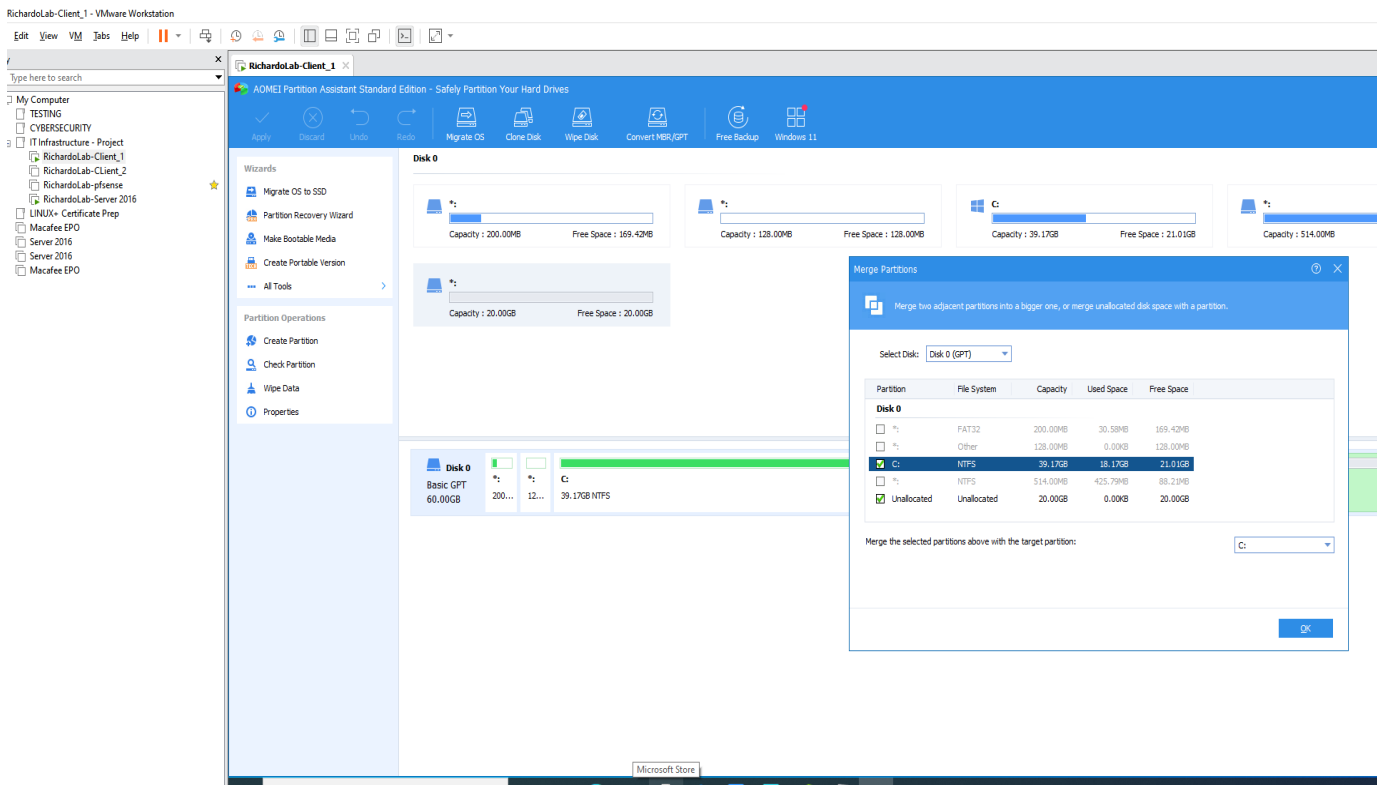
I saw an end user using command prompt. I'm kindly asking to block such capability. Only give permission to me and Sarah Powell

