RM Broadband
SSL Connect

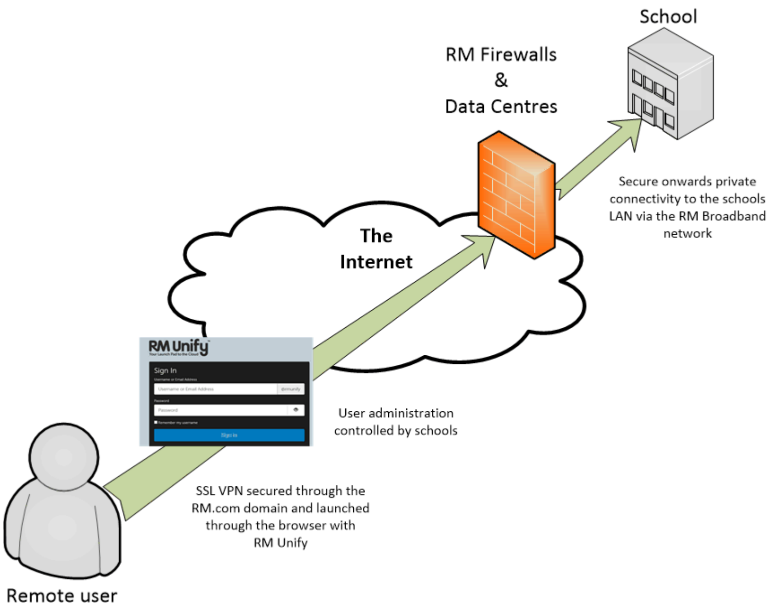
SSL Connect Admin guide

Contents

Introduction

SSL Connect for RM Broadband is an SSL VPN service that lets school staff securely access the school network from anywhere, giving them the same access to the school network as they would get from a computer in the school connected by wifi or a cable.

SSL Connect is based on BIG-IP Edge software from F5 Networks. It is accessed through RM Unify.


School
RM Firewalls
&
Data Centres
Secure onwards private connectivity to the schools LAN via the RM Broadband network
The Internet
RM Unify
Sign In
Sign In
User administration controlled by schools
SSL VPN secured through the RM.com domain and launched through the browser with RM Unify
Remote user

The advantage of this central service is that the school doesn’t need to host any software in the school. The only essential set-up tasks are to configure RM Unify to synchronise user accounts and install software on computers as required.

This guide describes how to set up your network for SSL Connect and install the required client software; how it can be used; and how to resolve or report any problems you may encounter.

SSL Connect licensing

SSL Connect is licensed by the number of concurrent users.

If you buy 10 user licenses you can allocate it to all of your teaching staff, but only 10 of them will be able to use it at the same time. When an 11th staff member tries to connect, they won’t be successfully authenticated and will see their status as Disconnected (see page 17 in the ‘Appendix II: Troubleshooting’ section).

If SSL Connect is part of your plan for operating the school when the building is closed due to snow or other unexpected adverse events, we recommend that you license it for the number of staff who will need to use it on that day.

Set up RM Unify

In this guide we assume that you've purchased the service already and our delivery team have configured your network to allow remote access. (Please allow several days for us to configure access after you order the service.)

The school needs to:

- Set up an RM Unify Establishment
- Create user accounts for SSL Connect in RM Unify.

If you are already using RM Unify – for example, for RM SafetyNet User Based Filtering or access to Office 365 or GoogleApps – the required user accounts will probably be already set up.

If you're not already using RM Unify, then it's simple to get RM Unify Basic set up and configured and use that to create users for the VPN Service from an uploaded CSV file. (Alternatively, if you want to create and maintain accounts automatically by integration with the school network's Active Directory, get RM Unify Basic Plus or RM Unify Premium.) You can request an RM Unify demo here; instructions for setting up user accounts are provided in the *RM Unify Quick Start Guide*.

RM Unify: choosing Basic, Basic Plus or Premium

SSL Connect will work on RM Unify Basic, in which case you don't need to install any software on the LAN.

However, if you're considering using RM SafetyNet User Based Filtering or accessing Office 365 or Google Apps in the future, we strongly recommend that you consider installing AD Sync to manage your users. AD Sync is a feature of RM Unify Basic Plus (free) and RM Unify Premium.

If you want to use RM Unify Basic now but think you may use these services later, we recommend that you use our free CSV Extraction Tool to provision user accounts into RM Unify, to avoid creating duplicate accounts and ensure that users will be able to use their school network usernames later. You can get the CSV Extraction Tool here (Knowledge Library article DWN3182515, available at the RM Support website).

Allocate SSL Connect to users

SSL Connect is an RM Unify application. In RM Unify, applications are allocated by user roles (Student, Teaching Staff, Non Teaching Staff, Governor, Other). An RM Unify Administrator can install the SSL Connect app for users with a specified RM Unify role, and add the SSL Connect tile to the shared Launch Pad for that role to make it available.

Fine-tuning access by role

You may not want all the users in a given role to use SSL Connect. Suppose you have many Teaching Staff users, but you only want some of them to have remote access. In this situation you may have several options:

- *Reassign SSL Connect users to the 'Other' role.*

  You could move a subset of staff from their current role to the Other role, and allocate SSL Connect only to the Other role. The limitation of this solution is that these users may find that some third-party RM Unify applications can't be installed to the Other role, so there are some things they won't be able to do. However, if you only use RM Unify for SSL Connect and RM Safety Net User Based Filtering, this approach may work for you.

- *Don't add the SSL Connect tile to shared Launch Pads.*

  If you have RM Unify Premium, you can tell selected users to add the SSL Connect tile from the App Library to their personal Launch Pad. Alternatively you could simply give selected users the SSL Connect URL so they can access it directly, without using the Launch Pad (see next section).

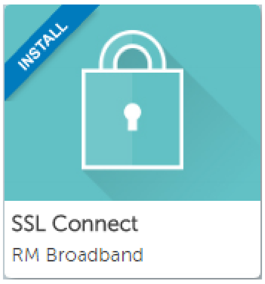
Note Access control is granted by the installed role. If you install SSL Connect for the Staff role and only give the URL details to the Senior Management Team, other Staff users in RM Unify could still start a session if they knew the URL.

Installing and allocating SSL Connect in RM Unify

For these instructions we assume you have already purchased the SSL Connect app.

1. Log on to RM Unify as an RM Unify Administrator.

2. From the top menu choose App Library. Locate and select the **SSL Connect** tile.



3. An information page for the app is displayed. Click **Install**.
   The Install window is displayed.

4. Under ‘Which roles should SSL Connect be installed to?’, tick the appropriate boxes to allocate SSL Connect to the required user roles.

5. Under ‘And which Launch Pads should SSL Connect appear on?’, tick the boxes for any shared Launch Pads that should include the SSL Connect tile.

Notes

If you aren’t yet ready to give users access to SSL Connect on their Launch Pads, you can leave the Launch Pad boxes blank for now and return to them later.

If you want to give selected users the SSL Connect URL instead of providing a Launch Pad tile, copy and share the ‘URL’ text link on this page.

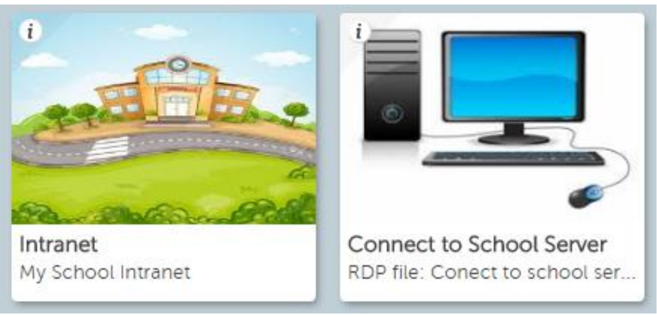
See also ‘SSL Connect licensing’ on page 2.

6. Click **Save**.

7. Close the Install window.

Publishing link tiles for SSL Connect

RM Unify Administrators can publish link tiles on shared Launch Pads, to point to anything that can be accessed by a browser. This is a convenient way to give users easy access to the applications they will be using with SSL Connect.

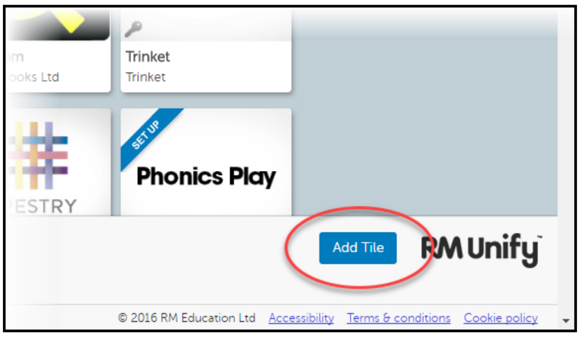


Note that RM Unify is only making the applications easy to find: access control is done using SSL Connect.

Instructions for adding a link tile to a website are given below.
See also ‘Appendix I: Creating a tile for an RDP connection’.

To add a link tile for a website

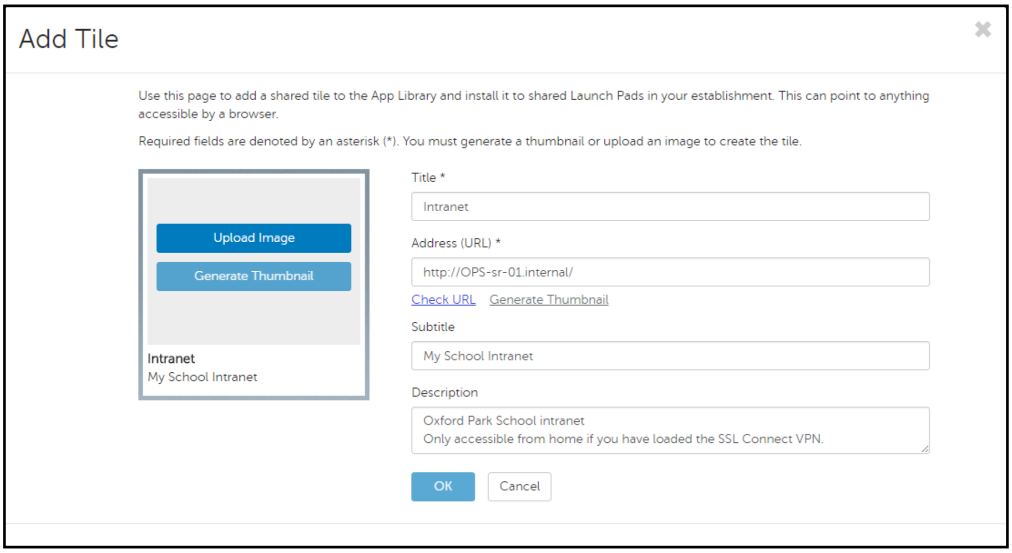
1. Log on to RM Unify as an RM Unify Administrator.
2. From the top menu choose **App Library**.
3. Click **Add Tile**.



An Add Tile window is displayed.

