



Rumba 9.3: Certificate Express Logon

A large, decorative graphic consisting of several overlapping, wavy blue lines that create a sense of motion and depth. The lines are in various shades of blue, from dark to light, and are set against a light blue gradient background.

Quick Start Guide

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK
<http://www.microfocus.com>

Copyright © Micro Focus 1984-2014. All rights reserved.

MICRO FOCUS, the Micro Focus logo and Rumba are trademarks or registered trademarks of Micro Focus IP Development Limited or its subsidiaries or affiliated companies in the United States, United Kingdom and other countries.

All other marks are the property of their respective owners.

2014-11-20

Contents

About Certificate Express Logon	4
Process	4
Security	4
Server support	4
Requirements for Host Configuration	5
Prerequisites for CEL Configuration	6
Preparing a Rumba Session and Macro for CEL	7
Configuring Rumba	7
Recording a macro	7
Editing the macro	8
Selecting the user certificate	12
Testing the macro	13
Distributing the Session Profile	15
Distributing the profile with the selected certificate	15
Distributing the profile to multiple users	15
File locations	16
Contacting Micro Focus	17
Information needed by Micro Focus SupportLine	17
Additional information needed by Micro Focus SupportLine	17
Tell Us What You Think	18

About Certificate Express Logon

Certificate Express Logon (CEL) enables Rumba mainframe display terminals to establish secure TN3270 sessions with mainframe applications. The applications use TN3270 ports that are configured to support CEL services using client security certificates.

Process

When Rumba is used to connect with CEL:

1. Rumba establishes a secure SSL/TLS connection with the TN3270 server, providing a client certificate for user ID logon.
2. After the connection is established and negotiations are complete, a Rumba macro transmits an application ID that is configured on the host for Certificate Express Logons.
3. The Rumba macro updates the host screen with a substitute user ID string `)USR.ID(` and a substitute password string `)PSS.WD(` in place of a typed user ID and password, then presses a key such as **Enter** to transmit the input to the host.
4. The host TN3270 server uses the CEL application ID and the user ID associated with the client security certificate to generate a temporary PassTicket (password) and replaces the `)USR.ID(` and `)PSS.WD(` placeholder strings in the Rumba input with the user ID and PassTicket values.
5. The logon is authenticated and the user application session logon is complete.

Security

When CEL is used, the connection is secured by TLS/SSL negotiation and the communications link is encrypted. In addition, no user ID or password value is transmitted to the host.

Server support

CEL is supported by the following TELNET/TN3270 servers for IBM mainframe z/OS session:

- Communications Server for AIX
- Communications Server for OS/2
- Communications Server for Windows
- Communications Server for z/OS

The TN3270 server that Rumba connects to must also support (VTAM)SNA and maintain TCPIP connectivity as described in the *IBM z/OS Communications Server IP Configuration Guide*.

In a two-tiered security solution, Rumba connects and interacts directly with the IBM z/OS mainframe system. Some system configurations use a three-tiered DCAS security solution in combination with host TCPIP and security services. It is also possible to configure a combined two-tier and three-tier environment. For more information on two- and three-tiered CEL configuration requirements, refer to the appropriate IBM documentation.

Requirements for Host Configuration

To use CEL, the mainframe host must be configured. For up-to-date details, refer to the IBM z/OS documentation.

- RACF must be installed and active on the mainframe.
- The following must be configured on the host TN3270 server port:

- SSL
- EXPRESSLOGON
- CLIENTAUTH SAFCERT
- KEYRING
- SECUREPORT
- CONNTYPE SECURE

- Personal users security certificates (PKCS12 X.509 DER) must be installed in RACF Certificate KEYRING on the host and Rumba client.
- RACF PassTickets must be defined with the applications to be logged onto.
- RACF PassTickets must be defined with the application and user ID or users to log on.

Prerequisites for CEL Configuration

Before configuring a Rumba session for CEL connections, you need the following information:

- The host application name(s) that the Rumba user will logon to.
- The secured PassTicket profile host application name:

For TSO, this is usually `TSO+SysID`. For example, for a TSO logon to SMF System ID SY2, the PassTicket profile host name is `TSOSY2`. If TSO is configured using TSO generic resource names, a different value is required based on the `TCASGNAM` value defined in `SYS1.PARMLIB(TSOKEYxx)` or equivalent library/member. For more information, refer to the *IBM z/OS RACF Security Administrators Guide*.

