VIRTEL How To ...

User's Guide

Version : 4.56

Release Date : 1 Sep 2016

Publication Date : 21/11/2016

Syspertec Communication
196, Bureaux de la Colline 92213 Saint-Cloud Cedex
Tél. : +33 (0)1 46 02 60 42
www.syspertec.com

NOTICE

Every possible effort has been made by SysperTec Communication to ensure that this document is complete and relevant. In no case can SysperTec Communication be held responsible for any damages, direct or indirect, caused by errors or omissions in this document.

As SysperTec Communication uses a continuous development methodology; the information contained in this document may be subject to change without notice. Nothing in this document should be construed in any manner as conferring a right to use, in whole or in part, the products or trademarks quoted herein.

Table of contents

1. Virtel Web Access 5

1.1. VWA User Interface 5

1.1.1. Toolbar 6

1.1.2. Status line 16

1.2. Dynamic Directory Interface (DDI) 18

1.2.1. "Your VIRTEL is not configured for dynamic directories" 18

1.2.2. HTTP 404 or 406 while accessing directory 19

1.2.3. User have no access to the macro stored in DD 20

1.2.4. GLOBAL macros are avalaible but not to the GROUP or USER 20

1.2.5. No access to the Local Storage when using Dynamic Directories 21

2. Lines 22

2.0.6. Starting and stopping a line 22

3. Terminal 24

3.1. Controling LU Names 24

3.1.1. LU nailing using the work station name (Predefined terminals) 24

3.1.2. LU nailing using an LU name (Predefined Terminal) 28

3.1.3. Lu Nailing using an LU Name (No predefined terminal) 28

3.1.4. Lu Nailing using a cookie (Correspondent Sub Application) 30

3.1.5. LU Nailing by IP 31

4. Transactions & Applications 33

4.1. Virtel Multisession within Virtel Web Access 33

4.2. How to access a host application directly 34

4.2.1. Full path URL 34

4.2.2. Default URL for the entry point 34

4.3. How to use different screen sizes 35

4.3.1. LOGMODE defined by the transaction 35

4.3.2. Assigning a LOGMODE by URL parameter 36

4.3.3. User-specified LOGMODE 37

4.3.4. Dynamic logmode with user-specified screen size 38

4.4. Session management in the Application Menu List 38

4.4.1. Open session in separate tab 38

4.5. How to handle host session termination 39

4.5.1. Return to the application selection menu 39

4.5.2. Displaying a specific page on disconnection 39

4.5.3. Closing the browser window automatically 39

5. Security 41

5.1. How to activate SSL using AT-TLS 41

5.1.1. Installation steps 41

5.1.2. Operations 42

5.1.3. Problem determination 42

5.1.4. Bibliography 43

5.2. SSL - Signing on using server and client certificates 44

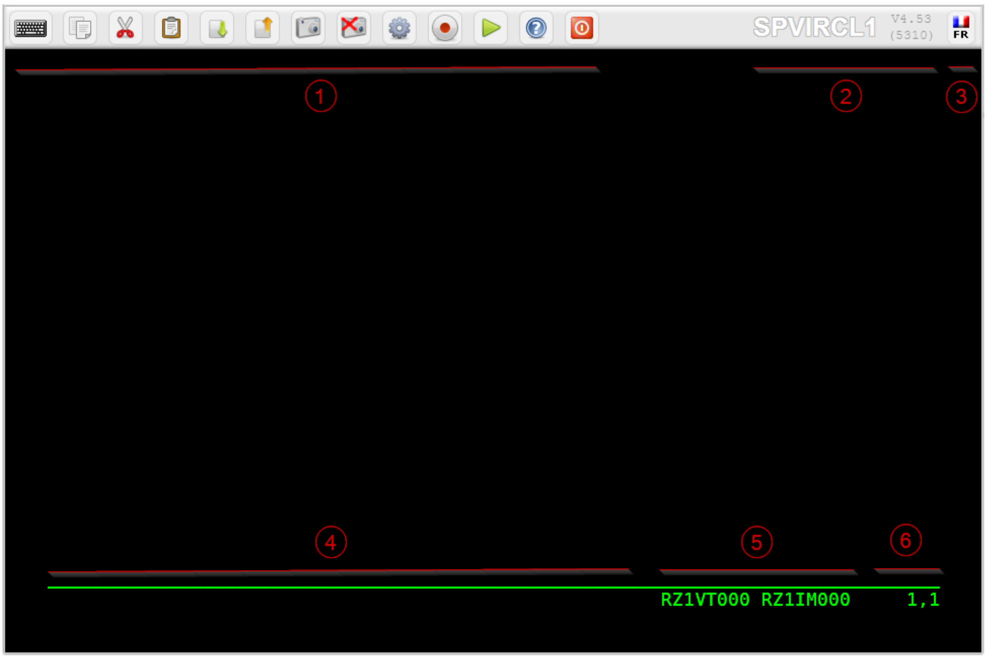
5.2.1. Certificates 44

1. Virtel Web Access

1.1. VWA User Interface

