Sabre Red 360
Remote Desktop Server

Technical Guide

Document Version: 3.2
Author: Malcolm Davies

©SABRE

All rights reserved. No part of this publication may be reprinted, reproduced, stored in a retrieval system or transmitted, in any form or by any means, without the prior permission in writing from the owners.

Table of Contents

1 Introduction

1.1 About This Guide

This document has been designed to assist with the installation of Sabre Red 360 and its components on a Remote Desktop Server. Support for all Sabre products in a server environment is a customized service and only limited support is available from the Sabre Technical Support team.

This guide focuses on Remote Desktop Servers, but the points raised can be translated to desktops, laptops, VDIs and other platforms in more complex or controlled environments.

1.2 Windows Requirements

Sabre Red 360 is certified for **Windows Server 2016, 2019 & 2022.**

The IT technician performing this installation will need to have full local Administrator access and permissions to the servers. Do not proceed if Admin rights are not available.

During initial setup, set the Windows server language settings to English (your country) with a US Keyboard. Other language packs can be installed once testing is complete but please be aware that some unsupported languages and keyboard settings have been seen to cause anomalies in Sabre Red 360. A reboot of the server is required for changes to the Windows language to take effect.

1.3 Sabre Prerequisites

Either a *Core Connect VPN* (hardware) or the *SCVPN JVM VPN* (software) roles are required when using Sabre Red 360 through Remote Desktop Services. These enable Sabre Host connectivity and without one of these options, connections may fail. More details are in the Core Connect VPN & SCVPN sections of this guide.

IT specialists may wish to test Sabre Red 360 with their own Sabre logins. Only Travel Agency staff (usually managers or supervisors) can set up Sabre logins for an agency, so IT teams should refer to these teams for Sabre login assistance.

1.4 Recommended Spec

The exact requirements for Sabre Red 360 on a Remote Desktop Server depend on how many users are on the server, what Sabre Red Apps they use, what other 3rd party applications will be used, the speed of local disks and networks, etc.

The following information can be used as a guideline:

Hardware Specifications

- A recent model processor (CPU) meeting the minimum requirement for the version of Microsoft Windows Server edition (Intel Xeon or equivalent recommended for Remote Desktop Servers)
- Minimum 2 GB RAM for each Sabre Red 360 instance. Additional memory may be required for other agency applications
- 1024 x 768 16-bit (High Colour) video resolution or higher
- Min. 2GB of free disk space for the common files and 250 MB+ for each additional user
- Network access (please see later in this guide for specific information)

CPU Benchmarking

It is recommended to check your CPU benchmark on the Passmark website. This site will provide information like clock-speed; number of cores; year of release; CPU benchmark; single thread rating; etc.

As a general guide for server customers using Sabre Red 360, it is recommended that the CPU Single Thread Rating be above *2000*. Ratings below this can impact the launch time of Sabre Red 360 but can vary from server to server depending on other factors.

Best performance will be seen on hardware that is up to date. Pre-2017 processors are known to be less efficient, and issues have been seen with these. The InSpectre tool can also be useful to validate if older CPUs are affected by Spectre / Meltdown vulnerability patching and associated performance issues.

It is the responsibility of the customers IT team to test and monitor system resources, especially when Sabre is used alongside other applications.

2 Pre-installation setup – for Administrators

2.1 Installation locations

All steps within this pre-installation section should be performed by the *local* IT Administrator, with *full admin rights* to the server.

In a Server environment, it is expected that Administrators will lock down some areas of the server. Sabre Red 360 requires ***Full Control*** for all users to the chosen installation paths. The storage disks where Sabre Red 360 is installed need to be *local, persistent* storage.

This section details the recommended installation paths and how to pre-determine these file locations prior to user-installation. There are two primary sets of files required for Sabre Red 360:

Sabre Common files

On a single server, the Common and executable files should be placed in a central location, and this can be anywhere on the local disk that can be accessed by all users. For example: **C:\Sabre\SabreRed360.**

In *multi-server* environments the Common and executable files should be installed onto each server's local drive. They must be installed to an identical file path on each server (i.e. **C:\Sabre\SabreRed360)** so that these files will consistently be available whichever server the user lands on.

Important note: The Sabre *Common* files should not be installed to a network share as this will have an impact on SR360 performance and stability no matter how fast the network is. Using fast local disks is essential.

Sabre Profile files

By default, the user *Profile files* will automatically be created in the default location of *%LocalAppData%\Sabre Red 360* and it is recommended to keep this default for a single server installation.

In a multi-server environment the *Profile* directory needs to be available from whichever server the user lands on. If desired, they can be redirected to an alternate location using the Locator file (see next page). Whichever location is chosen, ensure that the Sabre users have **Full Control** permissions on all Sabre files.