For most other applications such as CICS or IMS, the PassTicket host profile application name is the same as the value normally typed on logon screens, such as `USSMSG10` for TN3270 servers.



Note: For applications that share user IDs (the same user ID can logon to the same application multiple times and at the same time, and the application must support this), specify `APPLDATA('NO REPLAY PROTECTION')` in the RACF `RDEFINE` command used to create the PassTicket `PTKTDATA` profile for the application. Failure to do so can result in user lockout or logon failures.

- A user ID and password to log onto the host application:

This user ID must have access to the same applications, logon screens, and negotiation processes as all the users for whom you might distribute a prepared Rumba configuration package for CEL secured logons. A Rumba macro requires the same screens and sequences for all users of the same macro. If security or access rules change the screens used to logon based on the user or host system management, or if administration changes, multiple profile/macro packages might be required for distribution.

- User certificates:

The IBM host RACF database must have user security certificates installed in `KEYRINGS` and available to the host applications and to the TELNET server that will substitute placeholder strings for PassTicket application profiles and users. The database must also have access to the stored user certificates.

For more information, refer to the following:


- *IBM z/OS RACF Security Administrators Guide*
- *RACF Command Language Reference*
- *z/OS Communications Server IP Configuration Guide*
- TSO HELP RACDCERT

Rumba has been tested with certificates in DER PKCS12 format.

Preparing a Rumba Session and Macro for CEL

This section describes how to configure a Rumba session and record a macro for a CEL session.

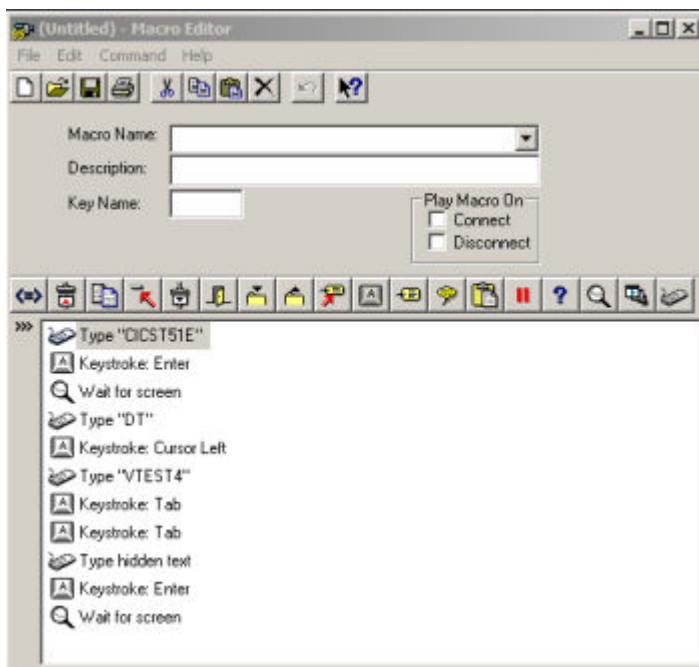
Configuring Rumba

1. Start Rumba.
2. Open a new mainframe session.
3. From the menu bar, select **Connection > Configure**.
The **Connection Configuration** dialog box appears.
4. In the **Installed Interfaces** box, select **TN3270**.
5. Select the model from the **3270 Startup Model** list.
6. Click the **TN3270** tab.
7. Next to the **Destination Name/Address** box, click **Insert**. The **TELNET: New IP Name/Address** dialog box appears.
8. In the **Destination Name/Address** box, type the host name or IP address, then click **OK**.
9. In the **Telnet Port** frame, select **User Defined** and set the port (if it is not default port 23).
 **Note:** This port is the EXPRESSLOGON port described in [Requirements for host configuration](#).
10. Click the **TN3270 Advanced** tab.
11. Do not check **Certificate Express Logon (CEL)**.
12. Click **Advanced Parameters**.
13. Do not click **Client Certificate**.
14. Check **SSL/TLS**.
15. Click **OK**.
16. Click **OK** again to close the **Connection Configuration** dialog box.