The VIRTEL Web Access user interface is in the form of a conventional 3270 screen divided into three areas:

- The toolbar located in the upper of the screen contains the icons of functions (1), the information envrionment (2), the language selection (3).
- The status line at the bottom includes the monitiring zone (4), particulars of the terminals associated with the session (5), mode and cursor position (6).
- The area between the toolbar and the status bar is used to display the contents of 3270 screens, it can be of variable size between 24x80 and 62x132.



The VWA 3270 screen's areas

1.1.1. Toolbar

The toolbar is located at the top of the 3270 screen. It contains, icons, language selection tool and environment information. Some of those component can be removed, added or modified.

1.1.1.1. How to hide the toolbar

The administrator may wish to prevent users from accessing features like copy/paste, print, and settings by removing correponding icons, or by hidding the toolbar. This example shows how to hide the toolbar using a custom.css file:

```
/* VIRTEL Web Access style sheet for site customization
 * (c)Copyright SysperTec Communication 2007,2010 All Rights Reserved
 */

 #toolbar {display:none;}/*
```

Example custom.css for hiding the toolbar

You can also use custom.js to remove icons individually from the toolbar, see "Removing unwanted toolbar icons", page 9.

1.1.1.2. Changing background color of the toolbar buttons

This example shows how to change the backgroung color of the toolbar buttons by adding orders in the custom.css file:

```
/*
 * VIRTEL Web Access style sheet customisation the background of the toolbar
 * buttons(c)Copyright SysperTec Communication 2014 All Rights Reserved
 */
  |- transparent "at rest"
  |- white when cursor moves on
  |- yellow when button is clicked

 #toolbar td .tbButton {
  background-color: inherit;
 }
 #toolbar td .tbButton:hover {
  background-color: white;
 }
 #toolbar td .tbButton:active {
  background-color: yellow;
 }

  | To remove the background color and the border of buttons "at rest":

 #toolbar td .tbButton {
  background-color: inherit;
  border: 1px solid transparent;
 }
```

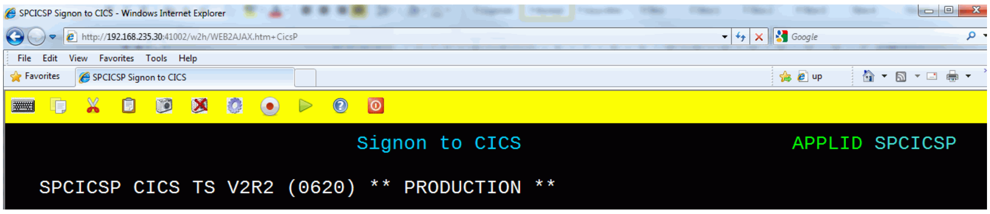
Example custom.css managin the background color of the toolbar buttons

1.1.1.3. Customizing the toolbar color by application

It is sometimes useful for the user to have a clear visual indication of which system he or she is logged on to. This example shows how to set the color of the toolbar to yellow for SPCICSP and pink for SPCICSQ.

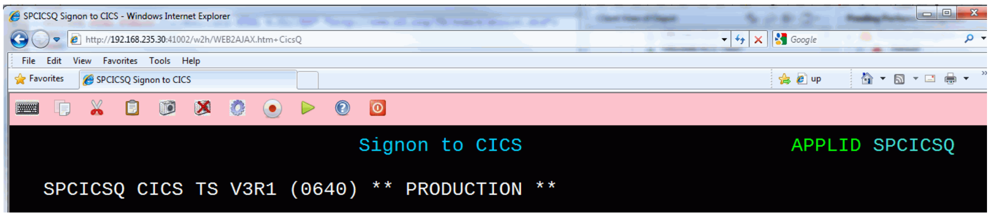
```
/* VIRTEL Web Access style sheet for site customization
 * (c)Copyright SysperTec Communication 2007,2010 All Rights Reserved
 */

 .SPCICSP #toolbar {background-color:yellow;}
 .SPCICSQ #toolbar {background-color:pink;}
```