Note The number of tiles that can be created is limited to 5 unless you have RM Unify Premium. Premium also allows you to use per user Launch Pads

http://www.rm.com/products/rm-unify/main-page-contents/pricing-and-subscriptions-plans



Add Tile

Use this page to add a shared tile to the App Library and install it to shared Launch Pads in your establishment. This can point to anything accessible by a browser.

Required fields are denoted by an asterisk (*). You must generate a thumbnail or upload an image to create the tile.

Title *: Intranet

Address (URL) *: http://OPS-sr-01.internal/

Subtitle: My School Intranet

Description: Oxford Park School intranet
Only accessible from home if you have loaded the SSL Connect VPN.

4. Enter a suitable **Title**, **Subtitle** and **Description** for this link.

5. Enter the **Address (URL)** for this link.
The server name to enter will depend on what instructions you gave RM for setting up your SSL Connect VPN:

   - If you specified the search suffix and DNS servers to use, enter the fully qualified domain name for the server (e.g., http://OPS-sr-01.internal)

   - If you chose not to set up DNS, use the private IP address for the server name (e.g., http://10.0.1.1)

6. Click **Upload Image**. Locate and select a suitable image for the tile. It must not exceed 50 KB and can be a PNG, JPEG or GIF file.

   Note You can only use an uploaded image, as the Generate Thumbnail option will not work with SSL Connect.

   Click **Upload**. An Install window is displayed.

7. Under 'Which roles should SSL Connect be installed to?', tick the appropriate boxes to allocate SSL Connect to the required user roles.

8. Under 'And which Launch Pads should SSL Connect appear on?', tick the boxes for any shared Launch Pads that should include the SSL Connect tile.

   Note Including a link tile on a Launch Pad does not give remote access to the resource unless the user is running SSL Connect. For example, an Intranet tile on a shared Teaching Staff Launch Pad will give intranet access in the school to all teachers, but only those teachers who are using SSL Connect will be able to use it to access the intranet from home.

9. Click **Save**.

10. Close the Install window.

Installing the client software on computers

SSL Connect uses a third-party software product from F5 Networks which can be installed on a client computer to connect to the VPN.

There are two installation options:

- MSI installation (recommended)

  This is the most practical option, particularly for centrally managed computers where end users don't have admin rights to install software.

- Browser based plugin installation (not recommended)

  If the MSI hasn't been installed on a computer, the first time an end user tries to use SSL Connect, they will be prompted to install a browser plugin. F5 Networks have made plugins available for some but not all browsers. Admin rights on the computer are required to do this.

  You may find that the plugin for Internet Explorer installs without problems. However the MSI installation is easier and more reliable, and will result in fewer prompt messages after installation. Therefore we recommend the MSI installation, even on home computers.

  Instructions for the Internet Explorer plugin installation are given in 'Appendix III: Installing the F5 plugin via Internet Explorer'.

For more information about the F5 browser plugins, see 'Appendix IV: Notes on other browsers'..

Installing the MSI software

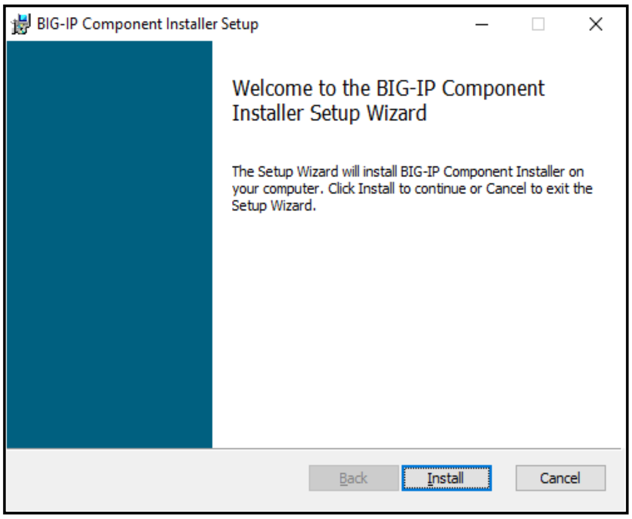
This option uses an Edge Client MSI produced by F5 Networks, which installs browser plugins for supported browsers. You can install it manually on each computer, or create a package to deploy over the network. The MSI option will present the user with fewer security prompts when they connect.

1. Download the pre-configured **BIGIPComponentInstaller.msi** file from Knowledge Library article DWN5306849 on the RM Support website.

2. If you want to create a package for unattended deployment, follow the instructions given by F5 here: https://support.f5.com/kb/en-us/solutions/public/13000/700/sol13710.html

   Note If you have downloaded the MSI from the location specified in step 1, the components to install are already configured, so you can ignore the 'ADDLOCAL' instructions after step 5.

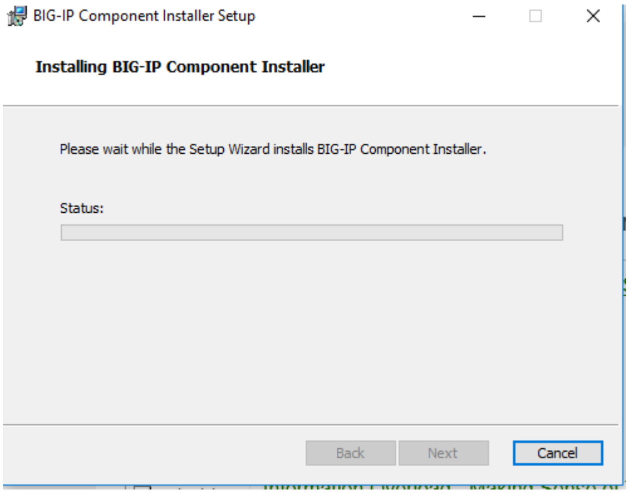
3. To install manually, log on to the computer as a user with administrative rights and double-click the **BIGIPComponentInstaller.msi** file.



BIG-IP Component Installer Setup

Welcome to the BIG-IP Component Installer Setup Wizard

The Setup Wizard will install BIG-IP Component Installer on your computer. Click Install to continue or Cancel to exit the Setup Wizard.



BIG-IP Component Installer Setup

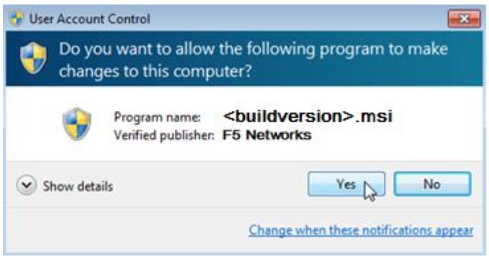
Installing BIG-IP Component Installer

Please wait while the Setup Wizard installs BIG-IP Component Installer.

Status:

4. Click **Install**, and click **Yes** at the UAC prompt.

Note The style of the UAC dialogue below depends on the version and build of Windows.



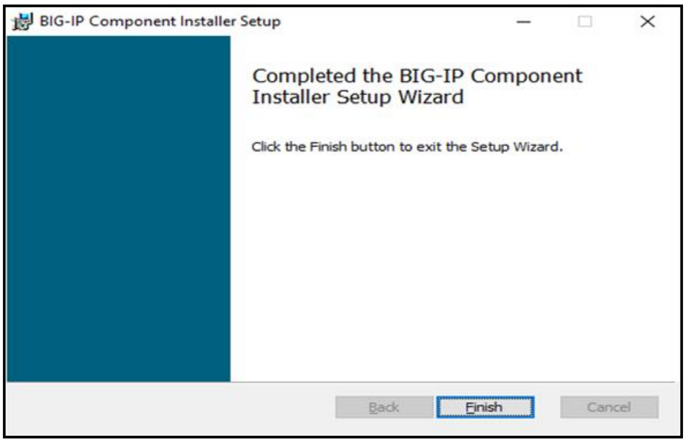
User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: <buildversion>.msi
Verified publisher: F5 Networks

(where <buildversion> will be a string of characters such as ce6f1b)

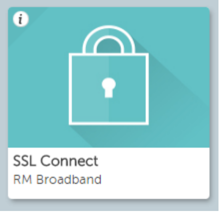
5. Click **Finish**.



Completed the BIG-IP Component Installer Setup Wizard

Click the Finish button to exit the Setup Wizard.

6. When the MSI has been installed, use Internet Explorer to log on to RM Unify and click the SSL Connect tile to connect to the school network.



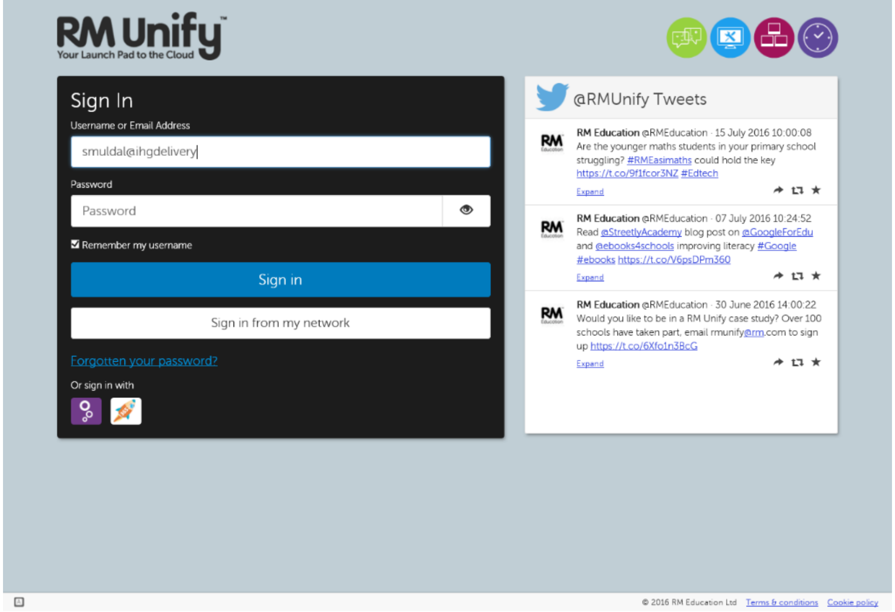
Connecting with SSL Connect

Once the F5 browser plugin has been installed, the user connects to the school network as follows:

(note for non Windows platform please see Appendix IV)

1. At the laptop, open the browser.

2. Browse to your RM Unify website, enter your usual RM Unify username and password and click **Sign in**.



Sign In

Username or Email Address

smuldal@ihgdelivery

Password

Password

☑ Remember my username

@RMUnify Tweets

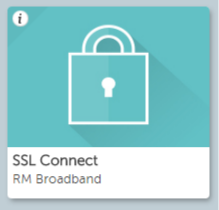
RM Education @RMEducation · 15 July 2016 10:00:08
Are the younger maths students in your primary school struggling? #RMEasimaths could hold the key https://t.co/9f1fcor3NZ #Edtech
Expand

RM Education @RMEducation · 07 July 2016 10:24:52
Read @StreetlyAcademy blog post on @GoogleForEdu and @ebooks4schools improving literacy #Google #ebooks https://t.co/V6psDPm360
Expand

RM Education @RMEducation · 30 June 2016 14:00:22
Would you like to be in a RM Unify case study? Over 100 schools have taken part, email rmunify@rm.com to sign up https://t.co/6Xfo1n3BcG
Expand

© 2016 RM Education Ltd Terms & conditions Cookie policy

3. To launch SSL Connect, either by click the **SSL Connect** tile on a shared Launch Pad or enter the URL address for SSL Connect.