# Drive Encryption

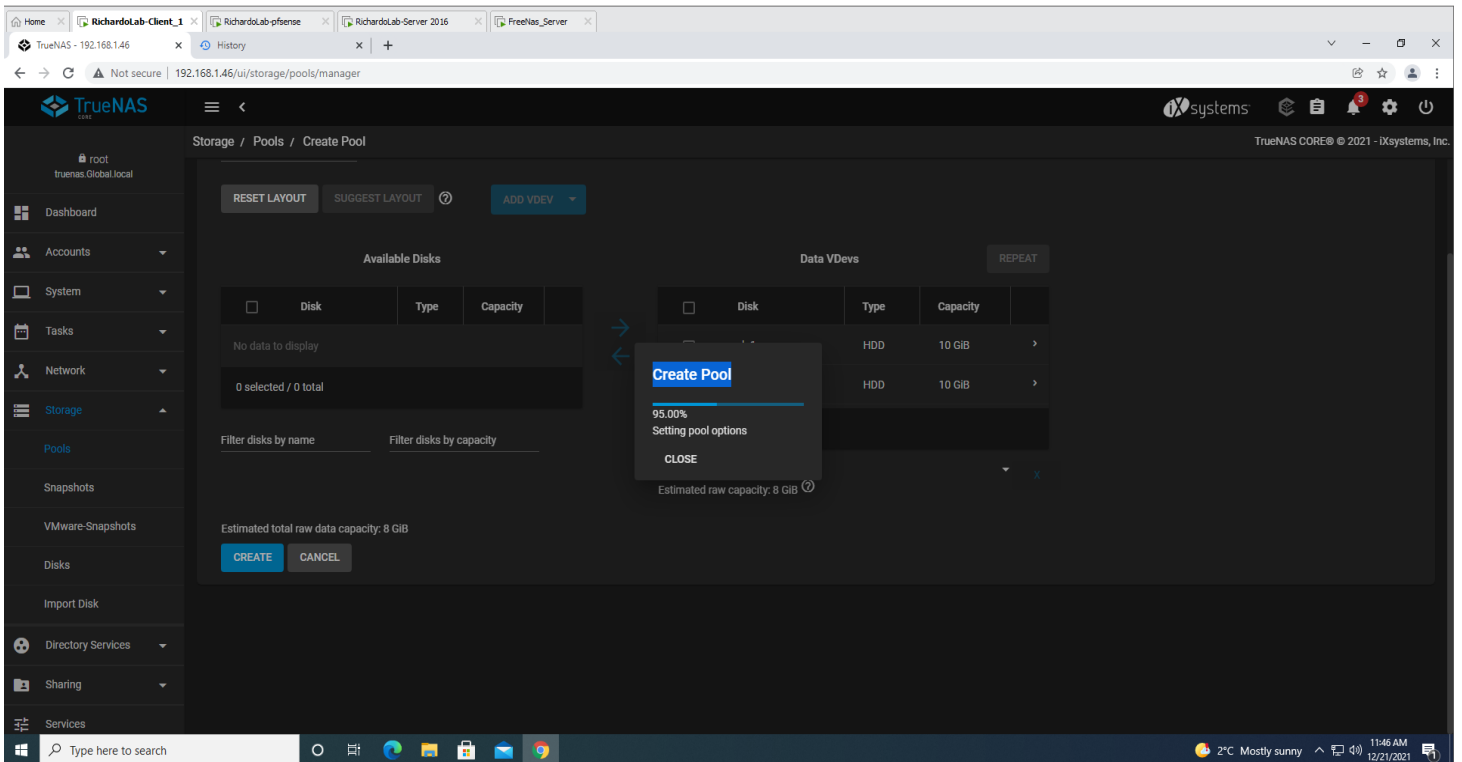


*Hard Drive are encrypted using BitLocker*