While the *Common* files should *not* be placed on a network share, placing the user *Profiles* on a fast network share that is accessible from all servers is generally ok. The performance of this setup will depend on the number of users, network bandwidth and other factors. Thorough performance testing should be conducted before going live.

2.2 Golden Images / Nightly Rollbacks

Some server Administrators like to use a "Golden Image" restoration process or nightly rollbacks, restoring the server to a previously known "good" state each night. Sabre Red 360 is constantly updating files and plugins and any form of rollback process can delete important, recently downloaded files causing errors and corruptions in Sabre Red 360. To avoid ongoing issues, Sabre Red 360 should be installed to a local, persistent storage location so that the Sabre files are not impacted.

In these situations, a secondary local drive (i.e. a D Drive) with persistent storage is recommended. This will allow the Golden image restore process to take place each night on the C Drive, leaving the Sabre files on the secondary drive uncorrupted and up to date.

The common files should not be touched, deleted or changed manually or by any automated process without risk of a SR360 corruption. The self-healing ability of the SR360 single.exe can repair user's individual profiles and plugins, but if core files are removed or damaged SR360 may not be able to recover. In a Remote Desktop Server environment this can mean all users on a server or within the entire environment may not be able to login to Sabre Red 360.

2.3 Locator file

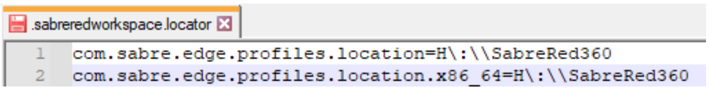
Administrators may prefer to change the location of the users Sabre *Profile* files. To do this we can create a **locator** file which will direct the SR360 installer to use an alternate Profiles location. Without this file, user Profiles will default to *%LocalAppData%\Sabre Red 360*. To begin, choose your preferred path (the examples below use *H:\SabreRed360*), open Notepad on the server and paste the following into it:

32-bit installer:	**com.sabre.edge.profiles.location=H\:\\SabreRed360**
64-bit installer:	**com.sabre.edge.profiles.location.x86_64=H\:\\SabreRed360**

If unsure, both 32-bit and 64-bit formats can be added without any negative impact.

Important note: The paths in the locator file use Java formats with additional backslashes. If standard Windows file paths are added here, they will not work

Save the file using the filename ***.sabreredworkspace.locator*** ensuring the suffix is .locator not .txt. The naming convention of this file is very specific (please note the dot in front of the name). The newly created locator file then needs to be moved to the **C:\Windows** directory of each server that will have Sabre Red 360 installed on it. An example of a .sabreredworkspace.locator file will look like this:



```
com.sabre.edge.profiles.location=H\:\\SabreRed360
com.sabre.edge.profiles.location.x86_64=H\:\\SabreRed360
```

2.4 Installing the Sabre Red 360 Common Files

The Sabre zip file package can be downloaded from the following link. These links are updated monthly and will always contain the latest available version of the Sabre Red 360 zip files.

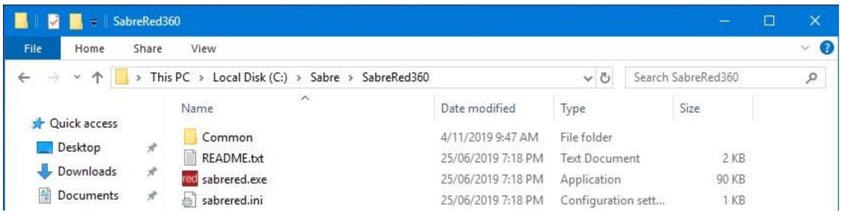
64-bit: https://updatesite.my.sabre.com/updatesite/installers/newprov/sabrered.win32.x86_64.release.html

32-bit: https://updatesite.my.sabre.com/updatesite/installers/newprov/sabrered.win32.x86.release.html

Whether you use the 32-bit or 64-bit installer is dependent on what other applications you use in your environment, and whether they need to interact with each other. For example, if you have a 32-bit back-office application, 32-bit Adobe Reader and 32-bit Microsoft Office then it is recommended to use the Sabre 32-bit installer so that if there is any interaction between these applications the architecture will be consistent.

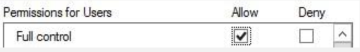
Note: Do not mix the different architectures in a multi-server environment. It is essential that all servers are set up with the same architecture. i.e. all 32-bit or all 64-bit.

The Zip file contains the Common and executable files that are used by all Sabre users. Extract the zip file to the newly created **C:\Sabre\SabreRed360** folder (or alternative preferred location).