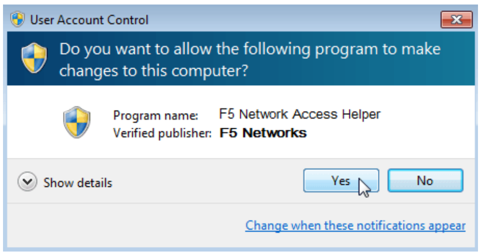


If the SSL Connect tile hasn't been added to the shared Launch Pad, you may be allowed to add it from the App Library to your personal Launch Pad (for instructions, see the *RM Unify Quick Start guide* or *RM Unify: A guide for school staff*).

4. The F5 Virtual Webtop is displayed and the connection starts automatically if pop ups are allowed and the MSI has been installed.

4.1 Internet Explorer:

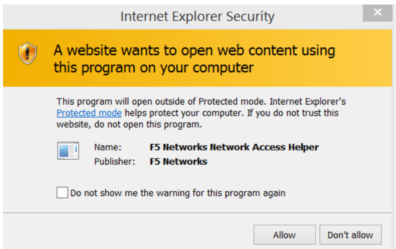
You may need to grant access to the F5 Network Access Helper, by clicking **Yes** one or more times in the User Account Control and Internet Explorer Security pop-ups:



Do you want to allow the following program to make changes to this computer?

Program name: F5 Network Access Helper
Verified publisher: **F5 Networks**

Change when these notifications appear



A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

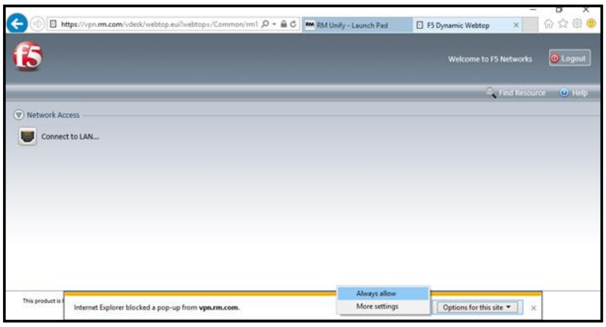
Name: **F5 Networks Network Access Helper**
Publisher: **F5 Networks**

□ Do not show me the warning for this program again

No extra security prompts are required to start the session, but if a popup blocker is enabled for the user, they will need to allow **vpn.rm.com**.

If pop ups aren't allowed then you'll see the following:

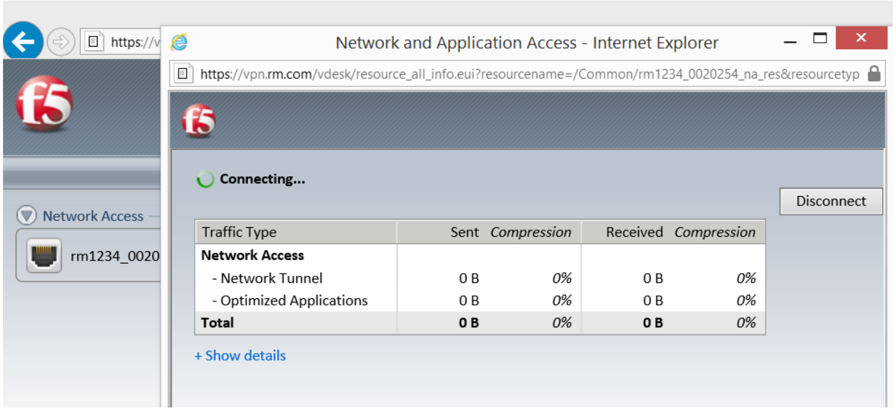
If the computers are centrally managed, this can be pushed out via GPO.



Internet Explorer blocked a pop-up from **vpn.rm.com**.

Note If you click on 'Connect to LAN…' , the pop-up 'Network and Application Access' window will launch even if pop-ups are disabled.

Once the pop up loads you'll see the connection window:


Network and Application Access - Internet Explorer
https://vpn.rm.com/vdesk/resource_all_info.eui?resourcename=/Common/rm1234_0020254_na_res&resourcetyp
Network Access
rm1234_0020
Disconnect
+ Show details

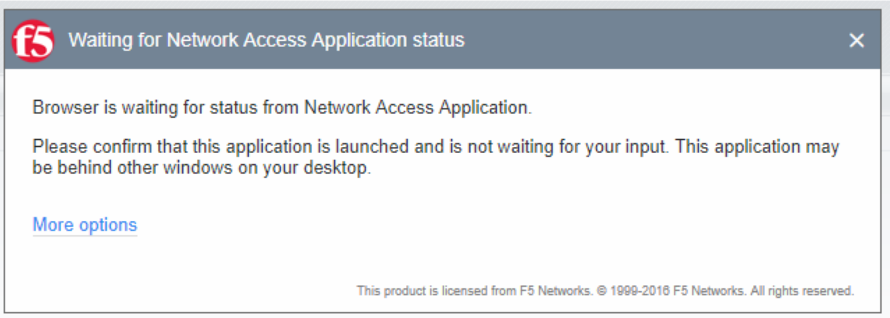
Connecting...

Traffic Type	Sent	Compression	Received	Compression
Network Access				
- Network Tunnel	0 B	0%	0 B	0%
- Optimized Applications	0 B	0%	0 B	0%
Total	**0 B**	0%	**0 B**	0%

5.2 Other Browsers:

F5 support a more modern API on Edge Chrome & Firefox and so the User Experence is slightly different:

(note the screensots below assume you've installed the MSI as above, if you havent' the browser will attempt to install the plugin as per Adendix IV. We recommend using the MSI to streamline the installation.)



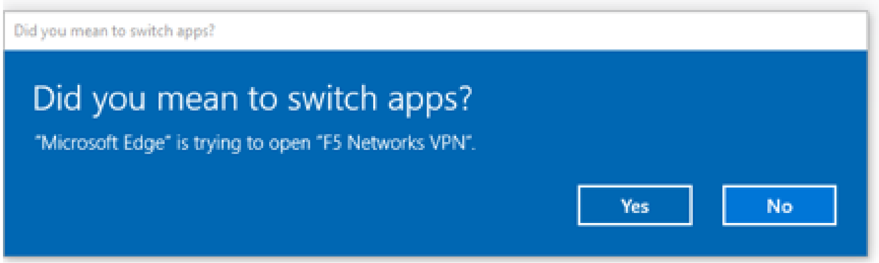
Waiting for Network Access Application status

Browser is waiting for status from Network Access Application.

Please confirm that this application is launched and is not waiting for your input. This application may be behind other windows on your desktop.

This product is licensed from F5 Networks. © 1999-2016 F5 Networks. All rights reserved.

Edge:

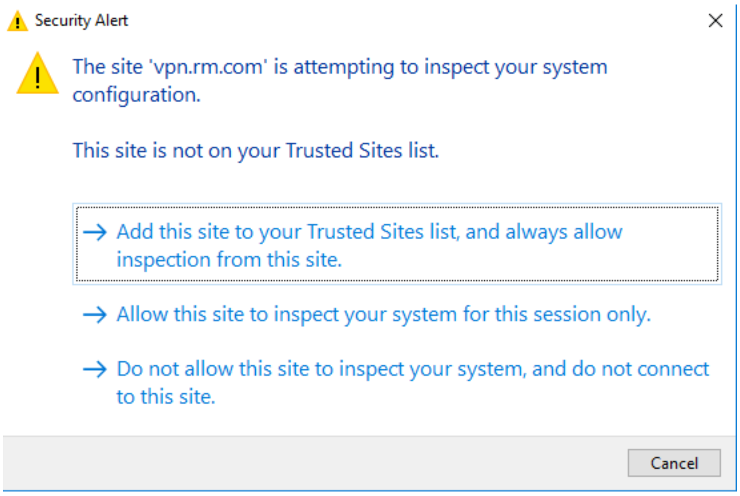


Did you mean to switch apps?

Did you mean to switch apps?

"Microsoft Edge" is trying to open "F5 Networks VPN".

You will be reqested to add vpn.rm.com to your trusted sites to enable system inspection



Security Alert

The site 'vpn.rm.com' is attempting to inspect your system configuration.

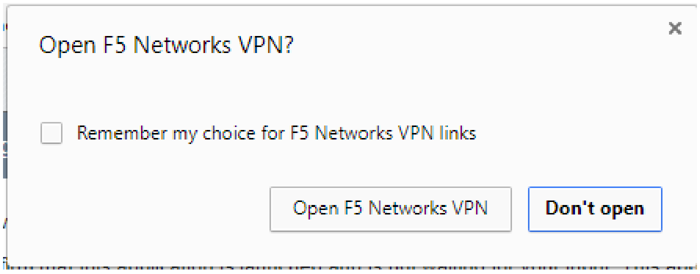
This site is not on your Trusted Sites list.

→ Add this site to your Trusted Sites list, and always allow inspection from this site.

→ Allow this site to inspect your system for this session only.

→ Do not allow this site to inspect your system, and do not connect to this site.

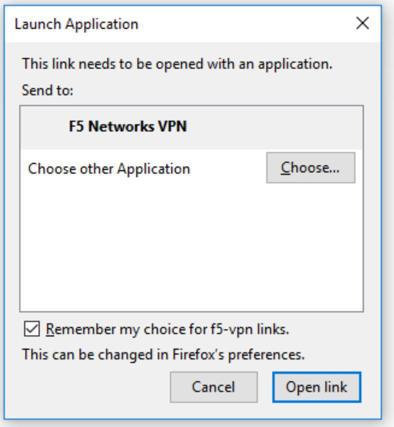
Chrome:



Open F5 Networks VPN?

□ Remember my choice for F5 Networks VPN links

Firefox:



Launch Application

This link needs to be opened with an application.

Send to:

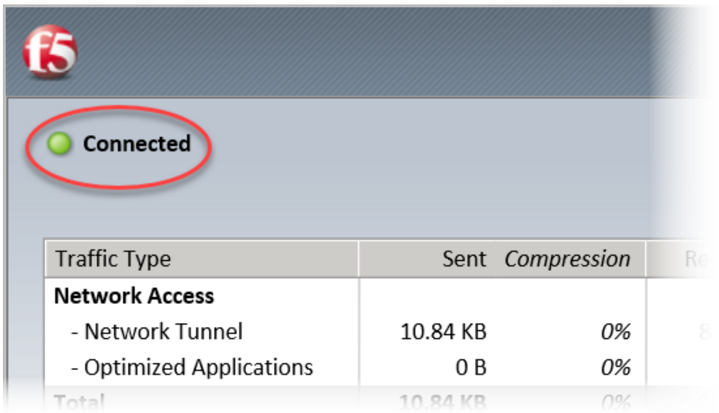
F5 Networks VPN

Choose other Application

☑ Remember my choice for f5-vpn links.