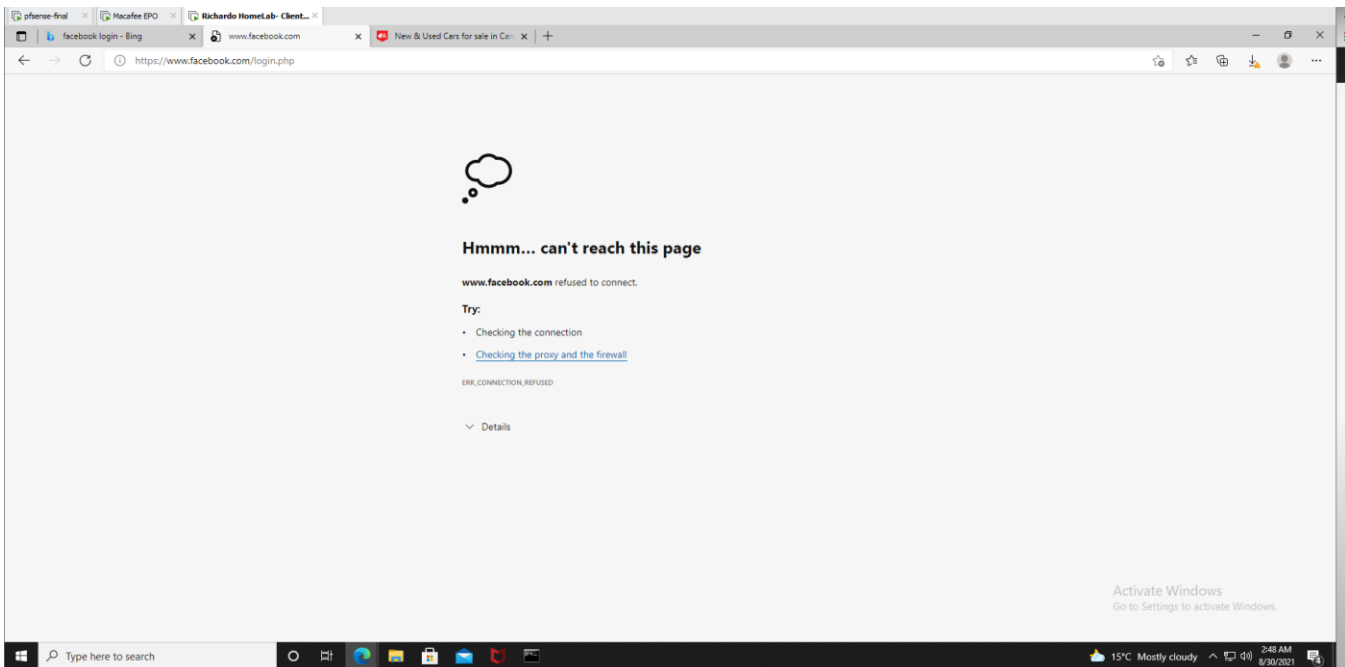
# Merging two Partitions



# Truenas File