**[/Users/detaylor/Library/Containers/com.microsoft.Outlook/Data/Library/Caches/Signatures/signature_1862348092](https://f5.com/we-make-apps-go?utm_source=WMAGSIG/)**

Microsoft Server 2012 CIFS File Share

Web CIFS Portal Access on APM Webtop v13.0

**Produced by:**

Dean Taylor                           F5 Senior System Engineer

**Dated 10/07/17**

Table of Contents

[Introduction 3](#_Toc489959713)

[Microsoft Server 2012 File Share Setup 3](#_Toc489959714)

[Pre-requisites 3](#_Toc489959715)

[Microsoft Server 2012 RDS Server Setup 3](#_Toc489959716)

[F5 BIG-IP LTM & APM Configuration 6](#_Toc489959717)

[Access Profile 8](#_Toc489959718)

[Screenshot of Web CIFS Access 9](#_Toc489959719)

[Potential Issues 9](#_Toc489959720)

# Introduction

This document details publishing a browser based CIFS file share on the APM webtop. Access policies are APM Webtop access. However, direct access to the file share via. a browser is possible by entering authentication parameter details in the browser URI along with the path to the backend file share.

This document covers a Web CIFS Portal Access on APM webtop and F5 BIG-IP APM policy configuration.

# Microsoft Server 2012 File Share Setup

## Pre-requisites

1. Ensure that the server is separate to a pre-built Domain Controller / DNS Server 2012 server.
2. Join the server to the domain.
3. Ensure you have a domain user added into local users as administrator.
4. Ensure you are logged on with this account (f5demo.com\user would be fine) as this is a pre-requisite enabling sharing on the file share directory.

## Microsoft Server 2012 RDS Server Setup

1. Open Windows Explorer and select a folder to share, i.e. c:\users\user\desktop.
2. Select the folder properties and ensure you select ‘Advanced Sharing’. This will ensure a short path is created as per. screen shot:



1. Click on the checkbox for ‘Share this folder’ and then click on Permissions:



1. In Permissions, you can select individual users or ‘everyone’. Make sure you select correct controls for read-only etc.:



# F5 BIG-IP LTM & APM Configuration

1. Deploy VE with LTM + APM licensed on v13.
2. Create following objects for APM policy:
   1. AAA AD object with admin rights for Authentication.
   2. Portal Access object for the file share
   3. Create a Full webtop
3. Create Portal Access object with the correct hostname / IP address and path for the file share:



\*path will be something like this:

?domain=WIN4I7SB5HV350&sharename=Desktop&winhost=10.1.20.35&user=%{session.sso.token.last.username}&pass=%{session.sso.token.last.password}



1. Create a Forms SSO profile:



\*Form Action will be something like:

[http://10.1.10.55/?domain=WIN4I7SB5HV350&sharename=Desktop&winhost=10.1.20.35&user=%{session.sso.token.last.username}&pass=%{session.sso.token.last.password}](http://10.1.10.55/?domain=WIN4I7SB5HV350&sharename=Desktop&winhost=10.1.20.35&user=%25%7bsession.sso.token.last.username%7d&pass=%25%7bsession.sso.token.last.password%7d)

\*Make sure you add / in Start URI

1. Go to iRulesLX under Local Traffic Manager -> iRules -> iRulesLX and import the webcifs LX Workspace from Hive post here.
2. If required, create iRulesLX plugin from the workspace.
3. Create iRuilesLX profile with iRulesLX Workspace selected in dropdown.
4. Create simple iRule for referencing the Web CIFS TCP only Vietual from the Access Policy Virtual:

# This irule links the RDS virtual to the webcifs virtual.

when HTTP\_REQUEST {

virtual Web\_CIFS

}

1. Standard Connectivity profile from parent Connectivity profile.
2. Client SSL profile.
3. Create Virtual Server for Web CIFS Access with following properties:

* Destination address
* HTTP as service
* Default TCP Profile
* Pre-configured iRulesLX profile
* SNAT Automap

1. Create Virtual Server for Access Policy with the following properties:

* Destination address
* HTTPS as service
* Default TCP Profile
* Default HTTP Profile
* Client SSL profile
* SNAT Automap
* Predefined Rewrite profile
* Predefined Access Profile (screenshot below)
* Connectivity profile
* Predefined iRule for referencing Web CIFS Virtual

## Access Profile

This section details the main access profile policy configuration. Here are the required steps:

1. Create an All type of profile.
2. Add a Logon Page with default properties.
3. Add an AD Auth object with the pre-configured AD AAA.
4. Add in an Advanced Resource Assign object and add pre-configured webtop & Web CIFS Portal Access.

# Screenshot of Web CIFS Access



# Potential Issues

* User parameters appear in the clear within the URI field when you access the Portal Access.
* Cannot delete files from the Web CIFS screen.
* iRules LX are unsupported.