This can be changed in Firefox's preferences.

5. Look for the ‘Connected’ status indicator.



● Connected

Traffic Type	Sent	Compression	Re
Network Access			
- Network Tunnel	10.84 KB	*0%*	8
- Optimized Applications	0 B	*0%*	
Total	10.84 KB	*0%*	

This shows that the VPN connection is now working.

Leave the two ‘F5’ browser windows open while you use the school network

If you have requested RDP sessions or mapped drives to start when you connect then you will be promped for secuitry credentials for these.

.

Using SSL Connect

What users can do

SSL Connect gives users access to all the programs, files, folders and servers they would normally have access to from a computer connected to the network by a wifi connection or cable. For example they could load files from a Windows server network share and access an Intranet server. Authorised users could RDP to a school server for administration and access SIMS.NET.

While a user is connected to the VPN, their default DNS server becomes the school's, so they can use DNS to connect to local resources as they would do from within the school.

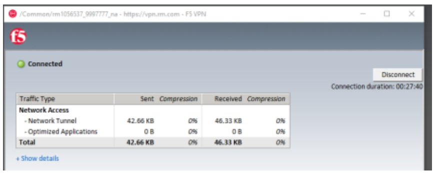
If your school has a local firewall this will still control access, and you can choose what access you grant to SSL Connect users by permitting the VPN IP pool in to selected parts of your network.

Note that traffic not destined for the school network will still go via the Internet. If your network has access to LAN resources in a partner school via a site-to-site VPN or IP connection, these won't be available via the SSL VPN. While users are connected to the VPN, their access to Internet sites is not sent via the school and is not subject to the school's network filtering.

Signing out

To ensure your school's security, and to free up a licence so that another user can connect, a user should always **log out from SSL Connect** when they have finished using the VPN, as follows:

Find the SSL Connect pop up window and select "Disconnect"



/Common/rm1056537_9997777_na - https://vpn.rm.com - F5 VPN

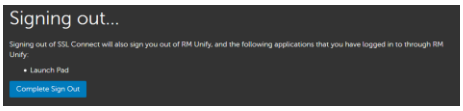
● Connected

Disconnect

Connection duration: 00:27:40

Traffic Type	Sent	Compression	Received	Compression
Network Access				
- Network Tunnel	42.66 KB	0%	46.33 KB	0%
- Optimized Applications	0 B	0%	0 B	0%
Total	42.66 KB	0%	46.33 KB	0%

This will then trigger a complete sign out from RM Unify



Signing out...

Signing out of SSL Connect will also sign you out of RM Unify, and the following applications that you have logged in to through RM Unify:

- Launch Pad

Note you can also sign out directly from RM Unify.

However this is unable to terminate the VPN session in Edge Chrome or Firefox. We recommend users to initiate Sign Out from the VPN rather than RM Unify.

2. If an F5 window prompts you to confirm that you want to close the connection, click **Yes**.

3. We recommend that you close all browser windows after logging out of RM Unify.

Security considerations

When you introduce remote access to the school network for your users, it becomes more important than ever to ensure that good security practices are followed. In this section we discuss some of the more important points, but this list is not exhaustive.

Passwords

If you're using AD Sync to synchronise your passwords with RM Unify, then your school password policy is key to ensuring that your passwords are strong enough. We recommend that all users of SSL Connect have strong passwords that are not shared or known to other people.

See https://xkcd.com/936/ for one simple way of making acceptable passwords.

Virus and malware protection, local firewalls and device updates

You should insist on the same level of protection for people accessing the network from home as you do for devices connected to your school LAN. Your security requirements for computers accessing school resources must be clearly set out in a school policy.

We recommend that users are only allowed to use the SSL Connect VPN from devices that are configured with antivirus software, a local firewall, and up-to-date OS patches. The good news is that the free Microsoft Windows versions of all of these are quite good and enabled by default in Windows.

Data encryption on the device

If users have the ability to copy school data onto home computers using the SSL Connect VPN, you should consider requiring users to have encryption on their computers. Windows 10 makes Bitlocker available for all users with modern hardware, so it's no longer expensive to require this. If you choose not to require encryption, you may want to introduce a policy of not allowing staff to download Personally Identifiable Information (PII) data onto home computers.

For a view from the UK's Information Commissioner's Office, see https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ and https://ico.org.uk/for-organisations/encryption/

End-to-end encryption

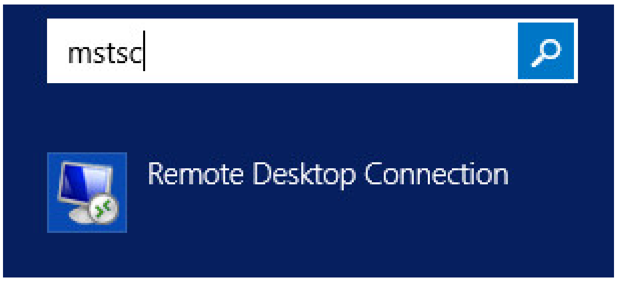
SSL Connect's VPN service will encrypt any data going from the connected device to RM's datacentre. This protects the traffic from eavesdroppers in the untrusted location you are connecting from. However we recommend that extra care is taken when connecting from public Wifi, to ensure that your password is only entered into RM Unify and that no SSL warnings are seen. The connection from RM's datacentre to your school is over our network and is secure but not encrypted. If you need full end-to-end encryption, we recommend using applications that provide encryption down to the server, for example installing SSL on the server you're connecting to.

Appendix I: Creating a tile for an RDP connection

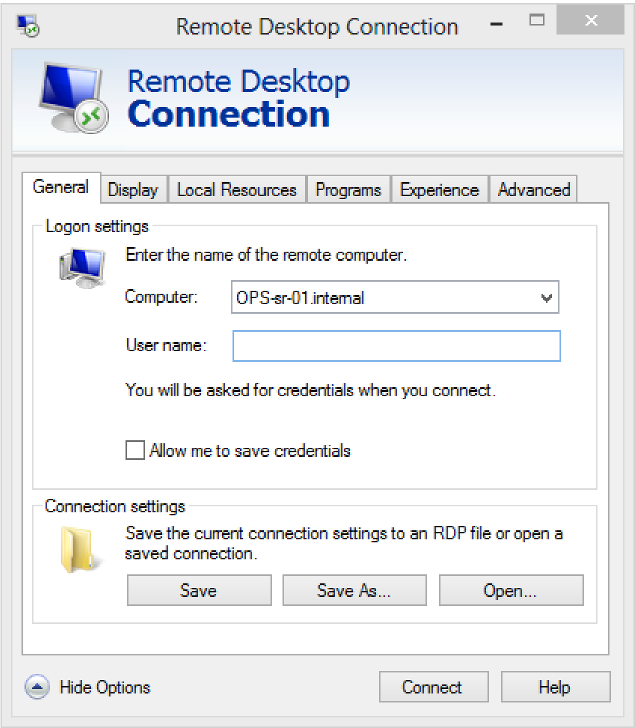
You may want selected staff to RDP to an admin computer or server, for example to run the SIMS application.

A good way to do this is to publish an RDP configuration file on a school webserver and then publish a link tile in RM Unify giving access to that file. To do this:

1. At a machine with access to the webserver where you want to make the RDP configuration file available, run **mstsc**.



The Remote Desktop Connection window is displayed.



Logon settings

Enter the name of the remote computer.

Computer: OPS-sr-01.internal

User name:

You will be asked for credentials when you connect.

□ Allow me to save credentials

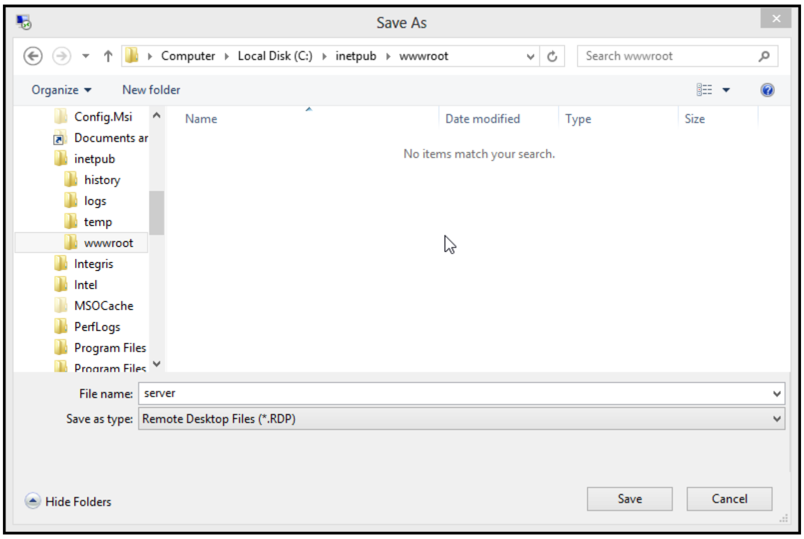
Connection settings

Save the current connection settings to an RDP file or open a saved connection.

2. Enter the details of the machine you want users to connect to. Do **not** enter a Username, as the RDP file will be shared.

3. Click Save As, and save the connection file to a webserver location where your servers can download it (e.g., on the Intranet server).

Note: The dialogue below assumes you want to use the default website on your webserver. You will have to determine the best place to serve the RDP file in the school.



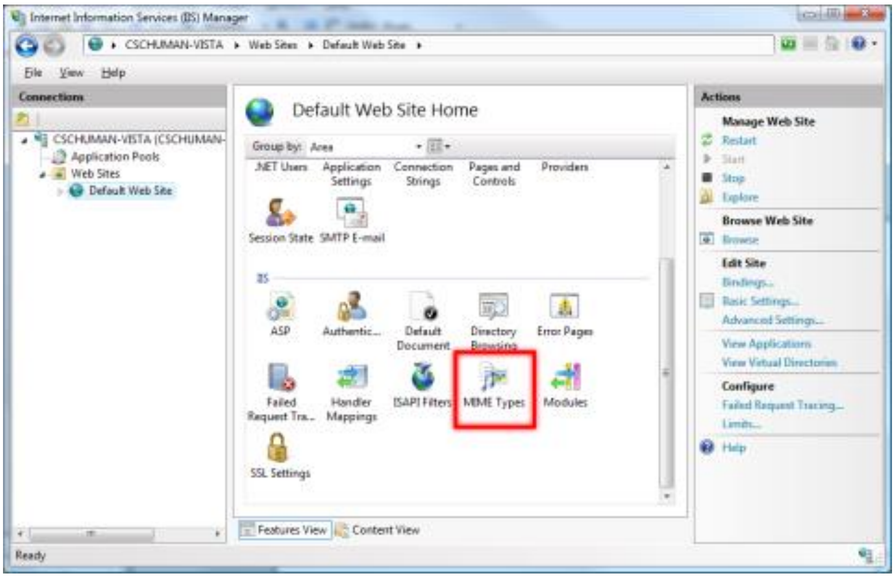
No items match your search.