Server

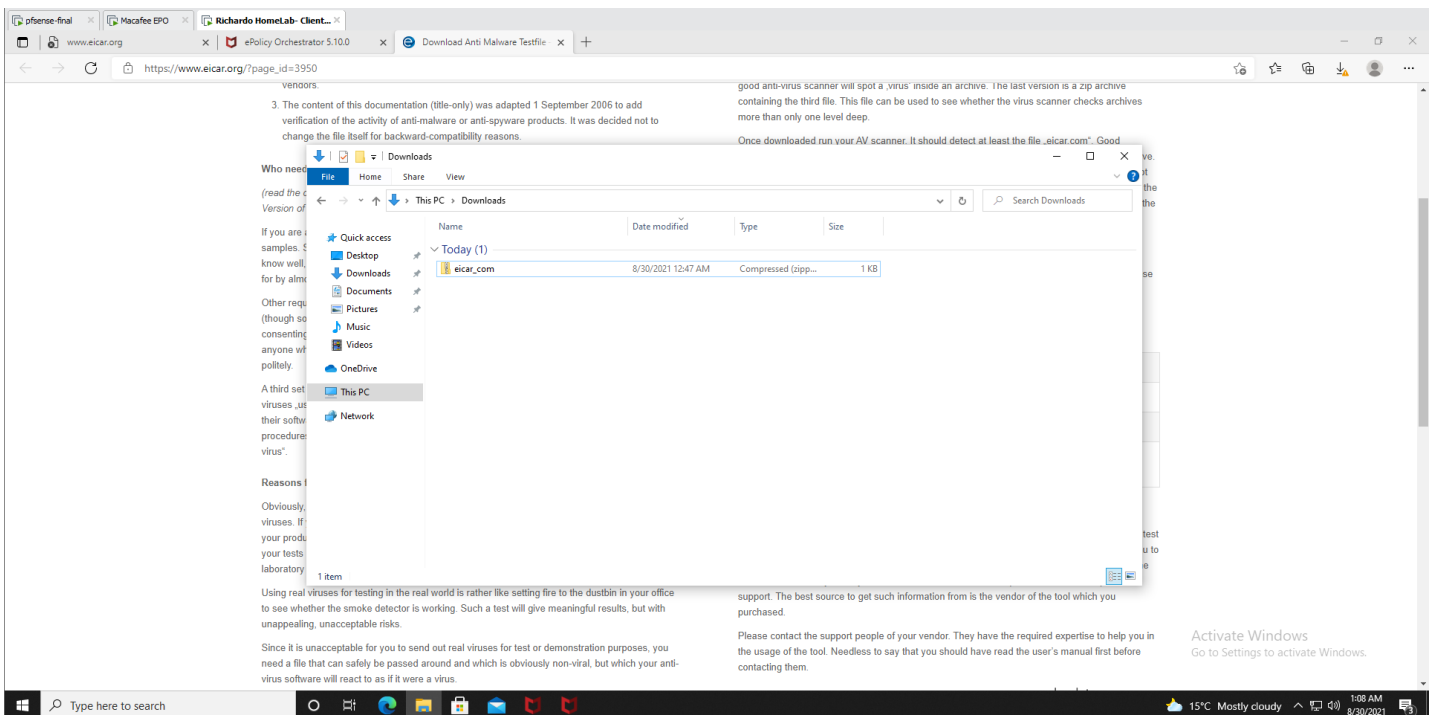
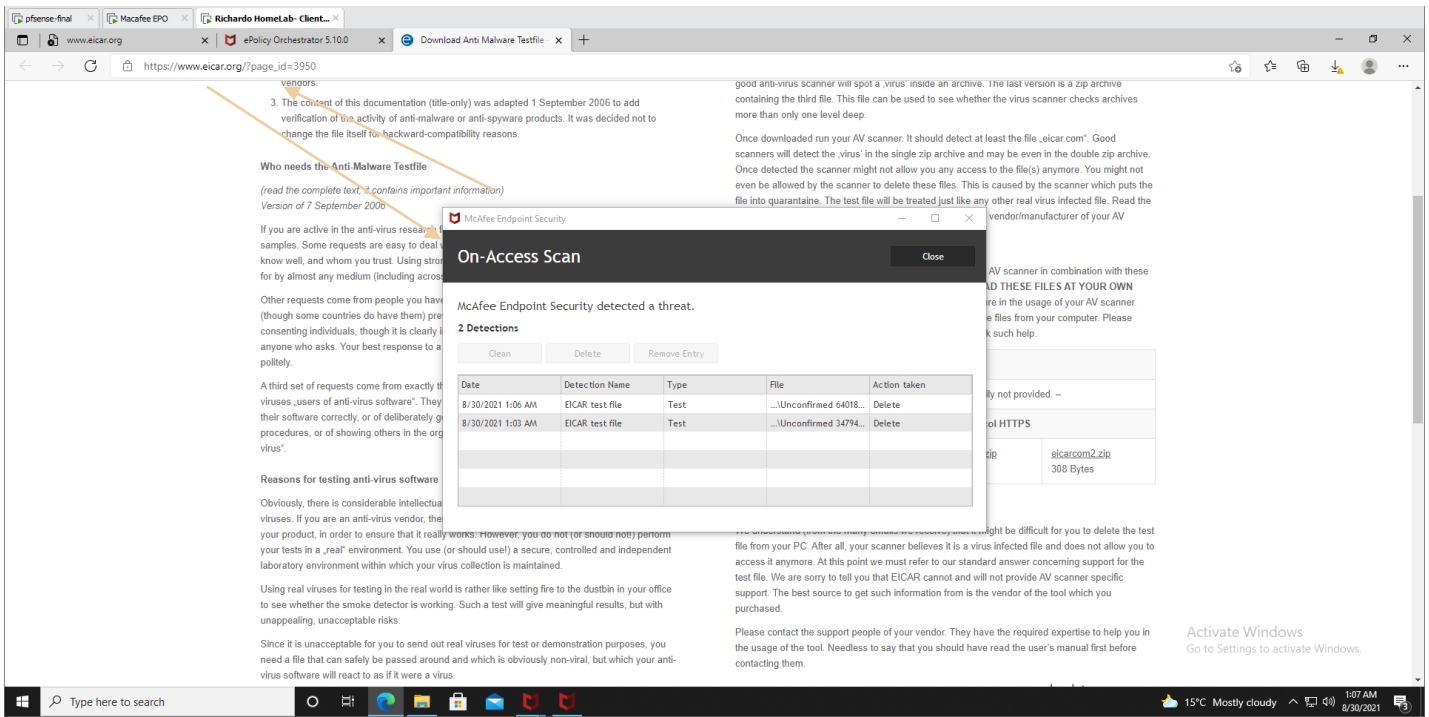