Example custom.css for coloring the toolbar according to CICS region


SPCICSP Signon to CICS - Windows Internet Explorer
http://192.168.235.30:41002/w2h/WEB2AJAX.htm+CicsP
Google
File Edit View Favorites Tools Help
Favorites
SPCICSP Signon to CICS
up

```
                     Signon to CICS                      APPLID SPCICSP

  SPCICSP CICS TS V2R2 (0620) ** PRODUCTION **
```

Web Access screen with yellow toolbar for SPCICSP


SPCICSQ Signon to CICS - Windows Internet Explorer
http://192.168.235.30:41002/w2h/WEB2AJAX.htm+CicsQ
Google
File Edit View Favorites Tools Help
Favorites
SPCICSQ Signon to CICS
up

```
                     Signon to CICS                      APPLID SPCICSQ

  SPCICSQ CICS TS V3R1 (0640) ** PRODUCTION **
```

Web Access screen with pink toolbar for SPCICSQ

1.1.1.4. Add a web link in the toolbar

You can add a web link in the toolbar by using the following order included in a custom.js file:

```
function after_standardInit() {
    * Adds a button to the toolbar which performs a Google search
    addtoolbarbutton(position, "http://www.yourtargetsit.com/favicon.ico",
    "Title", linked_function);
}
```

Example to add a web link in the toolbar.

1.1.1.4.1. Example : Add a Google Search link in the toolbar

```
function after_standardInit() {
    /*
    * Adds a button to the toolbar which performs a Google search for
    * the text selected in the red box in the 3270 screen, or for the
    * word at the cursor if no box is drawn
    */
    addtoolbarbutton(999, "http://www.google.com/favicon.ico",
    "Search engine query", do_search);
}

function do_search() {
    var searcharg = VIR3270.getBoxedText() || VIR3270.getWordAtCursor();
    var windowname = "search";
    var searchURL = "http://www.google.com";
    if (searcharg) searchURL += "/search?q=" +
    encodeURIComponent(searcharg.replace(/\s+/g, ""));
    var windowopts = "location=yes,status=yes,resizable=yes," +
    "scrollbars=yes,toolbar=yes,menubar=yes,width=640,height=480";
    var searchwin = window.open(searchURL, windowname, windowopts);
    if (searchwin) searchwin.focus();
}
```

1.1.1.5. Adding a company logo

This example shows how to display an icon (for example, a company logo) at the left of the toolbar:

```
/*
 * VIRTEL Web Access style sheet customisation for company logo
 * (c)Copyright SysperTec Communication 2012 All Rights Reserved
 */

 #toolbar td#companyIcon {
  height:30px;
  display:table-cell;
 }

 #companyIcon div {
  background-image:url("/w2h/virtblue.jpg");
  background-position:0px -4px;
  background-repeat:no-repeat;
  height:26px;
  width:145px;
 }
```

Example custom.css for displaying company logo in the toolbar

This example shows how to replace the Virtel logo in the VIRTEL Web Access menu and the Application menu by your company logo:

```
/*
 * VIRTEL Web Access style sheet for site customisation
 * (c)Copyright SysperTec Communication 2013 All Rights Reserved
 * $Id$
 */

 #appmenulogo {
  background-image: url("mycompany.gif");
  height: 65px;
  width: 266px;
 }
```

Example custom.css for replacing the Virtel logo by a company logo

Note: If no explicit path is given, the company logo will be loaded from the same directory as the custom.css file.