File name: server

Save as type: Remote Desktop Files (*.RDP)

You must register a MIME type for the RDP file on the webserver. Otherwise Internet Information Services (IIS) cannot make RDP files available to users.

4. At the webserver, run IIS Manager.
   The Internet Information Services (IIS) Manager console is displayed.



5. Select **MIME Types**. The registered MIME types for the selected connection are listed.

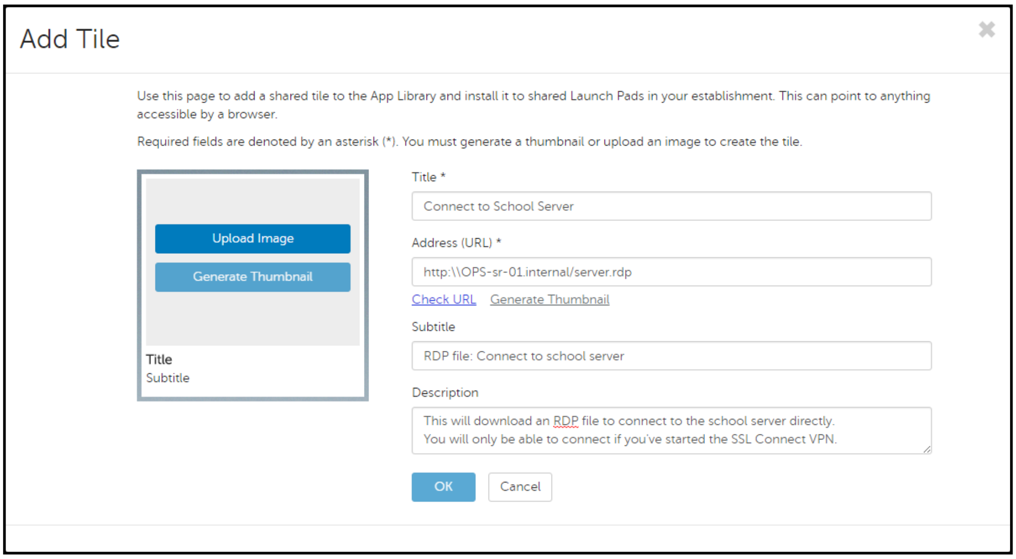
6. Under Actions choose **Add…**

6. In the Add MIME Type window, enter the file name extension **.rdp** and the MIME type **application/rdp**. Click **OK**.

Now create a link tile in RM Unify to the location the RDP file was saved:

7. Log on to RM Unify as an RM Unify Administrator, go to the **App Library** and click **Add Tile**.

   An Add Tile window is displayed.



Add Tile

Use this page to add a shared tile to the App Library and install it to shared Launch Pads in your establishment. This can point to anything accessible by a browser.

Required fields are denoted by an asterisk (*). You must generate a thumbnail or upload an image to create the tile.

Title *: Connect to School Server

Address (URL) *: http:\\OPS-sr-01.internal/server.rdp

Subtitle: RDP file: Connect to school server

Description: This will download an RDP file to connect to the school server directly. You will only be able to connect if you've started the SSL Connect VPN.

8. Enter a suitable **Title**, **Subtitle** and **Description** for this link.

9. Enter the **Address (URL)** for this link.
   The server name to enter will depend on what instructions you gave RM for setting up your SSL Connect VPN:

   - If you specified the search suffix and DNS servers to use, enter the fully qualified domain name for the server
     (e.g., http://OPS-sr-01.internal)

   - If you chose not to set up DNS, use the private IP address for the server name (e.g., http://10.0.1.1)

10. Click **Upload Image**. Locate and select a suitable image for the tile.
    It must not exceed 50 KB and can be a PNG, JPEG or GIF file.

    Note You can only use an uploaded image, as the Generate Thumbnail option will not work with SSL Connect.

    Click **Upload**. An Install window is displayed.

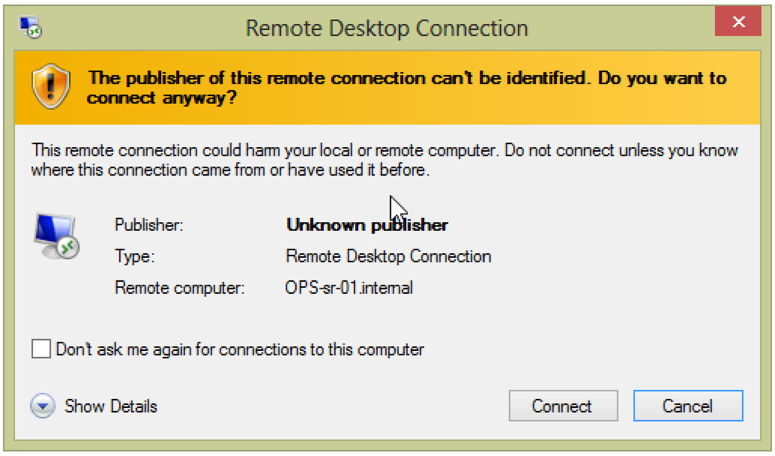
11. Under 'Which roles should SSL Connect be installed to?', tick the appropriate boxes to allocate SSL Connect to the required user roles.

12. If you want to make this tile available on any shared Launch Pads, tick the appropriate boxes.

13. Click **Save**.

14. Close the Install window.

Once you’ve made the tile available you can try clicking on it. You should then be able to download and launch the file. The first time you do this from a location, a warning message will be shown:



Remote Desktop Connection

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: **Unknown publisher**
Type: Remote Desktop Connection
Remote computer: OPS-sr-01.internal

□ Don't ask me again for connections to this computer

To prevent this message from being displayed again, click the **Don’t ask me again…** box. To accept the connection click **Connect**.

You can then log on to the server or computer using your network user credentials as normal. Once connected you can launch the required application, e.g. SIMS.

Appendix II: Troubleshooting

Gathering diagnostic information

If users experience problems with using SSL Connect, our support engineers will be able to help you better if you make a note of the following information:

What happens when you click the SSL Connect tile?

- Does it start to install the plugin? What windows messages are displayed? (see 'Installing the MSI software' from page 8).

- Is the F5 'Network and Application Access' helper window displayed?

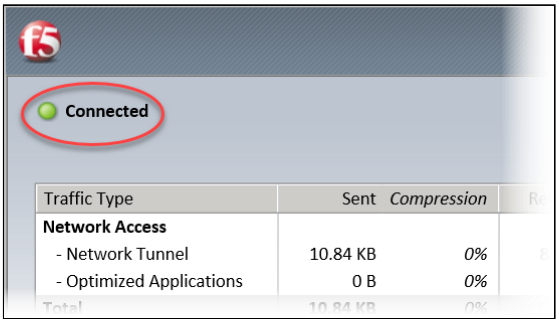
Has the F5 Networks client software installed?

- Is it shown in the Add/Remove Programs list?

  If it hasn't installed via the browser, try using the MSI (see 'Installing the MSI software' on page 8).

What status is shown in the 'Network and Application Access' helper window?

- 'Connected'?



Connected

Traffic Type	Sent	*Compression*	Re
Network Access			
- Network Tunnel	10.84 KB	*0%*	8
- Optimized Applications	0 B	*0%*	
Total	10.84 KB	*0%*	

- If not, what does the status message say?

See ''Network and Application Access' helper diagnostics' on page 22.

Does DNS work – can I use nslookup?

For instructions see '*I get connected but then nothing works*'on page 23.

Do no applications work, or only a particular one?

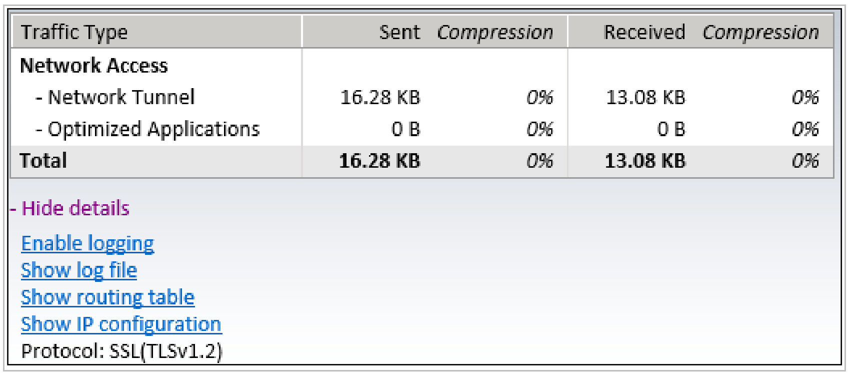
If you can get some resources but not others, then check that the hostname resolves correctly.

Is there a local firewall in the school?

The SSL Connect VPN terminates behind the Central RM Firewall, protecting your site. However if you have a local school firewall, that will need to be configured to allow the traffic from the SSL VPN IP Pool (see page 15).

‘Network and Application Access’ helper diagnostics

In the ‘Network and Application Access’ helper window, click **Show details** to access various diagnostic aids.



Traffic Type	Sent	*Compression*	Received	*Compression*
Network Access				
- Network Tunnel	16.28 KB	*0%*	13.08 KB	*0%*
- Optimized Applications	0 B	*0%*	0 B	*0%*
Total	**16.28 KB**	*0%*	**13.08 KB**	*0%*

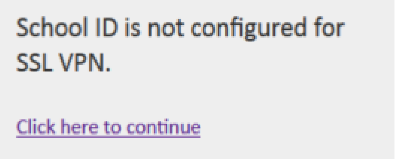
Protocol: SSL(TLSv1.2)

The **Show routing table** and **Show IP configuration** information will be very helpful to the Support desk in resolving issues.

To obtain very detailed log files, use **Enable logging** and **Show log file**. These can be exported and sent to RM if required.

Resolving known issues

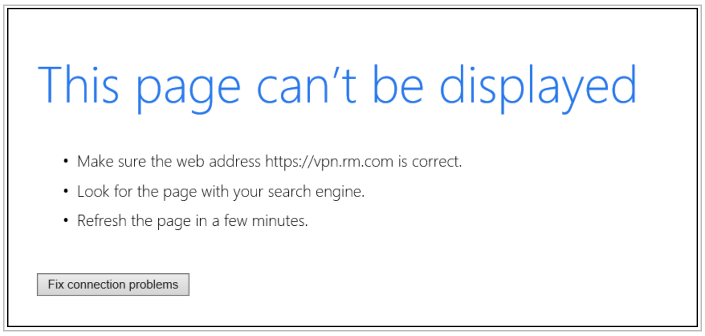
“School ID is not configured for SSL VPN”



School ID is not configured for SSL VPN.

If this message is displayed instead of the F5 Webtop, the site has not been configured correctly. If you have been told by the delivery team that SSL Connect has been configured, please log a support request with the Support Desk.

“This page can’t be displayed”



This page can’t be displayed

- Make sure the web address https://vpn.rm.com is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

If you see a message like this after clicking the tile, a failed logout is preventing you from starting a new session. To clear the stuck session, close all browser windows, and then log on to RM Unify and try again.