# Applying Content Filtering Using Pf Sense Firewall



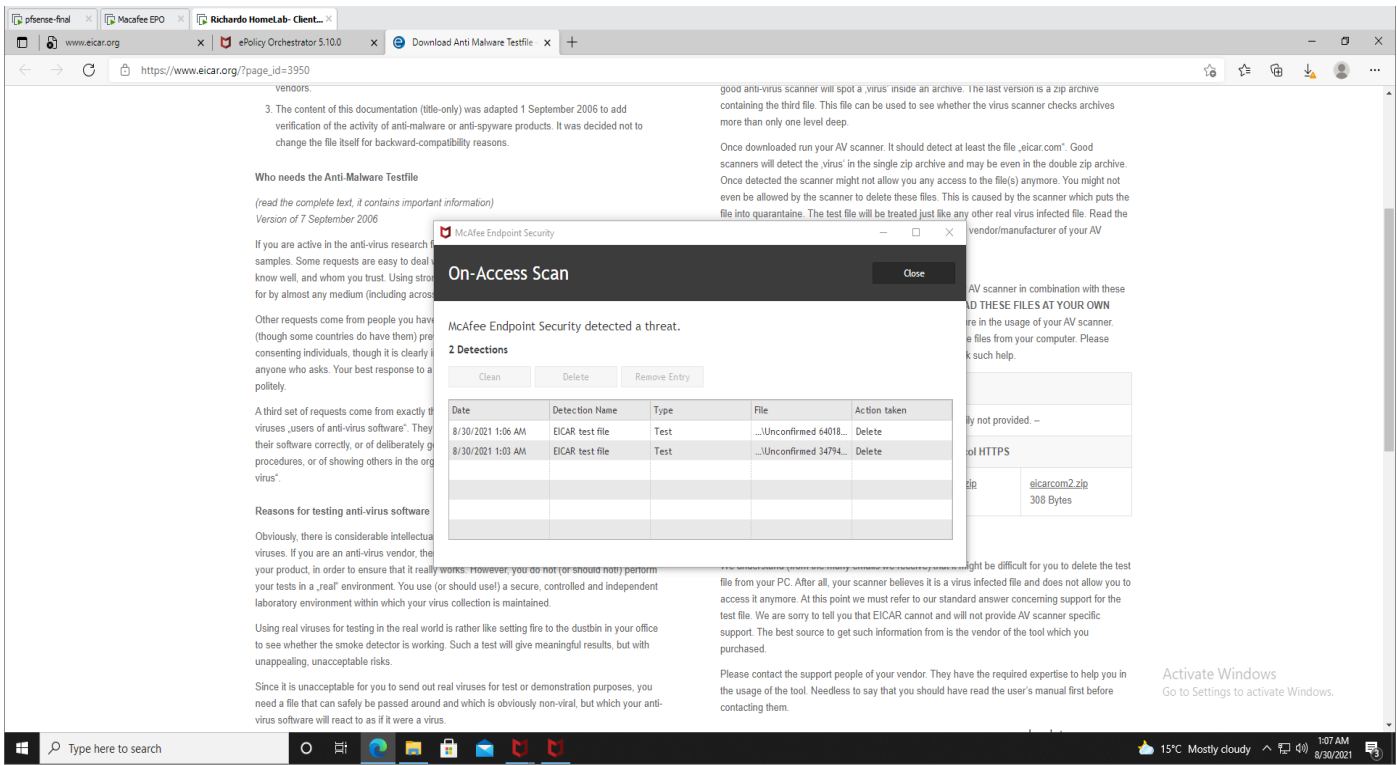
# Macafee Endpoints

Visited a malicious website, and attempts to download a malicious file. On-Access Scan policy is being deployed to the endpoints, hence it was able to detect that the file was malicious and was able

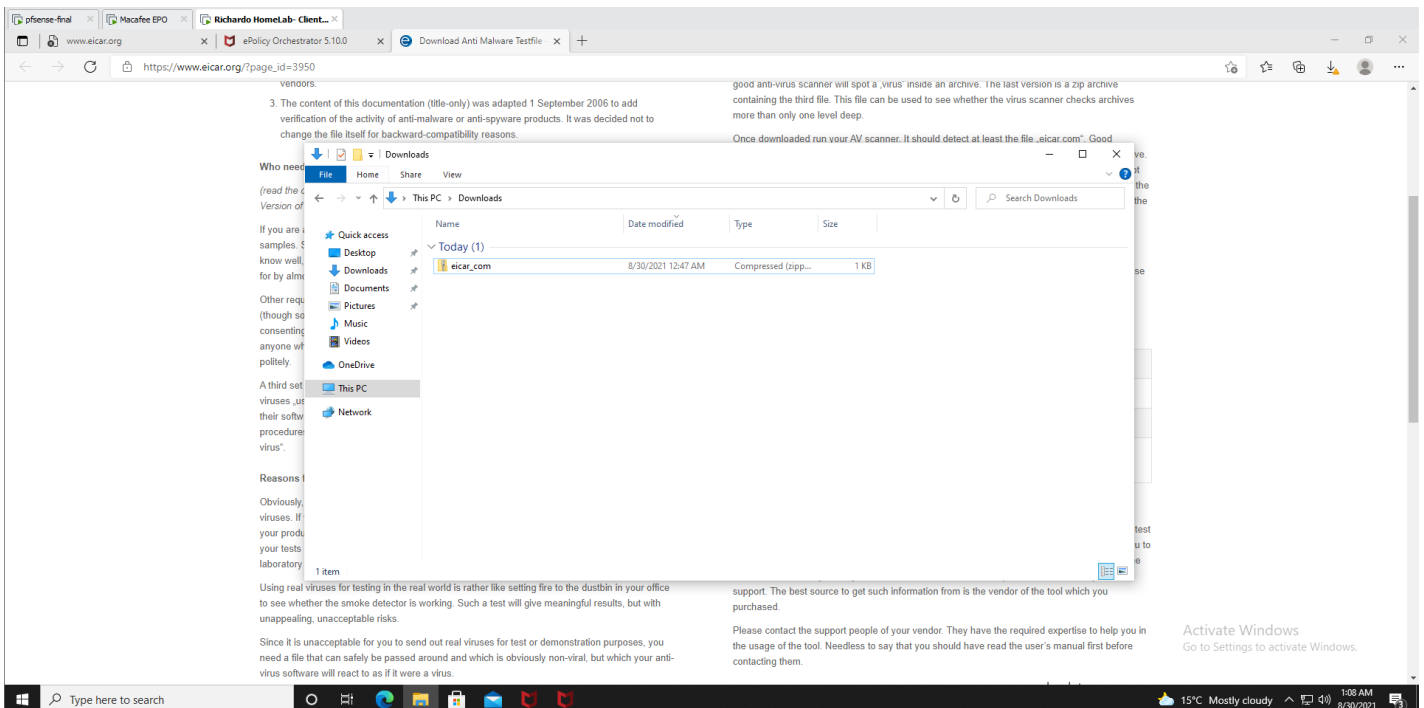


*Scheduling an-demand Scan using Macafee on my Endpoint. A full scan will be scheduled to be conducted at 8:30 am every week.*