Name	Date modified	Type	Size
Common	4/11/2019 9:47 AM	File folder	
README.txt	25/06/2019 7:18 PM	Text Document	2 KB
sabrered.exe	25/06/2019 7:18 PM	Application	90 KB
sabrered.ini	25/06/2019 7:18 PM	Configuration sett...	1 KB

Important note: Ensure that all users have *Full Control* of this directory.



Permissions for Users	Allow	Deny
Full control	☑	□

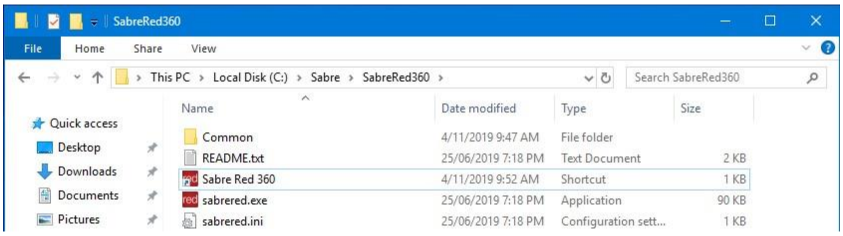
Insufficient permissions can cause updates to fail or files to become corrupted.

Sabre Red 360 was previously branded as Sabre Red Workspace.
There may still be existing references to Sabre Red Workspace in some file or folder locations and older installations, but it is the same base application.

2.5 Create Desktop shortcuts

Create a Sabre Red 360 shortcut. Right click the *sabrered.exe* file and select **Create shortcut**. A new shortcut will be created in the folder.

Rename the new shortcut to **Sabre Red 360.**



Name	Date modified	Type	Size
Common	4/11/2019 9:47 AM	File folder	
README.txt	25/06/2019 7:18 PM	Text Document	2 KB
Sabre Red 360	4/11/2019 9:52 AM	Shortcut	1 KB
sabrered.exe	25/06/2019 7:18 PM	Application	90 KB
sabrered.ini	25/06/2019 7:18 PM	Configuration sett...	1 KB

Then copy the new **Sabre Red 360** shortcut onto the desktops of any Sabre users. Alternatively, you can push the shortcut to all server users by placing it in **C:\Users\Public\Desktop** (hidden folder).

If you plan to predefine the consultant's user *Profiles* location with the locator file, do this now.

Once Sabre Red 360 has been installed, do not attempt to manually move any files to a new location. This will corrupt this installation due to broken paths. Relocating Sabre Red 360 can only be done by performing a fresh installation.

It is possible for an Agency Administrator to semi-automate or package the process described above, extracting the zip files, granting permissions, creating a locator file and pushing shortcuts, as long as the described rules are followed. Automation advice is not supported by Sabre and would be up to the server Administrator to design and manage.

2.6 Updates & Sabre Red 360 versions

An existing Sabre Red 360 installation will continually keep itself up to date while in use. When a user logs into Sabre it will automatically check for updates 20 minutes after first login and every 4 hours subsequently. Local, persistent storage is essential to retain these updates.

Any downloaded updates for existing users become available to use when the user next logs into Sabre Red 360 after having closed the application.

If a new Sabre installation is required (for example, adding a new server), always download and use the latest zip files.

Installing a new user on Sabre Red 360 with an old, previously downloaded installer is likely to cause issues.

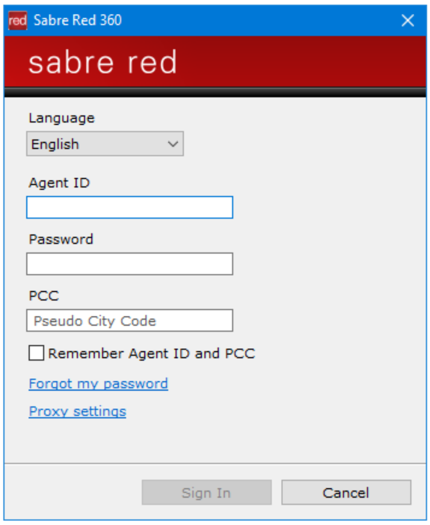
3 Sabre Red 360 installation – for End Users

The steps in the previous section were performed by the server Administrator. The steps in the following section are performed by the end user within their own Windows profile and allows users to self-install Sabre Red 360 following simple prompts.

This process cannot be performed by Administrators, bypassed or automated as each Sabre user has their own unique credentials, a EULA agreement to accept and one-off profile and security questions to complete.

3.1 Sabre Red 360 installation

Ask the first user to log in to their Windows session and direct them to the Sabre Red 360 shortcut on their Desktop. Double click the Sabre Red 360 shortcut. They will then be required to log in to Sabre using their Sabre provided credentials. They should input the **Agent ID** (EPR), Sabre **Password**, and Pseudo City Code (**PCC**) and click **Sign In**.