I can't install the browser plugin

If you don't already have the F5 software installed, then when you first try using SSL Connect you will be prompted to install a browser plugin. However we recommend that instead of following those prompts, you install the F5 software from the MSI (see page 8).

Further information about the browser installation is given in 'Appendix III: Installing the F5 plugin via Internet Explorer' and 'Appendix IV: Notes on other browsers'.

The connection attempt gets stuck at 'Finalizing'

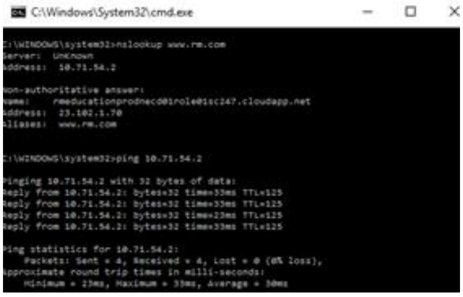
The Network and Application Access window may show a persistent status of 'Finalizing' instead of 'Connected'. If this happens, check that there isn't a UAC prompt that has not been accepted.

I get connected but then nothing works

Can you resolve hostnames via DNS?

1. Open a command prompt (cmd.exe).

2. Type **nslookup www.rm.com**



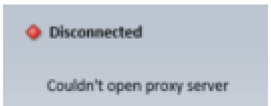
```
C:\WINDOWS\system32>nslookup www.rm.com
Server:  UnKnown
Address:  10.71.54.2

Non-authoritative answer:
Name:    rmeducationprodnecd0irole0isc247.cloudapp.net
Address:  23.102.1.70
Aliases:  www.rm.com


C:\WINDOWS\system32>ping 10.71.54.2

Pinging 10.71.54.2 with 32 bytes of data:
Reply from 10.71.54.2: bytes=32 time=33ms TTL=125
Reply from 10.71.54.2: bytes=32 time=33ms TTL=125
Reply from 10.71.54.2: bytes=32 time=23ms TTL=125
Reply from 10.71.54.2: bytes=32 time=33ms TTL=125

Ping statistics for 10.71.54.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 33ms, Average = 30ms
```

3. Check the 'Ping statistics for' address (e.g. 10.71.54.2). This should be the school's DNS server address which you gave to RM when ordering the SSL Connect service.

4. If the address is correct, try to ping it and traceroute to it.

   If you need to change that IP address, raise a service call with RM, including this DNS diagnostic information.

"Disconnected - Couldn't open proxy server"



Disconnected

Couldn't open proxy server

We've seen this message in networks where an incorrect proxy server setup is being used and the plugin is being installed via the browser.

Make sure that the system-level proxy details match those in Internet Explorer, as follows:

1. As a user with administrative privileges, open a command prompt (cmd.exe).

2. Type **netsh winhttp import proxy source=ie**

The system proxy details are now set to match those configured in Internet Explorer. Close Internet Explorer, reopen it and log in again.

Connection fails, status is ‘Disconnected’ and then the ‘Network and Application Access’ window closes

The connection may fail, with the ‘Network and Application Access’ window closing before you have time to read any error message. This happens if the number of concurrent users exceeds the number of licences purchased.

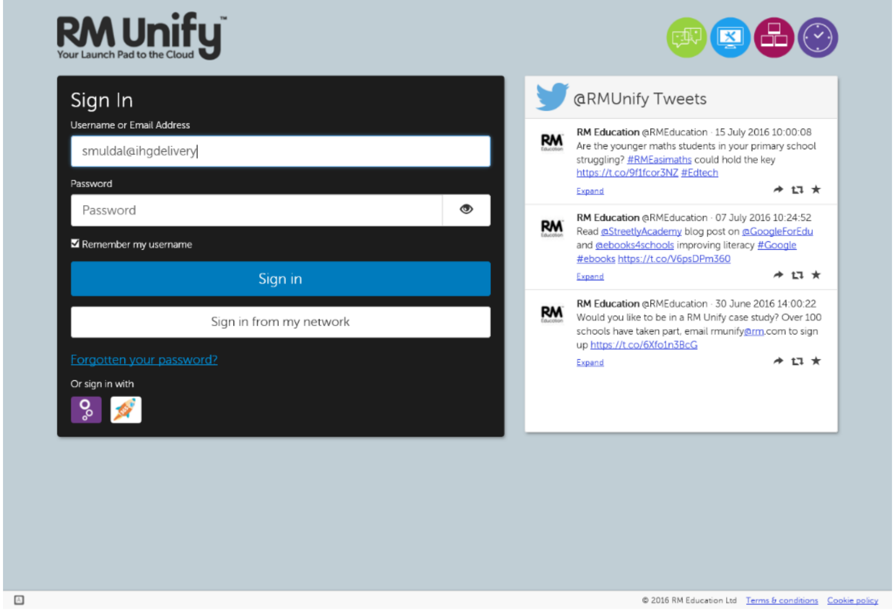
Make sure your users know they should sign out of RM Unify after they have finished using SSL Connect.

Appendix III: Installing the F5 plugin via Internet Explorer

If the F5 Networks software has not been installed on your computer (we recommend the MSI installation method (see page 8), you will be prompted to install it the first time you use SSL Connect. This requires admin rights on the computer.

1. At the computer, open Internet Explorer.

2. Browse to your RM Unify website, enter your RM Unify username and password and click **Sign in**.



Username or Email Address: smuldal@ihgdelivery

Password: Password

☑ Remember my username

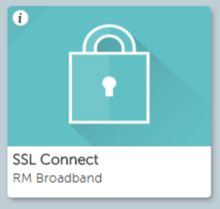
RM Education @RMEducation · 15 July 2016 10:00:08
Are the younger maths students in your primary school struggling? #RMEasimaths could hold the key https://t.co/9f1fcor3NZ #Edtech

RM Education @RMEducation · 07 July 2016 10:24:52
Read @StreetlyAcademy blog post on @GoogleForEdu and @ebooks4schools improving literacy #Google #ebooks https://t.co/V6psDPm360

RM Education @RMEducation · 30 June 2016 14:00:22
Would you like to be in a RM Unify case study? Over 100 schools have taken part, email rmunify@rm.com to sign up https://t.co/6Xfo1n3BcG

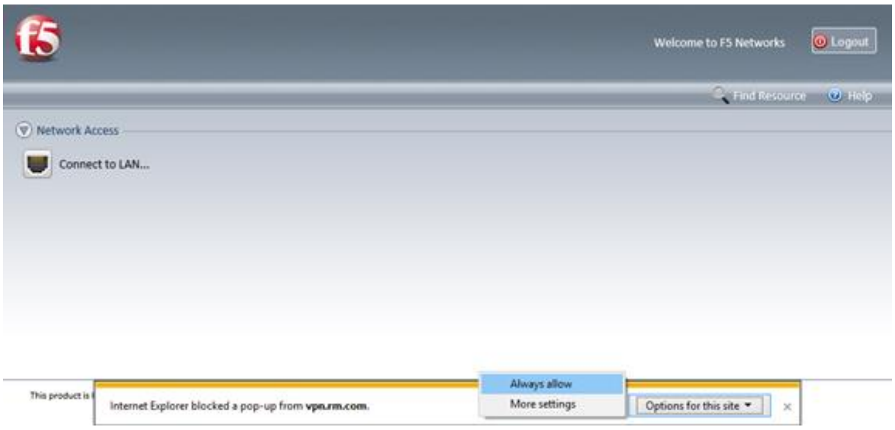
© 2016 RM Education Ltd   Terms & conditions   Cookie policy

3. Launch SSL Connect, either by clicking the **SSL Connect** tile on a shared Launch Pad or by entering the URL address.



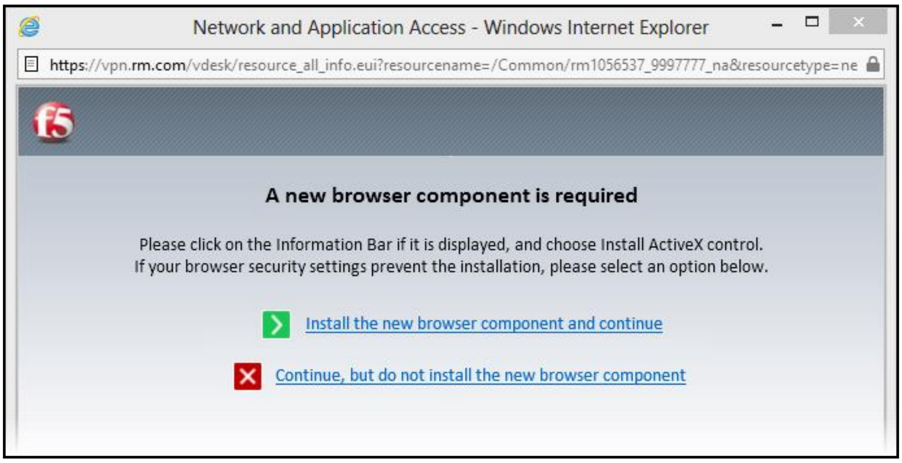
4. The F5 Virtual Webtop is displayed and the connection starts automatically unless you have a pop-up blocker enabled.

   If you do see a pop-up blocker message, allow pop-ups from **vpn.rm.com** and then click **Connect to LAN…** to start the connection.



Internet Explorer blocked a pop-up from **vpn.rm.com**.

The Network and Application Access window prompts you to install a new browser component.


Network and Application Access - Windows Internet Explorer
https://vpn.rm.com/vdesk/resource_all_info.eui?resourcename=/Common/rm1056537_9997777_na&resourcetype=ne

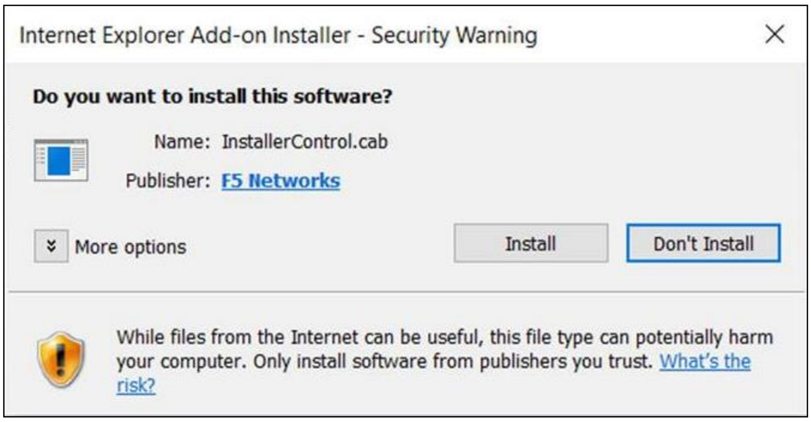
A new browser component is required

Please click on the Information Bar if it is displayed, and choose Install ActiveX control.
If your browser security settings prevent the installation, please select an option below.

Install the new browser component and continue

Continue, but do not install the new browser component

Click **Install the new browser component and continue**.