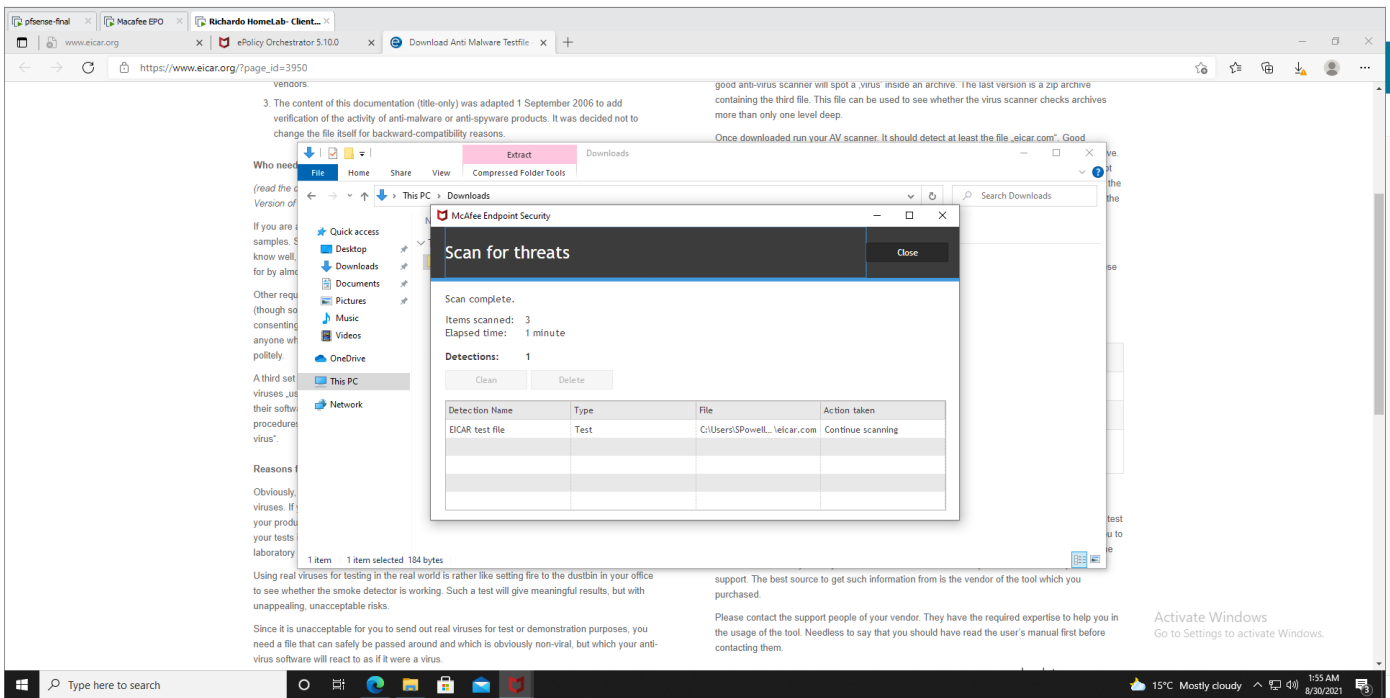
# Macafee Endpoints



*The Macafee Endpoint detected a downloaded malicious file and taken action to delete it.*