Language: English

Agent ID:

Password:

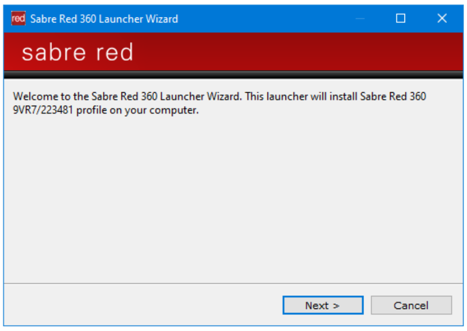
PCC: Pseudo City Code

□ Remember Agent ID and PCC

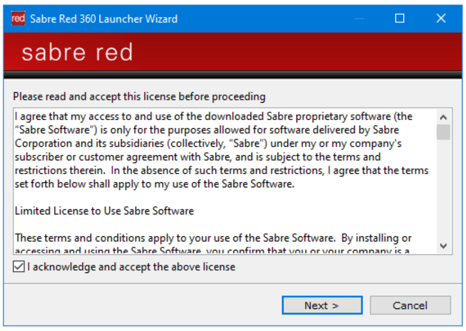
Users logging in for the first time and using a temporary password will be prompted to change their password at this point.

Users can also tick the **Remember Agent ID and PCC** box to retain their details for future use.

Click **Next** and Sabre Red 360 will ask the user to accept the End User Licence Agreement (EULA).



Welcome to the Sabre Red 360 Launcher Wizard. This launcher will install Sabre Red 360 9VR7/223481 profile on your computer.



Please read and accept this license before proceeding

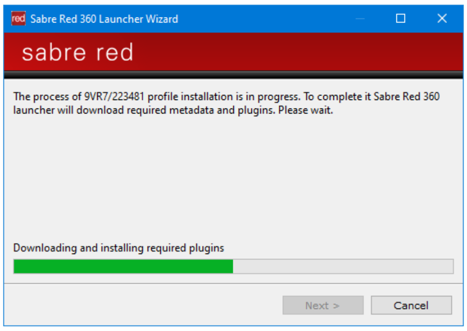
I agree that my access to and use of the downloaded Sabre proprietary software (the "Sabre Software") is only for the purposes allowed for software delivered by Sabre Corporation and its subsidiaries (collectively, "Sabre") under my or my company's subscriber or customer agreement with Sabre, and is subject to the terms and restrictions therein. In the absence of such terms and restrictions, I agree that the terms set forth below shall apply to my use of the Sabre Software.

Limited License to Use Sabre Software

These terms and conditions apply to your use of the Sabre Software. By installing or accessing and using the Sabre Software, you confirm that you or your company is a

☑ I acknowledge and accept the above license

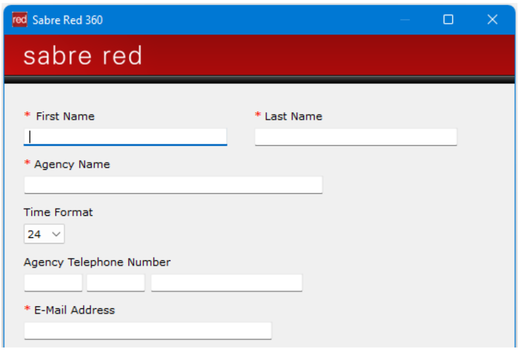
Sabre will the proceed to download any required data and plugins - This may take a few minutes.



The process of 9VR7/223481 profile installation is in progress. To complete it Sabre Red 360 launcher will download required metadata and plugins. Please wait.

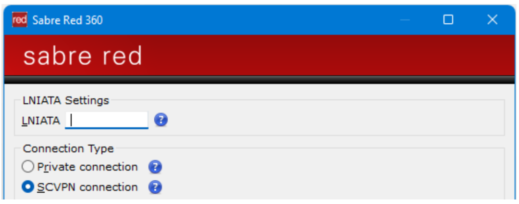
Downloading and installing required plugins

If a user is logging into Sabre for the first time, they will be directed to a Sabre Red profile page. This needs to be completed with their personal information. When completed, click **Next.**



* First Name
* Last Name
* Agency Name
Time Format: 24
Agency Telephone Number
* E-Mail Address

New users will be asked for their **LNIATA** which will have been provided with their login details. The default Connection Type is **SCVPN** which should be left as it us unless otherwise instructed. When completed, click **Finish.**

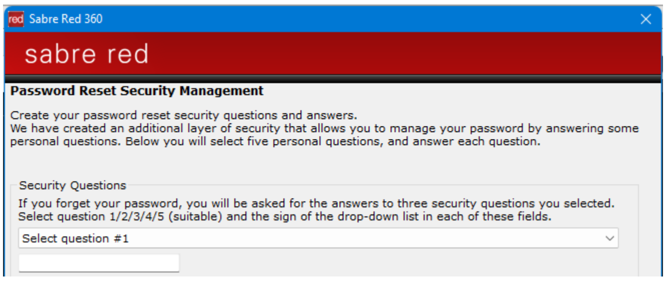


LNIATA Settings
LNIATA

Connection Type
○ Private connection
● SCVPN connection

If the Windows Firewall is enabled, a prompt may be seen at this point. Select **Allow**.

