

MRU Secure Remote Access Service (SRAS) External User Guide

The MRU Secure Remote Access Service (SRAS) allows MRU approved vendors and external clients, restricted remote access to internal computing resources at MRU.

Supported Client Platforms

Windows Desktop Platform requirements

• Qualified – Indicates that the item was systematically tested by the vendor.

• Compatible – Indicates that the item was not tested for this release, but based on testing done for previous releases, the vendor supports it.

Operating System	Browser/Java	Qualified	Compatible
Windows 8.1 Professional /	Internet Explorer 11		Y
Enterprise, 64-bit	Firefox 24 ESR		
	Google Chrome		
	Oracle JRE 7		
Windows 8 Enterprise, 64-bit	Internet Explorer 10	Y	
	Firefox 24 ESR		
	Google Chrome		
	Oracle JRE 7		
Windows 8 Enterprise, 32-bit	Internet Explorer 10		Y
	Firefox 3.0 and later, including Firefox 10		
	Oracle JRE 6 and later		



Windows 8 basic edition / Professional, 32-bit or 64-bit	Internet Explorer 10		Y
	Firefox 3.0 and later, including		
	Firefox 10		
	Oracle JRE 6 and later		
Windows 7 Enterprise SP1,	Internet Explorer 11,10, 9	Y	
64-DIT	Firefox 24 ESR		
	Google Chrome		
	Oracle JRE 7		
Windows 7 Enterprise SP1,	Internet Explorer 11,10, 9, 8, 7		Y
32-bit	Firefox 3.0 and later, including		
	Firefox 10		
	Oracle JRE 6 and later		
Windows Vista Enterprise /	Internet Explorer 11,10, 9, 8, 7		Y
Ultimate / Business / Home-	Firefox 3.0 and later, including		
bit or 64-bit	Firefox 10		
	Oracle JRE 6 and later		
Windows XP SP3 Home /	Internet Explorer 9, 8, 7		Y
Professional, 32-bit	Firefox 3.0 and later, including Firefox 10		
	Oracle JRE 6 and later		

*On Windows 8.1, 8 platforms the endpoint must use desktop mode and enable plug-ins in the Internet Explorer configuration.



Non-Windows Desktop Platform requirements

Operating System	Browser/Java	Qualified	Compatible
Linux Redhat Enterprise	Firefox 3.0 and later		Y
Linux 5	Oracle JRE 6 and later		
Linux openSUSE 12.1	Firefox 24 ESR	Y	
	Oracle JRE 7		
Linux openSUSE 12.1	Google Chrome		Y
Linux openSUSE 11.x, 10.x	Firefox 3.0 and later		Y
	Oracle JRE 6 and later		
Linux Ubuntu 12.04 LTS	Firefox 24 ESR	Y	
	Oracle JRE 7		
Linux Ubuntu 12.04 LTS	Google Chrome		Y
Linux Ubuntu 11.x, 10.x, 9.10	Firefox 3.0 and later, including		Y
	Firefox 10		
	Oracle JRE 6 and later		
Mac OS 10.9	Safari 7.0		Y
	Oracle JRE 7		
Mac OS X 10.8, 64-bit	Safari 6.0, 5.1	Y	
	Oracle JRE 7		
Mac OS X 10.7.4, 10.6 64-bit and 32-bit	Safari 6.0, 5.1, 5.0		Y



	Oracle JRE 6 and later	
Mac OS X 10.8, 10.7, 32-bit	Safari 6.0, 5.1, 5.0 X	Y
	Oracle JRE 6 and later	

Non-Windows Desktop Platform requirements for Network Connect

Operating System	Browser/Java	Qualified	Compatible
Linux Fedora 12	Firefox 24 ESR	Y	
	Oracle JRE 7, 6		
	Iced-Tea Web 1.2 with OpenJDK 7, 6		
Linux Fedora 12	Google Chrome		Y
Linux openSUSE 12.1	Firefox 24 ESR	Y	
	Oracle JRE 7, 6		
	Iced-Tea Web 1.2 with OpenJDK 7, 6		
Linux openSUSE 12.1	Google Chrome		Y
Linux Ubuntu 12.04 LTS	Firefox 24 ESR	Y	
	Oracle JRE 7, 6		
	Iced-Tea Web 1.2 with OpenJDK 7, 6		
Linux Ubuntu 12.04 LTS	Google Chrome		Y
Mac OS X 10.8, 64-bit	Safari 6.0, 5.1	Y	
	Oracle JRE 7		



Mac OS X 10.7.4, 10.6 64-bit	Safari 6.0, 5.1, 5.0	Y
and 32-bit	Oracle JRE 6 and later	
Mac OS X 10.8, 10.7, 32-bit	Safari 6.0, 5.1, 5.0	Y
	Oracle JRE 6 and later	

Operation Guides

This is a quick starting guide covering the following common operations:

- 1. Accessing the SRAS service
- 2. Using Remote Desktop (RDP) to access a computer inside the MRU network
- 3. Using Network Connect
- 4. Using Two Factors Authentication Access
- 5. Session timeout warnings
- 6. Potential issues

For more details, please refer to the product help page by clicking the



icon on your home page.