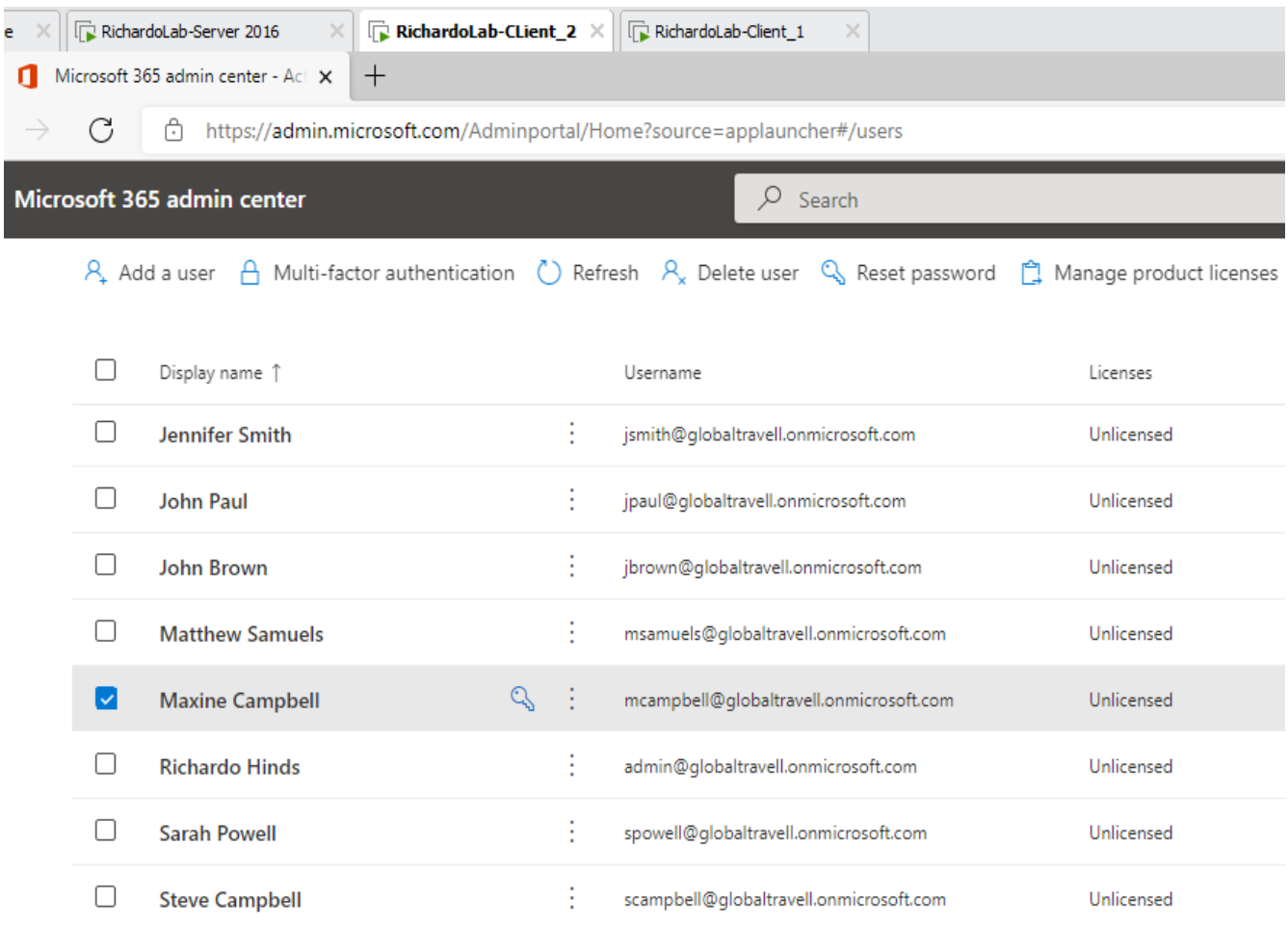


*A folder was copied to an endpoint*



*Macafee Endpoint protection was able to flag the above folder as threat.*

## Microsoft 365



# Software Inventory Using Spiceworks

The screenshot shows the Spiceworks Software Inventory page. The browser tabs include 'RichardLab-Server 2016', 'RichardLab-Client\_2', 'Macafee EPO', 'RichardLab-Client\_1', and 'RichardLab-pfense'. The URL is https://apps.spiceworks.com/tools/device-inventory/software. The page title is 'All Software (46)'. The table lists software items with columns for Name, Publisher, and Detected On. The detected on dates range from 4 to 13 days ago. The interface includes a search bar, navigation tabs, and a sidebar with utility links.

| Name   | Publisher             | Detected On |
|--|-----------------------|-------------|
| Agent Shell  | Spiceworks            | 4           |
| Browser for SQL Server 2017                        | Microsoft Corporation | 1           |
| Google Chrome                                      | Google LLC            | 1           |
| McAfee ePolicy Orchestrator                        | McAfee LLC.           | 1           |
| McAfee ePolicy Orchestrator 5.10.0                 |                       | 1           |
| Microsoft 365 Apps for business - en-us            | Microsoft Corporation | 1           |
| Microsoft Edge                                     | Microsoft Corporation | 1           |
| Microsoft Edge Update                              |                       | 1           |
| Microsoft ODBC Driver 13 for SQL Server            | Microsoft Corporation | 1           |
| Microsoft OneDrive                                 | Microsoft Corporation | 1           |
| Microsoft SQL Server 2012 Express LocalDB          | Microsoft Corporation | 1           |
| Microsoft SQL Server 2012 Management Objects (x64) | Microsoft Corporation | 1           |
| Microsoft SQL Server 2012 Native Client            | Microsoft Corporation | 1           |
| Microsoft SQL Server 2017 (64-bit)                 |                       | 1           |
| Microsoft SQL Server 2017 RsFX Driver              | Microsoft Corporation | 1           |
| Microsoft SQL Server 2017 Setup (English)          | Microsoft Corporation | 1           |

|  |                           |   |
|--|---------------------------|---|
| Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.20.27508    | Microsoft Corporation     | 3 |
| Microsoft Visual C++ 2019 X86 Additional Runtime - 14.20.27508 | Microsoft Corporation     | 3 |
| Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.20.27508    | Microsoft Corporation     | 3 |
| Microsoft VSS Writer for SQL Server 2017                       | Microsoft Corporation     | 1 |
| Mozilla Firefox (x64 en-CA)                                    | Mozilla                   | 1 |
| Mozilla Maintenance Service                                    | Mozilla                   | 1 |
| SQL Server 2017 Batch Parser                                   | Microsoft Corporation     | 1 |
| SQL Server 2017 Common Files                                   | Microsoft Corporation     | 1 |
| SQL Server 2017 Connection Info                                | Microsoft Corporation     | 1 |
| SQL Server 2017 Database Engine Services                       | Microsoft Corporation     | 1 |
| SQL Server 2017 Database Engine Shared                         | Microsoft Corporation     | 1 |
| SQL Server 2017 DMF  | Microsoft Corporation     | 1 |
| SQL Server 2017 Shared Management Objects                      | Microsoft Corporation     | 1 |
| SQL Server 2017 Shared Management Objects Extensions           | Microsoft Corporation     | 1 |
| SQL Server 2017 SQL Diagnostics                                | Microsoft Corporation     | 1 |
| SQL Server 2017 XEvent   | Microsoft Corporation     | 1 |
| Veeam Agent for Microsoft Windows                              | Veeam Software Group GmbH | 1 |
| VMware Tools   | VMware, Inc.              | 3 |