New users will also be prompted to complete their Password Reset Security Management questions. This should be completed so that users have the ability reset their own password if they forget it.



Sabre Red 360

sabre red

Password Reset Security Management

Create your password reset security questions and answers.
We have created an additional layer of security that allows you to manage your password by answering some personal questions. Below you will select five personal questions, and answer each question.

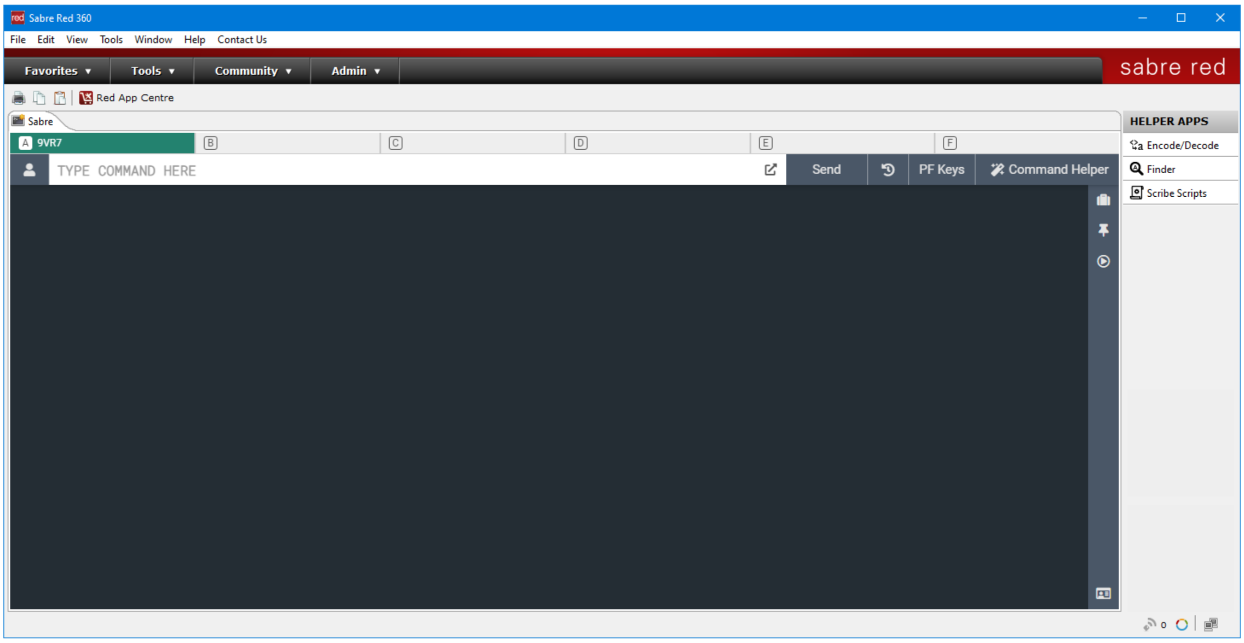
Security Questions

If you forget your password, you will be asked for the answers to three security questions you selected.
Select question 1/2/3/4/5 (suitable) and the sign of the drop-down list in each of these fields.

Select question #1

Users that have previously completed these profile screens only need to complete them once. After that the data is stored and these screens will not pop-up during subsequent installations.

At this point Sabre Red 360 is installed and ready to use. If the Core Connect or SCVPN connection to Sabre is unavailable, the host screen will not appear.

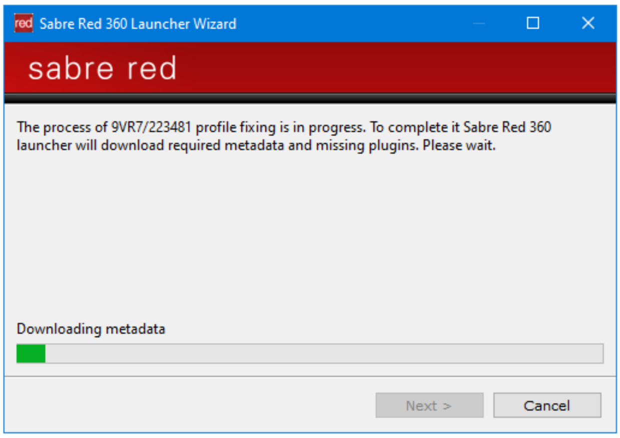


Sabre Red 360 does offer the ability to configure a proxy server on the login screen. If proxy settings are required then please refer to the proxy section later in this guide for more details.