Recording a macro

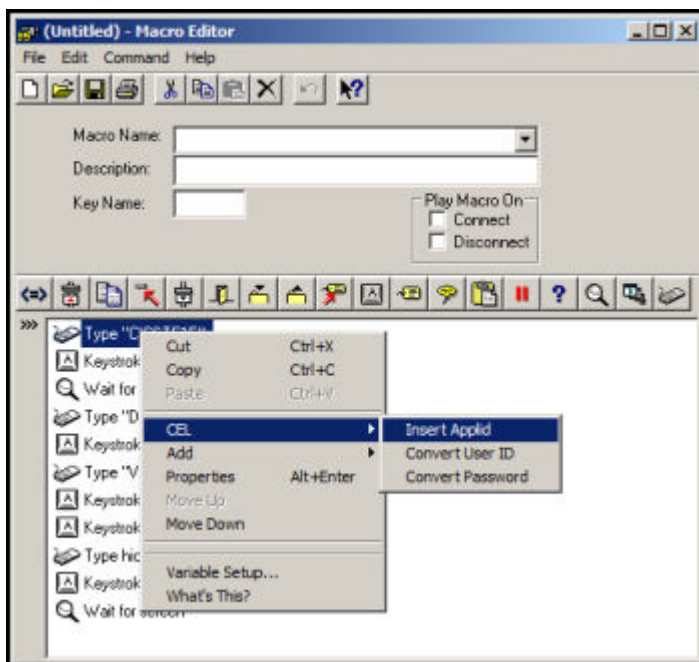
1. From the menu bar, select **Connection > Connect**.
2. Do one of the following:
 - If the logon process to be automated and distributed begins at the first screen, select **Tools > Record Macro**.
 - If the logon process to be automated and distributed does not start with the first screen, navigate to the desired screen, then select **Tools > Record Macro**.
3. Enter the application name, an actual user ID and password, and continue until the desired application screen is reached (logon complete).
4. To stop recording, select **Tools > Record Macro**.

The **Macro Editor** window appears:

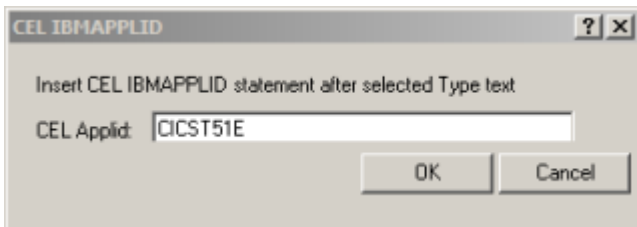


Editing the macro

1. In the **Macro Editor** window, right-click the `Type` statement for the application ID and select **CEL > Insert Applid** from the pop-up menu:



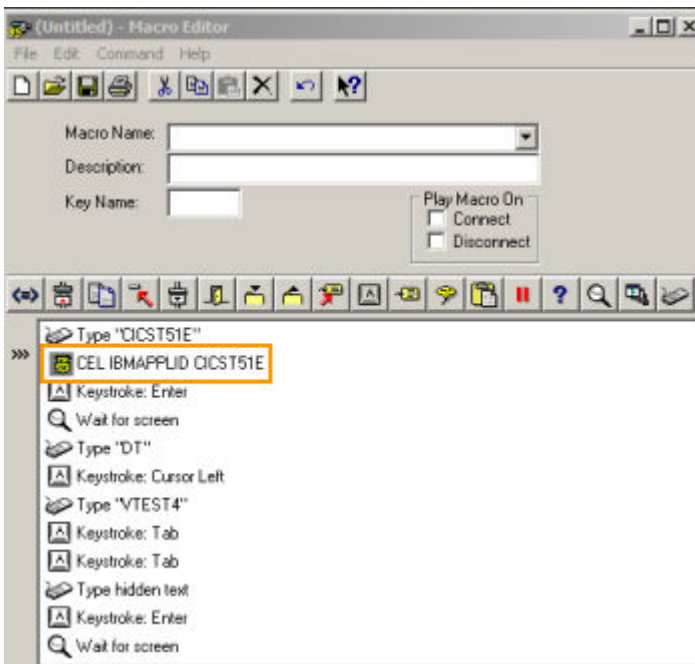
The **CEL IBMAPPLID** dialog box appears:



2. Do one of the following:

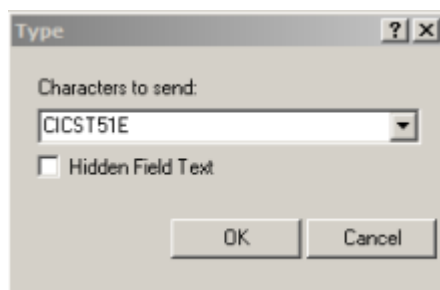
- If the applid in the **CEL Applid** box is the same as the PassTicket application name (see [Requirements for host configuration](#)), click **OK**.
- If the applid in the **CEL Applid** box is not the same as the PassTicket application name, change the applid to match the host PassTicket information, then click **OK**.