# Inventory Management - Spiceworks

The screenshot shows the Spiceworks web interface for Device Inventory. The main table lists 5 devices:

| Device Name    | Last Check-in | Name           | IP Addresses           | MAC Addresses     | Data Source      | OS                  | Device Type | Intel vPro |
|----------------|---------------|----------------|------------------------|-------------------|------------------|---------------------|-------------|------------|
| client1        | 4d ago        | client1        | 192.168.1.31.fe80::... | 00:0C:29:76:CB:E5 | Collection Agent | Microsoft Window... | Desktop     | Unknown    |
| client2        | 5d ago        | client2        | 192.168.1.32.fe80::... | 00:0C:29:C7:2B:0F | Collection Agent | Microsoft Window... | Desktop     | Unknown    |
| macafee        | 4d ago        | macafee        | 192.168.1.33.fe80::... | 00:0C:29:4B:1D:D9 | Collection Agent | Microsoft Window... | Server      | Unknown    |
| PFsense        | N/A           | PFsense        | 192.168.1.1            |                   | Manual Entry     | Linux               | Firewall    | Unknown    |
| windows-server | 5d ago        | windows-server | 192.168.1.30           | 00:0C:29:99:BC:45 | Collection Agent | Microsoft Window... | Server      | Unknown    |

## VPN – Remote Access

The screenshot shows the SoftEther VPN Server Manager interface. The 'Manage VPN Server' window for 192.168.159.175 is open, displaying a table of Virtual Hubs and various configuration options.

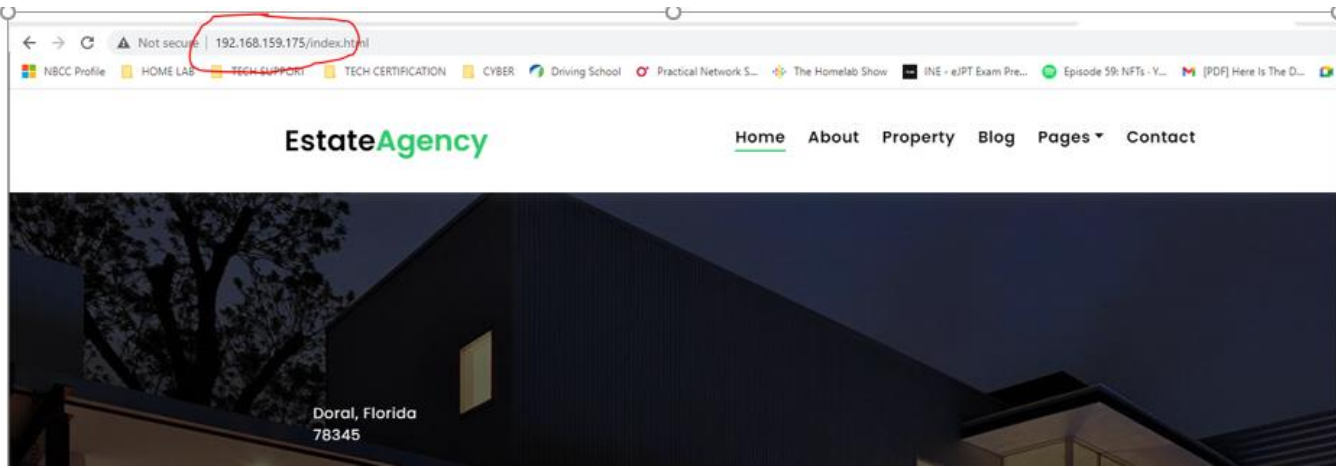
| Virtual Hub Name | Status | Type       | Users | Groups | Sessions | MAC Tables | IP Tables |
|------------------|--------|------------|-------|--------|----------|------------|-----------|
| VPN              | Online | Standalone | 2     | 0      | 0        | 0          | 0         |

The screenshot shows the SoftEther VPN Client Manager interface. The table below shows the status of VPN connections:

| VPN Connection Setting Name | Status    | VPN Server Hostname                   | Virtual Hub | Virtual Network A... |
|-----------------------------|-----------|---------------------------------------|-------------|----------------------|
| Add VPN Connection          |           |                                       |             |                      |
| Remote Connect              | Connected | 192.168.159.175 (Direct TCP/IP Con... | VPN         | VPN                  |

*Setup and configured Ethersoft VPN for remote access to the network. As a result, network resources can be shared to only users that the VPN Server will have to authenticate.*





*End user can access internal website when connected to VPN*

## Hosting Website on IIS Manager

Internet Information Services (IIS) Manager

Server Manager Dashboard

Local Servers

Internet Information Services (IIS) Manager

REMOTEAACCESS Home

Filter: Go Show All Group by: Area

Authentic... Compression Default Document Directory Browsing Error Pages Handler Mappings HTTP Respon... Logging MIME Types

Modules Output Request Server Worker Caching Filtering Certificate Processes

Actions

Manage Server

- Restart
- Start
- Stop
- View Application Pools
- View Sites
- Get New Web Platform Components
- Help

192.168.159.175/index.html

EstateAgency

Home About Property Blog Pages Contact

Doral, Florida 78345

**204 ALIRA  
ROAN ROAD ONE**