3.2 Self-Healing

Sabre Red 360 will automatically check for updates 20 minutes after logging in each day, and every four hours after that, so files will be regularly updated. These updates are usually small but critical for smooth operation of the system.

Sabre Red 360 is self-healing and if required plugins are missing at login, a status window will pop-up during the login process and prompt to re-downloaded missing files.



The process of 9VR7/223481 profile fixing is in progress. To complete it Sabre Red 360 launcher will download required metadata and missing plugins. Please wait.

Downloading metadata

While this is a positive pop-up, if the self-healing process is happening on a regular basis then it may mean that plugin files are being lost, deleted or not downloaded. It is recommended to discuss this with your Sabre Technical Specialist to ensure you have the optimum setup for your environment.

If any required files are mapped to a network share but the network share is offline then unavoidable errors will still occur and will not recover until the network share is available again.

4 Sabre Red 360 Connectivity

4.1 Network ports and access

Sabre Red 360 requires connectivity to key systems to manage authentication, connectivity to content sources, and system update components.

Please refer to the latest version of the *Sabre Red Connectivity Guide* on myhelp.sabre.com for specific details.

4.2 Proxy Servers

During initial testing and setup, it is recommended to allow SR360 to access the internet directly to avoid issues with proxies and firewalls. Introducing proxies and firewalls after successful testing will help you quickly identify where an issue lies if subsequent problems occur.

Proxies can be manually configured on a per user basis by clicking on the **Proxy Settings** link on the login screen of SR360. In environments where all users use need a proxy configuration, you can centrally configure these settings.

For site administrators that wish to enforce a proxy server for all users, this can be done by adding an additional argument to the **sabrered.ini** file. The sabrered.ini file will be located with the original Common files from the zip extraction (i.e. **C:\Sabre\SabreRed360**).

Open **sabrered.ini** and insert two more lines of argument in sequence after any other “arg” entries that are present. This would normally be arguments 3 and 4 as shown, but please validate this in your specific file.

```
arg.3=--proxy.host= TestProxyAddress
arg.4=--proxy.port=80
```

These lines will enable the proxy automatically and pre-populate the HTTP Proxy address and port number for all users of that sabrered.exe. Once the **sabrered.ini** file has been updated, these settings can be verified by opening SR360 and clicking on the **Proxy Settings** link on the login page.

Caution should be used when updating the **sabrered.ini** file. Accidentally changing or deleting other data in this file can cause errors than can affect all Sabre users on the server. To be safe, it is recommended to make a copy of the original sabrered.ini file before changing settings.

4.3 SCVPN (for Host Connectivity)

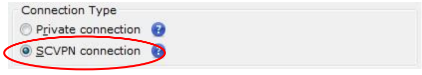
Overview

SCVPN – Sabre Customer Virtual Private Network – is a software VPN that allows customers to use their existing internet connection to establish a secure connection to Sabre Host without the need for hardware setups.

SCVPN with the **SCVPN_JVM_Integration** role is now certified and supported in a Remote Desktop Server environment depending on site size and complexity, but this role is not assigned by default. Please discuss this with your Sabre Technical Specialist prior to installation.

Enabling SCVPN

Sabre VPN is launched as part of the SR360 login process and does not require configuration by the end user. The SCVPN installation is a tick-box in the SR360 user profile. If this box is selected then SCVPN will attempt to launch each time the user logs in to Sabre Red 360 unless an existing VPN tunnel like Core Connect VPN is already present.



Connection Type

○ Private connection

● SCVPN connection

If a Sabre VPN like Core Connect is available when a user signs into Sabre Red 360 then Sabre will recognise that there is an existing tunnel and not attempt to launch SCVPN. Leaving SCVPN selected in the user profile is recommended.

Native SCVPN limitations

Customers should be aware of the following limitations of using native SCVPN if a Core Connect VPN is not available or the **SCVPN_JVM_Integration** role is not assigned.

- The first user signing into SR360 on the server will authenticate with Sabre and receive a token to enable connectivity. SR360 will launch SCVPN and connect in the same way it would on a desktop
- When the second and subsequent users sign in on the same server they will authenticate and connect using the token obtained by the first user.
- This is fine and all users will work without issue….. until…..
- When the 1st user (who was initially assigned the token) closes SR360, the clock starts ticking. The other users will continue to work, but if any of them are inactive in Sabre for a few minutes then Sabre won't recover as it can no longer find the token that was issued to the first user
- When the timed-out users try to type into the Sabre host screen after that, Sabre will not respond and they will need to close Sabre and start again

The previous steps are detailed here to help users identify the situation if it occurs.