The CEL applid statement is inserted:

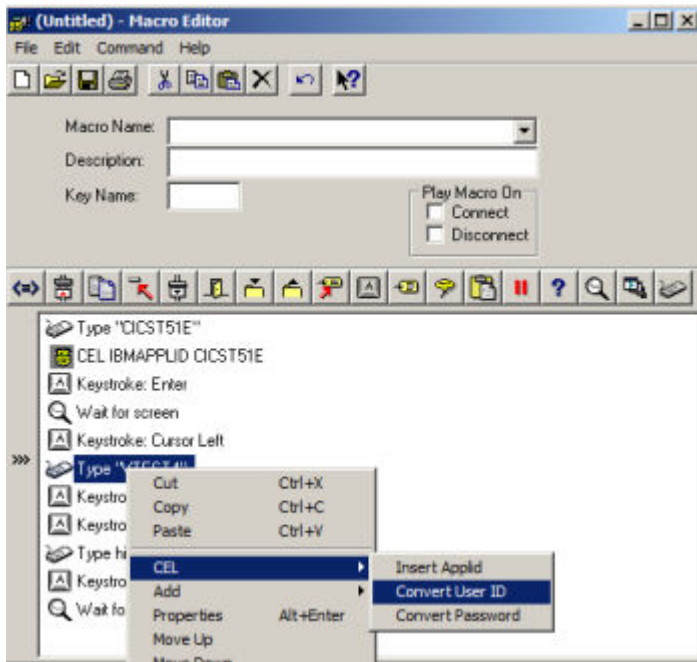


Note: If the negotiations did not type the application ID, but perhaps pressed a PF or PA key for example, insert a temporary `Type` statement at the top of the recording:

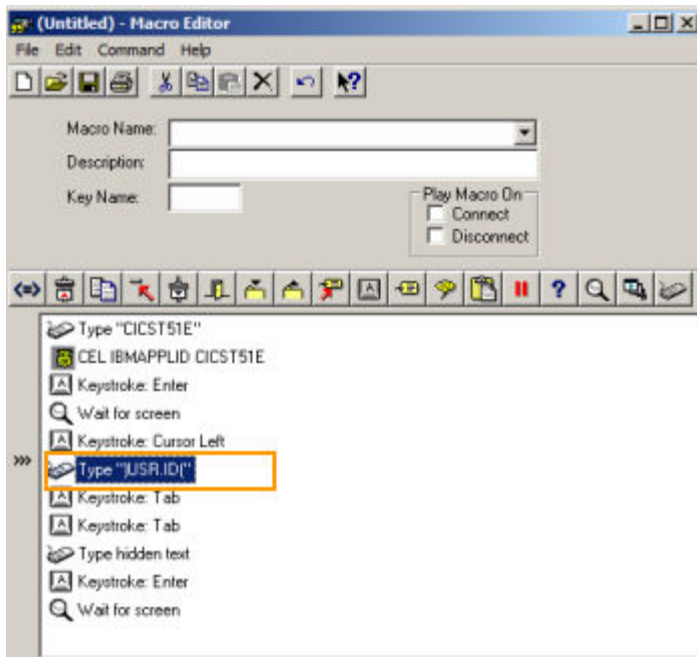
1. Right-click and select **Add > Type** from the pop-up menu, then provide the actual host application ID string (matching the PassTicket ID) as shown and click **OK**:



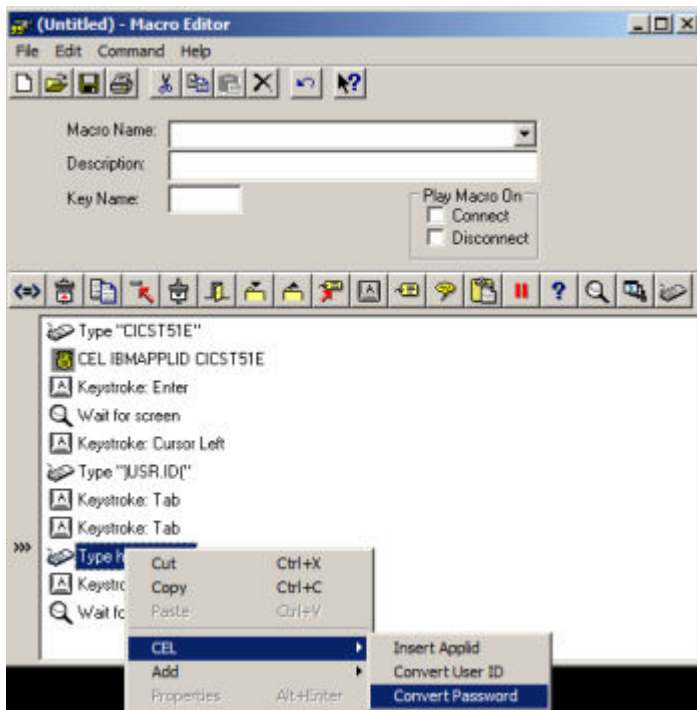
2. Follow the instructions above to insert a CEL applid statement.
 3. Select the inserted `Type` statement and press **Delete**.
3. Right-click the `Type` statement for the user ID you provided and select **CEL > Convert User ID** from the pop-up menu:



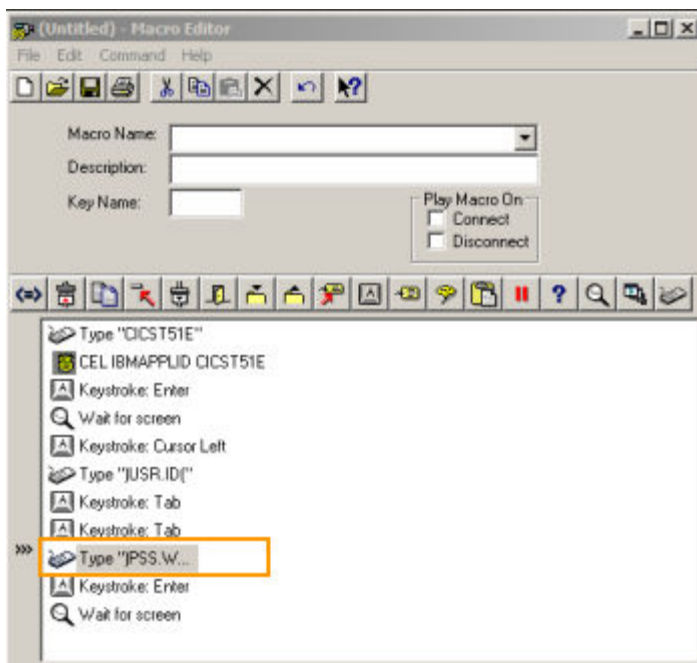
The substitute user ID string is inserted:




4. Right-click the `Type hidden text` statement where the user password was typed and select **CEL > Convert Password** from the pop-up menu:



The substitute password string is inserted:



 **Note:** If the field where you typed the user ID is 8 characters wide and has an autoskip attribute at the end, you might have recorded an extra `Keystroke: Tab` statement in the macro if the user ID you typed is less than 8 characters long. As shown in the example above, there are two `Tab` statements.

Because the inserted placeholder string is 8 characters long, the autoskip function is activated and the cursor tabs to the next field. When the actual recorded `Keystroke: Tab` statements are executed, the typed text (password) will be in wrong field. This will not be obvious until you try to play the macro, when you will see that the password text can be typed into an incorrect screen

field. To resolve this problem, select the `Keystroke: Tab` statement following the `Type)USR.ID(` statement and delete it.

5. Enter a macro name.

You might want to include the application ID name and, perhaps, the host name to help distribution and administration/support because this macro will be used by Rumba clients to log onto the application securely.

6. Optional: If you want this macro to run automatically for the current session when the user connects the session, check **Play Macro On Connect**.
7. Select **File > Save**.

To find and distribute macros later, save the location which defaults to `%AppData%\Local\Microsoft\Focus\Rumba\MFrame\Macro` or choose a new location for administering CEL macros for distribution.