1. Access the service

• Enter secure.mtroyal.ca/vendor into the address/URL field of the browser.



- Enter the MRU user name and password given to you by your MRU sponsor.
- Click the Sign button to continue.
- Once you have successfully logged in, your home page will display all the services that SRAS provides you as shown on the next page.



A typical external user home page:

MRU Secure Remote Access Service (SRAS) - Home - Mo	zilla Firefox 📃 🗖 🔀
Elle Edit View Higtory Bookmarks Tools Help	
MRU Secure Remote Access Service (SRAS) +	
S 2 mtroyal.ca https://secure.mtroyal.ca/d	ana/home/index.cgi 🏠 🔻 😋 🚼 🛪 Google 🔎 🏫
🔎 Most Visited 📋 Customize Links 🍞 Track-It 🌘 SANS-ISC 🗍 Sec	curityFocus 🕿 Secunia 🧭 RSA - Envision 🎹 SANS Top Risk 🛛 🔅 👋
MOUNT ROYAL UNIVERSITY 1910	Home Preferences Session O9:59:45 Help Sign Out
	Browse (tips)
Terminal Sessions 🛛 🗧 + 🚽 💌	Client Application Sessions
Windows Management Server - Terra	A Network Connect Start
Windows Management Server - Nova	1

Key elements on your home page:

User Toolbar	Description
	Click to go back to your home page shown above.
Home	
۶	Click to activate the user preference configuration page.
Preferences	
Session	Displays how much longer your session will remain open, as long
09:57:18	as it has not been idle for more than 15 minutes. This example
	shows 9 hours 57 minutes remaining.
Ô	Click to access the online user help manual.
Help	
	Click to sign out of the Juniper connection. Please sign out once
Sign Out	the service is no longer required.



Service Pane	Description
Terminal Sessions	This allows users run Remote Desktop (RDP) to internal MRU computers which they have been granted access to. Sometime this service is referred to as Microsoft Terminal Services.
Client Application Sessions	This provides different levels of VPN/network access into the MRU internal environment.
VPN Service Pane	

2. Remote Desktop (RDP) to a computer inside the MRU network

Note: This is only for a PC running Microsoft Windows. If you have a PC running another operating system, you will have to use the **Network Connect** feature (section 3) and the RDP client of your choice to connect.

• The Terminal Sessions Pane provides you this capability.



• Click the link provided to access the computer if you are using a Microsoft platform. Otherwise, you may need to follow section 3 below.

3. Use Network Connect

• You may need to use the Network Connect service under certain circumstances such as:

You are **not** using a Microsoft Windows based PC. The RDP functions provided on Terminal Sessions Panel may not work as Terminal Services may not be natively supported on the system. If this is the case, you can start the **Network Connect** service and run your **Terminal Services** client of your choice on your system.

• Click the **Start** button in the service pane to start up the service. It will install software on your system. Please follow the on screen instructions to allow the installation.



• Wait until the **Network Connect** icon is fully active (not grayed out) as shown below.

Microsoft Windows:



or



Apple Mac/Linux:



You can double click the icon shown above to see the connection status and disconnect it.

The screen captures shown on the next 2 pages show the expanded icon views for different platforms.



Microsoft Windows:

A Network Connect		
Session		
Connection:	secure.mtroyal.ca	
Status:	Connected	
Duration:	00:00:05	
Bytes Sent:	1,309	
Bytes Received:	300	
Assigned IP:	142.109.17.174	
Security:	AES128/SHA1	
Compression:	None	
Transport Mode:	ESP	
	Hide	Sign Out

Apple Mac:





Linux:



• Once successfully connected, you can launch applications, such as RDP client, on your local computer to access internal MRU computing resources.

4. Two Factors Authentication Access

MRU uses **one-time token** for two factors authentication. The token will be sent by email to the address you have provided to MRU.

You will only need to follow the **Initial setup** procedure once at the beginning. Afterwards, you should only need to follow the **Normal access** procedure after the **Initial setup**.

Initial setup

- 1. MRU's SRAS admin administrator will email you a temporary PIN (Personal Identification Number) needed for the initial connection.
- 2. Using the supported browser as listed in the **Supported Client Platforms** section above to access **secure.mtroyal.ca/vendor/2fa**.

MRU Secure Remote Access Service (SRAS) External User Guide rev 03 Jv8.0 23 Jul 2014 11



3. You should see the welcome screen shown below.

MOUNT R UNIVERSI 1910	OYAL	
Secure100 Usemame Possword Secondary password	Sign In	If you are an authorized user of this service, please sign in with your MRU user id and password. By continuing or by using this service, you agree to the Mount Royal University Computing Resources Acceptable Use a <u>Policy</u> .

Logon with the following information:

Username: The user name given to you by MRU.

Password: The password given to you by MRU. If you already have access, you should use the same password. Please ensure that your access is already enabled by going through the normal access request procedure.