To add the **SCVPN_JVM_Integration** role, please contact your Sabre Technical Specialist or Sabre Technical Support.

The separate *Sabre Red Connectivity Guide* contains the SCVPN networking requirements.

4.4 Core Connect VPN (for Host connectivity)

A Core Connect VPN is the preferred option for Sabre Host connectivity at larger sites. Core Connect is a "business to business" VPN connection for Sabre connected customers. It creates a continual VPN connection from the agency router or firewall to the Sabre Core Connect regional servers. The Core Connect solution uses a public internet connection but creates a private tunnel for Sabre Host connectivity.

Core Connect VPNs are used by larger sites and sites that cannot support a software VPN. There is a monthly cost attached to Core Connect VPNs and they are initially requested through the customers' Sabre Account Manager.

CCVPN has endpoints in three different regions. Each customer will choose the best pair of endpoints for them based on their location.

- North America - Dallas / Chicago
- Asia Pacific - Singapore / Sydney
- Europe - Frankfurt / Amsterdam

Either endpoint in the regional pair can be the primary, with the other one being the secondary.

If a site has a requirement for a Sabre Java Printing Module (SJPM) and requires 24/7 reliability, then a Core Connect VPN will be necessary.

5 Sabre Red 360 Roles

Sabre Red 360 has a variety of roles available to make setup and ongoing use of SR360 on a Remote Desktop Server simpler. These roles are not automatically applied and will need to be requested from your Sabre Technical Specialist.

5.1 SCVPN JVM Integration role

Role Name: `SCVPN_JVM_Integration`

As mentioned in the previous sections, the SCVPN_JVM_Integration allows customers to use the software SCVPN on a Remote Desktop Server. Without this role, SCVPN may appear to work initially but there could be unexpected connectivity issues later.

If the server has an SJPM installed, this role will impact SJPM connectivity unless there is also an active CoreConnect VPN.

5.2 Connectivity Tester role

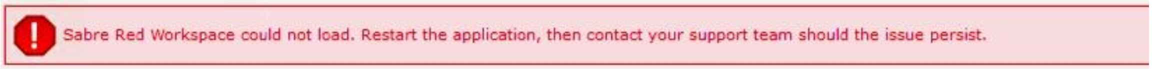
Role Name: `DR_UI_Connectivity_Tester`

The Connectivity Tester role gives a more detailed display of Sabre connectivity. Once assigned, double click the two computers symbol in the bottom right of SR360, it will open a Connection Details box. If any of the displayed services don't turn green within 1 minute of opening this box, it will help identify at a glance if there are any suspicious connection issues.

5.3 Webkit role

Role Name: `Dynamo_Browsers_Webkit_AUTO`

The Dynamo_Browsers_Webkit_AUTO role will detect if the agent is running on a Server platform and sets the mode for JX Browser to be *lightweight* for Red Apps. This would typically only be used on older hardware and can help with users that see this error when launching Sabre Red 360.



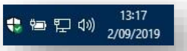
Sabre Red Workspace could not load. Restart the application, then contact your support team should the issue persist.

There are other known causes of this error, so this is just one of the possible troubleshooting steps.

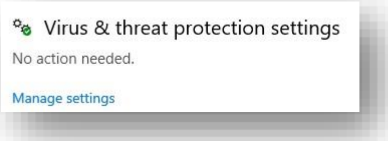
6 Antivirus exclusions

Recent versions of Windows Server come with built in Virus and Threat Protection, and on occasion this has been seen to over-scan the Sabre files and noticeably slow the Sabre Red 360 launch times. This issue can be bypassed by adding the following exceptions:

- Double click the **Shield** in the System Tray



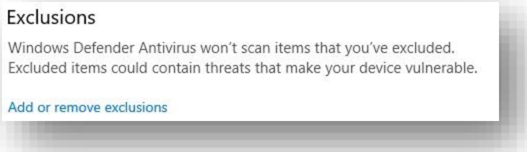
- Click **Manage settings** link under Virus & threat protection settings


Virus & threat protection settings

No action needed.

Manage settings

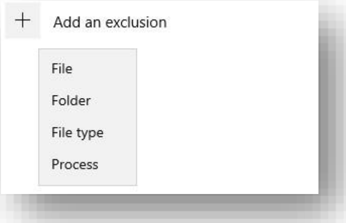
- Under Exclusions, select **Add or remove exclusions**


Exclusions

Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.