8. Select **File > Exit**.
9. If the session is still connected, select **Connection > Disconnect**.

Selecting the user certificate

1. Select **Connection > Configure**.

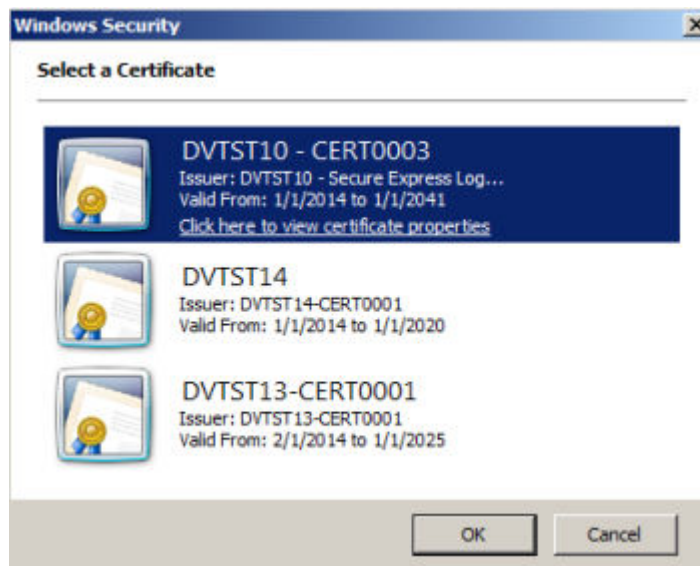
The **Connection Configuration** dialog box appears.

2. Click the **TN3270 Advanced** tab.
3. Check **Certificate Express Logon (CEL)**.

The **CEL Configuration** message box appears.

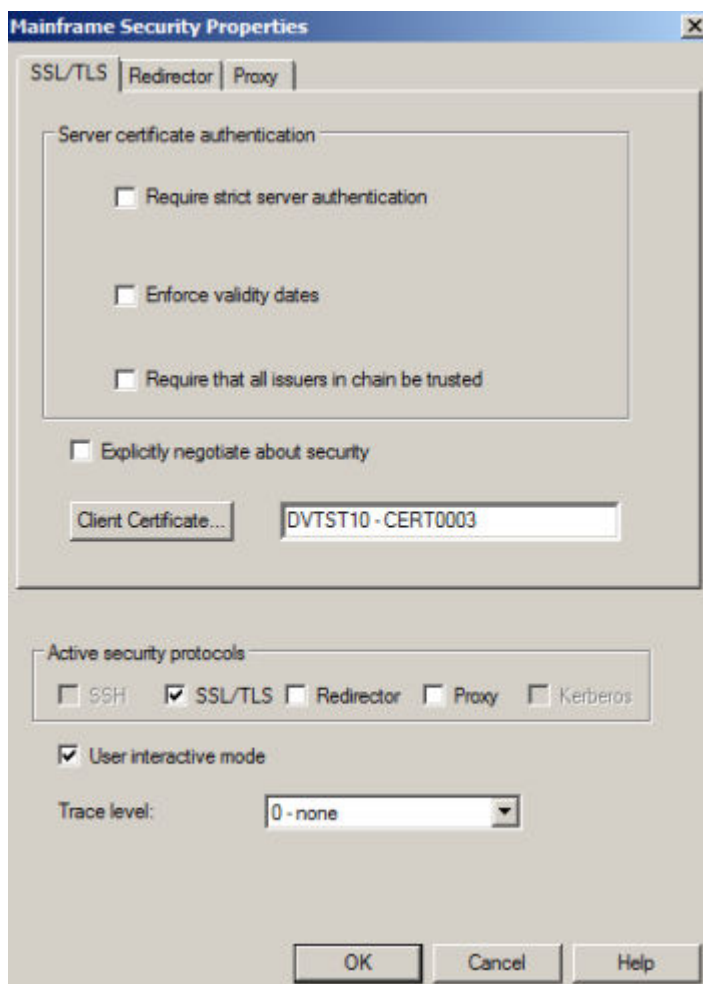
4. Click **OK**.
5. Click **Advanced Parameters**. The **Mainframe Security Properties** dialog box appears.
6. Click **Client Certificate**.