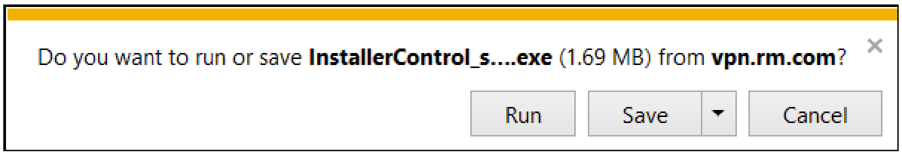
Do you want to install this software?

Name: InstallerControl.cab

Publisher: F5 Networks

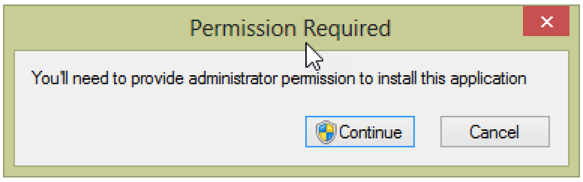
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

5. At the prompt to install ‘InstallerControl.cab’ click **Install**.



Do you want to run or save **InstallerControl_s....exe** (1.69 MB) from **vpn.rm.com**?

6. At the prompt to run or save the executable file, click **Run**.

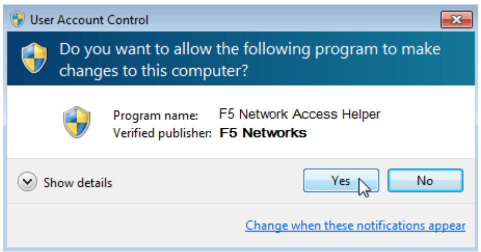


Permission Required

You'll need to provide administrator permission to install this application

7. If you see a ‘Permission Required’ pop-up, click **Continue**.

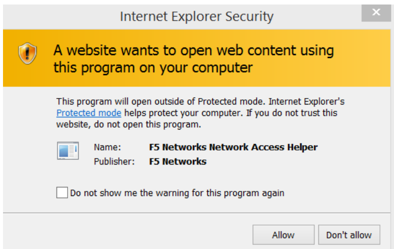
8. Grant access to the F5 Network Access Helper, by clicking **Yes** one or more times in the User Account Control pop-up, and by ticking ‘Do not show me the warning for this program again’ and clicking **Allow** in the Internet Explorer Security pop-up:



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: F5 Network Access Helper
Verified publisher: **F5 Networks**



Internet Explorer Security

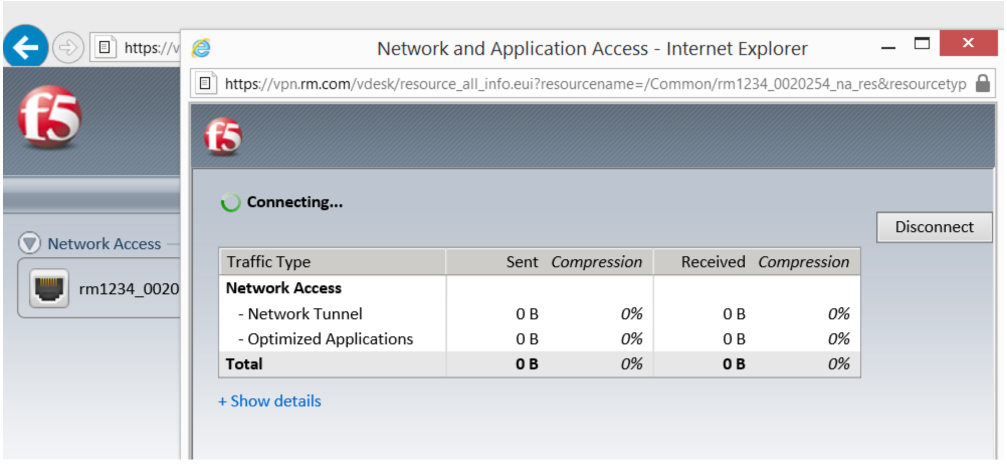
A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: **F5 Networks Network Access Helper**
Publisher: **F5 Networks**

□ Do not show me the warning for this program again

The connection proceeds automatically.



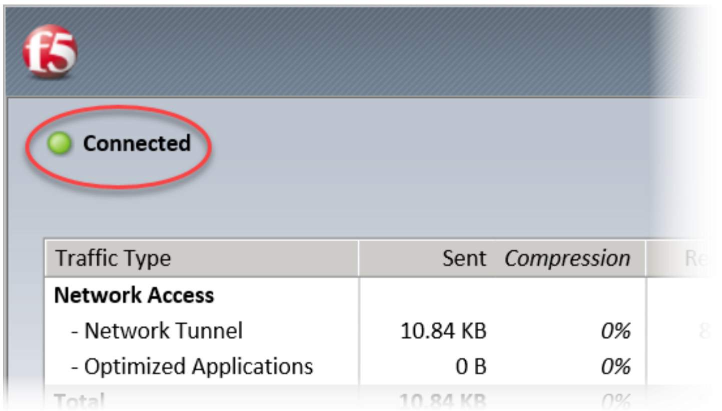
Network and Application Access - Internet Explorer

https://vpn.rm.com/vdesk/resource_all_info.eui?resourcename=/Common/rm1234_0020254_na_res&resourcetyp

Connecting...

Traffic Type	Sent	Compression	Received	Compression
Network Access				
- Network Tunnel	0 B	*0%*	0 B	*0%*
- Optimized Applications	0 B	*0%*	0 B	*0%*
Total	**0 B**	*0%*	**0 B**	*0%*

9. Look for the ‘Connected’ status indicator.



Connected

Traffic Type	Sent	Compression	Re
Network Access			
- Network Tunnel	10.84 KB	*0%*	8
- Optimized Applications	0 B	*0%*	
Total	10.84 KB	0%	

This shows that the VPN connection is now working.

Appendix IV: Notes on other browsers

If you have installed the MSI it will install the plugins required for all installed browsers

For full details of the browsers and combinations supported by F5 refer to F5's documentation:

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-clientcompatmatrix-13-0-0.html

Note not all F5 options documented here have been used or enabled in SSL Connect.

Windows 10 Edge, Windows Chrome, Windows Firefox

These are now supported via the new API.

If you installed the MSI prior to September 2017 you'll need to upgrade to the current MSI to include the improved browser support.

(note while you can install plugins via the browser we still believe it's simpler for the user to install the MSI first and rather than to download the plugin within the browser.)

Windows 10 Client

There is an "F5 Access" application in the Windows App store **however this doesn't currently support the authentication method used in SSL Connect and therefore will not work correctly. Please continue to use the browser based options to start the VPN.**

iOS and Android applications

An F5 Edge Client is available from the iOS App Store.

There is also an F5 Access application in the Google Play app store

After installing either application you will need to set up a new connection as follows:

1. Launch the app and click the **Settings** tab.

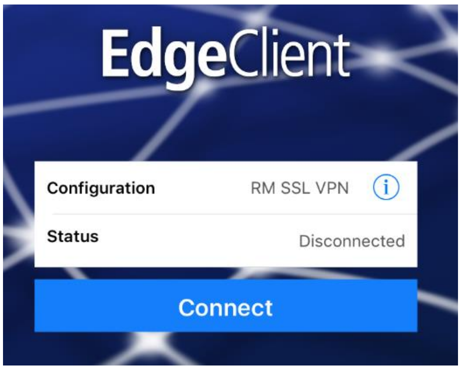
2. Click **Add Configuration**.

3. Enter a Description for this connection, e.g. **SSL Connect**.

4. In the Server field type the fully qualified domain name of the SSL Connect server. (https://vpn.rm.com/RMUnify)

5. Select **Web Logon**.

6. Click **Done**.



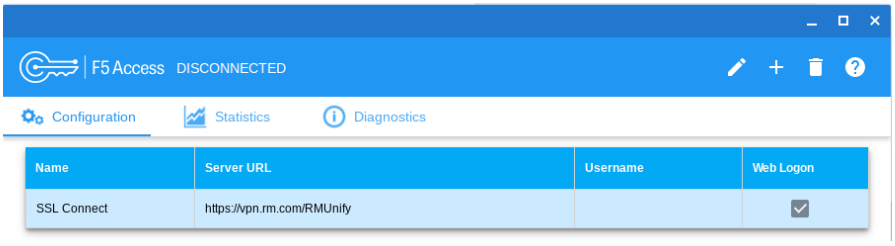
Once the new connection is configured, when you click **Connect** you will be prompted to log on to RM Unify and then SSL Connect will run. Clicking **Disconnect** will close the connection and close your RM Unify session.

Cromebook F5 Access

There is an F5 Access application in the Google Play app store for Chromebooks

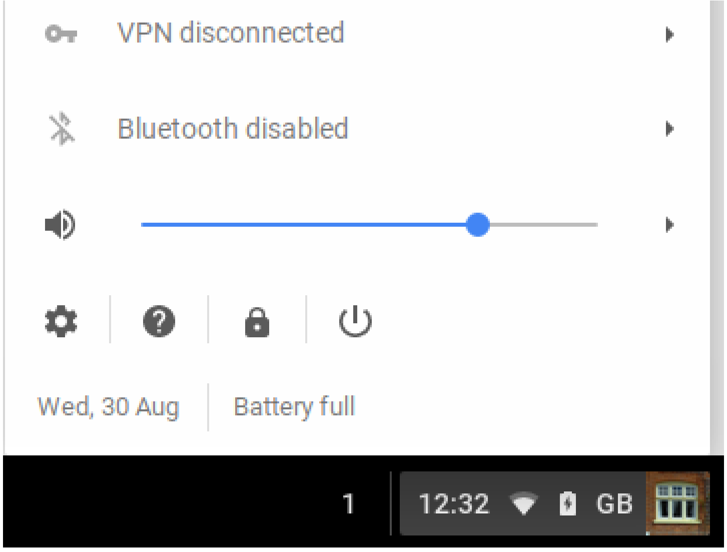
Install the F5 Access application

Launch the application and configure a session with Web Logon enabled and the URL as https://vpn.rm.com/RMUnify

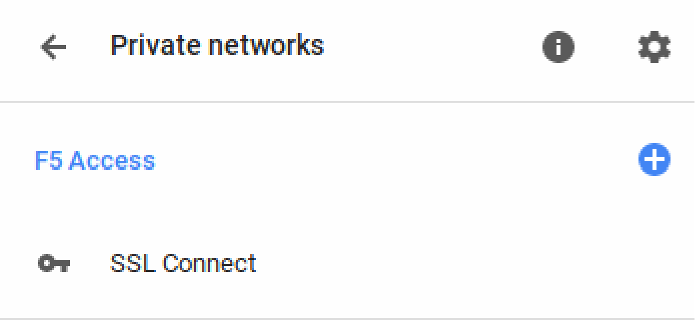


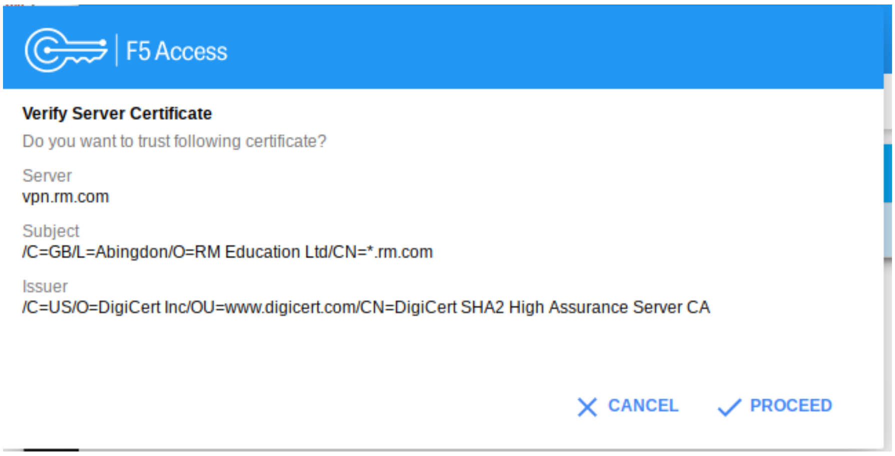
Name	Server URL	Username	Web Logon
SSL Connect	https://vpn.rm.com/RMUnify		☑

To start the VPN click on the Wireless symbol at the bottom right of the screen and select the arrow next to “VPN disconnected”



Select the session you have configured.