Add or remove exclusions

- Click on **Add an exclusion**



- Select **Process** and manually add two exclusions (one-at-a-time):

sabrered.exe *chromium.exe*

Sabre directories should also be excluded by also adding the folders to your chosen installation paths.

This issue can exist with any 3rd party antivirus software, so if you are experiencing slow Sabre Red 360 launch times or intermitted errors, this should be investigated further.

7 Other Information

7.1 Virtual Desktops

While *Virtual Desktop* environments like *Citrix Xen Virtual Desktop, Microsoft Azure Virtual Desktops* or *Amazon 360s* are built on server technology, the design is based on a unique desktop environment for each user. In theory, SR360 can be installed in these environments in the same way as you would on a standalone desktop, using default install paths and a standard Sabre .exe installer

Be aware *if* the VDIs have shared components like C Drives or port numbers. In those instances, you may still need to follow some instructions contained within this document to ensure there are no conflicts. Sabre must be installed to persistent storage as any rollbacks may corrupt the Sabre files.

7.2 Troubleshooting – Profile Reset

If a consultant with a shared installation is having odd responses in SR360 that other users are not experiencing, then one simple point of troubleshooting can be to “reset” their profile

Ask the end user to close the SR360 application. The Administrator can then go to the end users Profile folder (default location %LocalAppData%\Sabre Red 360 unless it has been redirected using the .locator file) and rename the **Sabre Red 360** directory to **Sabre Red 360.old**. It is best to retain this directory until the user has confirmed that everything is working correctly.

Ask the end user to log back in to SR360 and they will go through a Profile reinstall process. This should resolve any profile issues relating to the installation. The .old directory can be deleted once everything is confirmed as ok.

7.3 Troubleshooting – Replacing Common files

Centralised Common files are shared by all Sabre users on a server. If *all* consultants are having the same issue then it is possible that the Common files have been corrupted so it can be worth reinstalling the Common files, but bear in mind this will impact all Sabre users on the server. The steps for this process are:

- Download the latest version of the Sabre Zip file detailed earlier in this guide
- Ask everyone on the server to sign out of Sabre, close it and stay out until advised
- Rename the common files directory to SabreRed360.old
- Create a new SabreRed360 directory and ensure it has Full Control permissions
- Unzip the Sabre files to the new SabreRed360 directory
- Ask Sabre users to log back into Sabre

This directory contains the Red Apps and plugins used by consultants so it is very likely that some users will receive the self-healing pop-up (detailed previously in this guide) when they log back in. This is expected behaviour so you can advise them about this in advance.

If more errors occur then you can rename the .old directory to restore the previous installation. If all issues are resolved the .old directory can be deleted.

7.4 Disable the Sign In user list

If multiple users share the same Common files on a server, the Sabre sign in window will display a drop down menu with a list of installed users. This is usually the preferred option but it can be disabled.

To disable this feature, add the following line to the .sabreredworkspace.locator file:

```
com.sabre.edge.platform.core.common|attachProfilesData=false
```

7.5 Modifying the JVM memory size

Sabre Red 360 reserves a portion of Java Virtual Memory for dedicated use. Under some circumstances, a specific component – a Red App or the Agency Admin Tools – may need more JVM than what was reserved, impacting the performance.

In these cases, if the server has sufficient spare RAM available then the amount of reserved memory can be changed in the **sabrered.ini** file located in the main installation folder (Common files).

32-bit Default	***Medium Increase***	***Recommended:***
vmarg.1=-Xms128m	vmarg.1=-Xms256m	vmarg.1=-Xms512m
vmarg.2=-Xmx512m	vmarg.2=-Xmx768m	vmarg.2=-Xmx1024m

For the 64-bit version of Sabre Red 360, use the ***Recommended*** settings or even higher.

Caution should be used when updating the sabrered.ini file. Accidentally changing or deleting data in this file can cause errors than can affect all Sabre users on the server. It is recommended to make a copy of the original sabrered.ini file before changing settings.

7.6 Sabre Red 360 Performance

Sabre Red 360 performance is dictated by the resources available to the application, whether the installation guidelines have been followed and the application has full network access through antivirus software, firewalls, proxy servers and network scanners.

Ensuring there is sufficient RAM, CPU, disk speed and network/internet performance will ensure the best performance for the end users. It is recommended that System Administrators monitor their server resources if performance is degraded.

Old versions of Sabre Red Apps have also been seen to cause issues in Sabre Red 360 and it is recommended that the Agency Admin Tool Administrator for each agency ensures that all Red Apps are up to date and old Red Apps are removed.

Please contact your Sabre Technical Specialist if you experience any performance issues with SR360.