The **Select a Certificate** window appears:



7. In the **Select a Certificate** window, select a certificate and click **OK**.

The certificate name appears in the **Client Certificate** box:

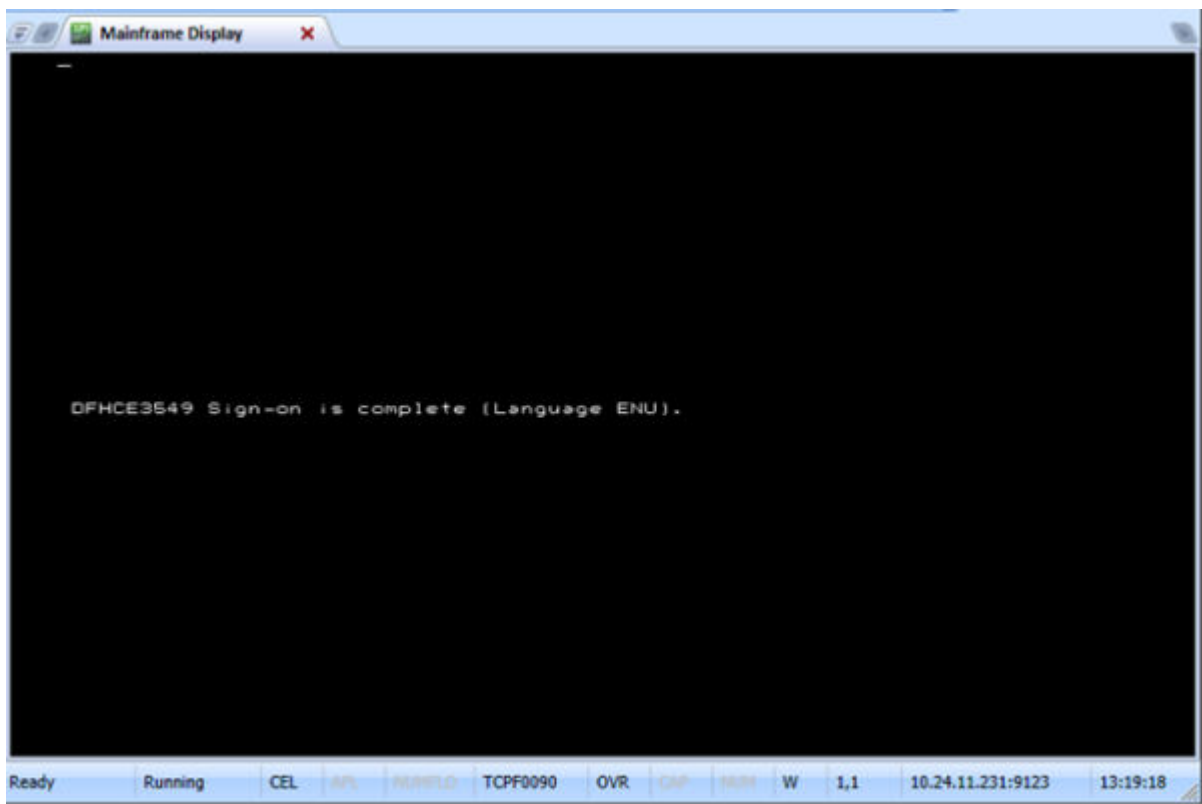


8. Click **OK** to close the **Mainframe Security Properties** dialog box.
9. Click **OK** again to close the **Connection Configuration** dialog box.

Testing the macro

1. Select **Connection > Connect**.

Connection proceeds. The macro navigates through the screens and stops running at the logon complete / macro complete screen. The figure below shows an example of a CICS logon:



2. Select **Connection > Disconnect**.

If you did not assign the new macro as auto connect:

1. Navigate to the correct screen.
2. Select **Tools > Run Macro**.
3. Select the macro in the **Select Macro to Run** dialog box, then click **OK**.

You can add or remove the macro as the auto connect macro for the session by selecting **Tools > Macro Properties**. In the **Macro Property Page** dialog box, select the macro to add it to the **Connect Macro** field, or delete the macro from the **Connect Macro** field. You can use this process to reset the default (unsaved) profile, created when you started the new mainframe session.

Distributing the Session Profile

When you have created the session profiles and CEL macros, you can distribute them to users with instructions for installing the updated files.



Notes:

- Users should install certificates before they connect to CEL-secured Rumba sessions (with macros).
- After working with CEL and macro configurations, it might be necessary to reset the macro connect setting and the configuration settings (CEL/SSL Certificate and so on) for new default Rumba sessions.