Verify Server Certificate

Do you want to trust following certificate?

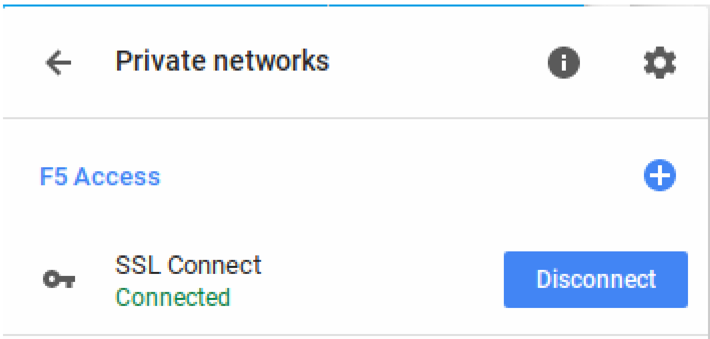
Server
vpn.rm.com

Subject
/C=GB/L=Abingdon/O=RM Education Ltd/CN=*.rm.com

Issuer
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA

Once you Proceed you’ll be asked to sign in to RM Unify and then be connected.

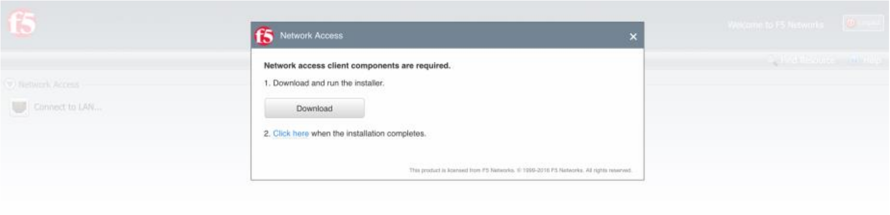
You can then disconnect when finished from the same section.



Apple Macs running OSX

F5 have made a plugin available for Apple OSX that can be installed via the browser

(Apple® OS X® 10.11 and Apple® macOS Sierra (10.12) devices, running Firefox, Safari 9.x, Safari 10.x or Chrome).



Network Access

Network access client components are required.

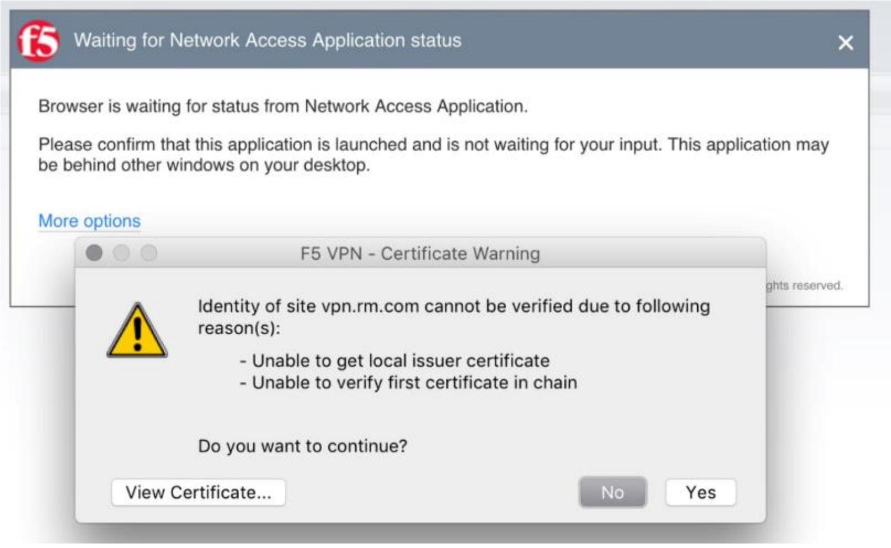
1. Download and run the installer.

2. Click here when the installation completes.

This product is licensed from F5 Networks. © 1999-2016 F5 Networks. All rights reserved.

Once you've downloaded the application and installed it (selecting default options and providing admin credentials) you can go back to the Click Here link above.

We currently have an issue with the certificate on some versions of OSX. It's safe to accept the warning.



Waiting for Network Access Application status

Browser is waiting for status from Network Access Application.

Please confirm that this application is launched and is not waiting for your input. This application may be behind other windows on your desktop.

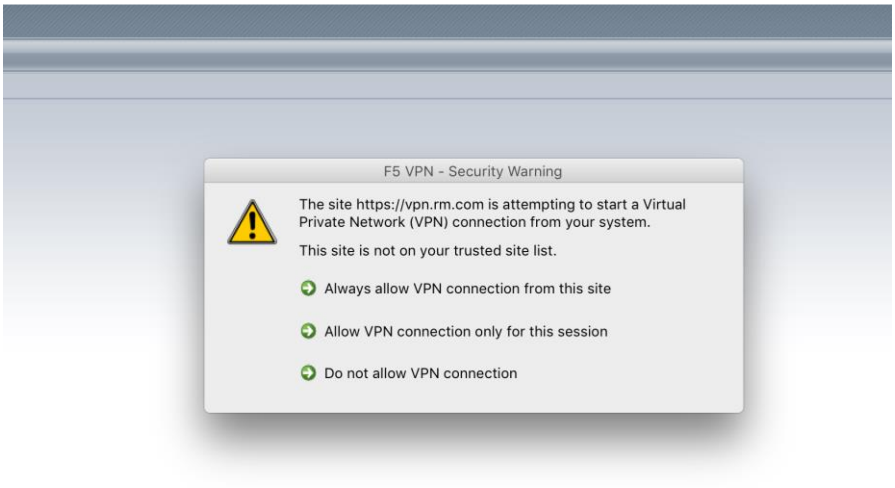
F5 VPN - Certificate Warning

Identity of site vpn.rm.com cannot be verified due to following reason(s):

- Unable to get local issuer certificate
- Unable to verify first certificate in chain

Do you want to continue?

You'll be asked to add vpn.rm.com into trusted sites to enable the application.



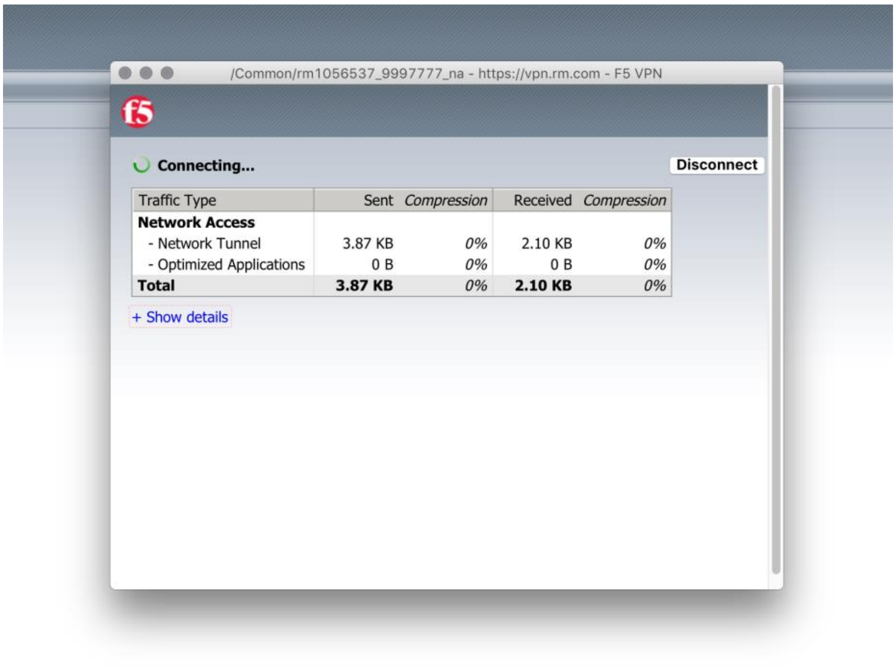
F5 VPN - Security Warning

The site https://vpn.rm.com is attempting to start a Virtual Private Network (VPN) connection from your system.

This site is not on your trusted site list.

- Always allow VPN connection from this site
- Allow VPN connection only for this session
- Do not allow VPN connection

It will then start the connection.



Connecting...

Traffic Type	Sent	*Compression*	Received	*Compression*
Network Access				
- Network Tunnel	3.87 KB	*0%*	2.10 KB	*0%*
- Optimized Applications	0 B	*0%*	0 B	*0%*
Total	**3.87 KB**	*0%*	**2.10 KB**	*0%*

+ Show details

Note: if you’re using an OSX device to access Windows networks you’ll need to install an RDP client or map SMB shares using native OSX tools

Appendix V: Uninstalling the F5 Networks plugin for Windows

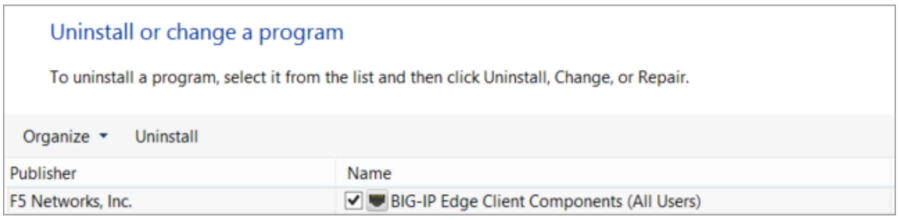
To enable the use of SSL Connect on a computer, a browser plugin will have been installed, either from the MSI file or directly through the browser.

If you need to uninstall the plugin:

1. From the Windows Start screen or menu, open **Control Panel**.

2. Choose **Programs**, **Uninstall a program** (or **Programs and Features**).

3. From the list of programs, select **BIG-IP Edge Client Components (All Users)**.



Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Publisher	Name
F5 Networks, Inc.	☑ BIG-IP Edge Client Components (All Users)

4. Click **Uninstall** and **Yes** to confirm.