Secondary password: The temporary PIN given by MRU.



4. Once the initial verification is successful, the screen shown immediately below will display asking you to create a new PIN which only you will know. As mentioned in the screen shot below, be sure to remember the PIN and keep it secure as you will need it for future access.

MOUNT ROYAL UNIVERSITY 1910
3 New PIN Required
You must create a new Personal Identification Number (PIN) before you can sign in. Your PIN should be 6 to 8 characters long.
New PIN: Confirm PIN:
Be sure to remember your PIN, because you need it to sign in. If you decide not to create a new PIN now, click Cancel. Save PIN Cancel

Note: The new PIN must contain 6 to 8 alphanumeric characters. Special characters are not supported. Please **do not** reuse the PIN in case it has been reset by MRU.



5. Once the new PIN has been set, the system will ask you to login with you new PIN to receive the one-time token code.

	WAI					
UNIVERSIT	Y					
1910 O						
Secure100 Your new PIN has be followed by the Secur	en saved. Be sure to remember your PIM 1D token code.	L because you need it each time you sign in. To continue logging in, please wait for the code on your SecuriD token to charge and then enter your NEW PIN .				
Usemame	Test_user	If you are an authorized user of this service, please sign in with your MP() user id and password				
Password	•••••	n you are an autorized user of this service, prease sign in with your wirk of user to and password.				
Secondary password		By continuing or by using this service, you agree to the <u>Mount Royal University Computing Resources Acceptable Use</u> Policy.				
	Sign In					

6. At this point, the one-time token code will be emailed to the email address that you have provided to MRU. It could be a personal email address if only one person is using the token code. A group email address will be more appropriate if a group of users need the token code.

The email will be sent from <u>MRU2fa@mtroyal.ca</u> and contains the following information:

On-Demand Tokencode: 11542703 (example code) Expires after use or 60 minutes

The Tokencode is a random number changed at every use.



7. Enter the token code received in the email to the following screen.

MOUNT	[ROYAL				
UNIVI 19	ERSITY DIO ①				
Secure10	00				
Token Re	esync Required				
Please ente	Please enter an additional token code to continue.				
The server requ	The server requires that you enter an additional token code to verify that your credentials are valid. To continue, wait for the token code to change and then enter the new code in the Securit Token Code Feld.				
SecurID To	ken Cude:				
	Enter Cancel				

8. Once the token is authenticated successfully, your normal SRAS home page will be displayed.



Normal access

The initial setup is only required to be performed once. Follow the steps below for access afterwards.

- 1. Using the supported browser as listed in the **Supported Client Platforms** section above to access **secure.mtroyal.ca/vendor/2fa**.
- 2. You should see the welcome screen shown immediately below.

MOUNT ROYAL	
UNIVERSITY 1910 O	
Secure100	
Username	It you are an authorized user of this service please sign in with your MR1 Luser id and password
Password	Provide an experience above of an experience, prease sign in many year mixed above and any presented.
Secondary password	By continuing or by using this service, you agree to the Mount Royal University Computing Resources Acceptable Use Policy.
Sign In	

Logon with the following information:

Username: The user name given to you by MRU.

Password: The password given to you by MRU. If you already have access, you should use the same password. Please ensure that your access has already been enabled by going through the normal access request procedure.

Secondary password: The PIN you set in the Initial Setup procedure above.

3. Once authenticated successfully, your normal SRAS home page will be displayed.



5. Session timeout

SRAS will time out user session which has been idle for more than **15 minutes**.

The system will prompt the user with the following message.

The page at https://secure.mtroyal.ca says:
Your session will expire in 5 minute(s) due to inactivity. Please click [OK] to extend your session.
OK Cancel

Click **OK** to continue. It may ask for your user name and password again. Most of the time the system can resume the last state the user was in when the session was timed out.

Also, the maximum session time for each successful log on is **10 hours** to save system resources.



6. Potential Issues

1. You may see the following or similar pop-up messages, please check the **Always trust/accept** check box and click **Yes** or **Save** to allow the process to finish.



2. Occasionally, you may be asked to save and run the **JuniperSetupClientInstaller.exe** as shown below. Please follow the instructions on screen to complete the installation.

Opening JuniperSetupClientInstaller.exe	X
You have chosen to open	
JuniperSetupClientInstaller.exe	
which is a: Binary File	
from: https://secure100.mtroyal.ca	
Would you like to save this file?	
	Save File Cancel

- 3 Remote desktop issues:
 - a. If you already have been granted RDP access, you may need to reboot your internal system to allow the computer policy to take effect.
 - b. If you do not have RDP access, please contact the MRU Service Desk to request access.



4. To run Net Connect on a supported 64 bits Linux platform. Please follow the instructions on this link:

http://www.juniper.net/techpubs/en_US/sa7.3/topics/reference/general/secure-access-nc-64-bit-linux-support.html

Also xterm is needed to allow the install script to ask for root/sudo password.

5. Please contact your MRU sponsor in case of an access problem.