Distributing the profile with the selected certificate

To distribute the session profile as configured with the specific certificate you selected:

1. Select **File > Save Session Profile As**.
2. In the **Save Session Profile** dialog box, choose the folder where you want to keep and administer user profiles.
3. In the **File name** box, type a profile name. It might be helpful to include the host or application name to help with later support investigations or instructions to users, for example.
4. Click **Save**.

Distributing the profile to multiple users

To distribute the session profile to multiple users and have the user select the client certificate (if multiple certificates are installed on the client machine) when they connect:

1. Select **Connection > Configure**.
2. Click the **TN3270 Advanced** tab.
3. Click **Advanced Parameters**.
4. Click **Client Certificate** and select the certificate name.
5. Press **Delete** to remove the certificate name.



Notes:

- Rumba automatically uses a single client certificate if only one certificate is installed on the client. If multiple certificates are installed and if the `<default>` value is set in the session profile, the **Select a certificate** dialog box appears when the user connects.
 - If a user initially has only one certificate, Rumba uses it but, if the user later installs more certificates, the **Select a Certificate** dialog box appears.
 - If the user, as part of the setup process, is instructed to select the certificate that is distributed, the **Select a certificate** dialog box does not appear when connecting.
6. Click **OK**.
 7. Create a session profile with the default certificate setting.

If a user has multiple certificates/multiple logons, that is they log onto two different applications or log onto the same application with two different user IDs, they might require two user client certificates and two separate sessions. Only one certificate can be used per connection.

There are also host configurations that support multiple users sharing a single certificate . In this case, the same certificate would be installed for each client user. Refer to your host security documentation to determine if the target applications support multiple users sharing certificates and any special PassTicket or certificate configuration actions that might be required.

File locations

By default (on Windows 7 and 8.x), Rumba stores and accesses user session profiles in the following locations:

This file type ...	Is stored here ...
Session profile	%AppData%\Local\Micro Focus\Rumba\Mframe\ <i><profile_name></i> .rsdm
Macro	%AppData%\Local\Micro Focus\Rumba\Mframe\Macro\ <i><macro_name></i> .rnc

These folders can be used as the target locations for Rumba session profiles and macros.

Contacting Micro Focus

Micro Focus is committed to providing world-class technical support and consulting services. Micro Focus provides worldwide support, delivering timely, reliable service to ensure every customer's business success.

All customers who are under a maintenance and support contract, as well as prospective customers who are evaluating products are eligible for customer support. Our highly trained staff respond to your requests as quickly and professionally as possible.

Visit <http://supportline.microfocus.com/assistedservices.asp> to communicate directly with Micro Focus SupportLine to resolve your issues or e-mail supportline@microfocus.com.

Visit Micro Focus SupportLine at <http://supportline.microfocus.com> for up-to-date support news and access to other support information. First time users may be required to register.

Information needed by Micro Focus SupportLine

When contacting Micro Focus SupportLine, please include the following information, if possible. The more information you can give, the better Micro Focus SupportLine can help you.

- The name and version number of all products that you think might be causing an issue.
- Your computer make and model.
- System information such as operating system name and version, processors, and memory details.
- Any detailed description of the issue, including steps to reproduce the issue.
- Exact wording of any error messages involved.
- Your serial number. To find this number, look in the subject line and body of your Electronic Product Delivery Notice e-mail that you received from Micro Focus.

Additional information needed by Micro Focus SupportLine

If reporting a protection violation, you might be asked to provide a dump (.dmp) file. To produce a dump file, use the **Unexpected Error** dialog box that is displayed when a protection violation occurs.

Unless requested by Micro Focus SupportLine, leave the dump setting as `Normal` (recommended), click **Dump**, then specify a location and name for the dump file. Once the dump file has been written, you can e-mail it to Micro Focus SupportLine.

You may also be asked to provide a log file created by the Consolidated Tracing Facility (CTF) - a tracing infrastructure that enables you to quickly and easily produce diagnostic information detailing the operation of a number of Micro Focus software components.

Tell Us What You Think

We welcome your feedback regarding Micro Focus documentation.

[*Submit feedback regarding this Help*](#)

Click the above link to e-mail your comments to Micro Focus.