1.1.1.6. Icons

1.1.1.6.1. Adding a toolbar icon

This example uses the after_standardInit function to insert additional icons into the toolbar when the session is started. Icons may subsequently be added or removed from the toolbar after each screen by means of the after_responseHandle function.

```
/*
 * (c)Copyright SysperTec Communication 2012 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions
 */
```

```
/*
 * Adds a button to the toolbar which performs a Google search for
 * the text selected in the red box in the 3270 screen, or for the
 * word at the cursor if no box is drawn
 */
function after_standardInit() {
  addtoolbarbutton(999, "http://www.google.com/favicon.ico",
    "Search engine query", do_search);
}
function do_search() {
  var searcharg = VIR3270.getBoxedText() || VIR3270.getWordAtCursor();
  var windowname = "search";
  var searchURL = "http://www.google.com";
  if (searcharg) searchURL += "/search?q=" +
    encodeURIComponent(searcharg.replace(/\s+/g," "));
  var windowopts = "location=yes,status=yes,resizable=yes,"+
    "scrollbars=yes,toolbar=yes,menubar=yes,width=640,height=480";
  var searchwin = window.open(searchURL, windowname, windowopts);
  if (searchwin) searchwin.focus();
}
```

Example custom.js to customize the toolbar icons

1.1.1.6.2. Removing unwanted toolbar icons

This example uses the after_standardInit function to disable macro functions by removing the corresponding icons from the toolbar.

```
/*
 * (c)Copyright SysperTec Communication 2012 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions
 */

function after_standardInit() {
  /* Remove macro buttons from the toolbar */
  removetoolbarbutton("startrecording");
  removetoolbarbutton("playback");
}
```

Example custom.js to remove selected toolbar icons

The names of the other toolbar icons which can be removed in this way are:

- capture,
- disconnect,
- document-print-preview,
- edit-copy,
- edit-cut,
- edit-paste,
- emptybuf,
- file-rcv,
- file-send,
- help,
- keypad,
- playback,
- printer,
- settings,

- settingsV2,
- startrecording.

(settingsV2 is présent only if w2hparms.js contains "settingsGUI":{"version":"V2"}, or "settingsGUI":{"version":"V1+V2"},)

To hide the toolbar completely, see “Hiding the toolbar”, page 6.

To hide only the Virtel Application name, see “Showing / Hiding server informations”, page 14.

1.1.1.6.3. Removing file transfer icons

VIRTEL Web Access supports transfer of files between the browser and a TSO session using the IND$FILE protocol. The function is activated displayed only for the transaction defined with the SCENINDT scenario entered in Input and Output scenario fields. For some specific users, it may be necessary to remove the file transfer icons from the toolbar. This can be done by using the removetoolbarbutton function using the appropriate variable name.(See “Removing unwanted toolbar icons”, page 9.)

1.1.1.6.4. Removing macro icons

Icons for recording or executing a Macro are automatically present in the toolbar. To make them unavailable you should use the removetoolbarbutton function using the appropriate variable name.(See “Removing unwanted toolbar icons”, page 9.)

1.1.1.6.5. Positionning toolbar icons

In certain circumstances, the default position of an icon may not be at the user's convenence. Is possible to change an icon's position based on the position of another icon.

```
/*
* Customize the location of dynamic toolbar buttons.
* The calls to this function are ignored when they
* return nothing, or an integer not greater than 0.
*
* Customizable buttons IDs :
*  > '3278T'
*  > 'document-print-preview'
*  > 'file-send'
*  > 'file-recv'
*  > 'printer'
*/
function customize_toolbarButtonIndex(id) {
  if (id==='printer' || id==='document-print-preview') {
    return getToolbarButtonIndex('disconnect') + 1;
  }
}
```

Example custom.js to select a position for printer icon

1.1.1.6.6. Centering non standard icons

The best size for an icon is 32x32 pixels. For bigger or smaller icons, it possible to offer better center rendering in modifying the content of the class attribut passed within the "addtoolbarbutton" function in conjunction of using a specific css attribut.

```
/*
 * (c)Copyright SysperTec Communication 2014 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions
 * Resizing a too small or too big toolbar icon.
 * For example toosmall_pic.png=22x22 and toobig_pic.jpg=145x30
 */

  addtoolbarbutton(999, "/w2h/toosmall_pic.png", "Custom button #1 tooltip",
                   do_search, "tbButton size22x22");
  addtoolbarbutton(999, "/w2h/toobig_pic.jpg",  "Custom button #2 tooltip",
                   do_search, "tbButton size145x30");
```

Example custom.js to specify the toolbar icon size

```
/*
 #toolbar td img.tbButton.size22x22 {
   width: 22px;
   height: 22px;
   padding: 5px; /* padding is calculated to center the picture horizontaly
                 and verticaly in the 32x32 allocated area. (5+22+5 = 32) */
 }

 #toolbar td img.tbButton.size145x30 {
   width: 145px;
   height: 30px;
   padding: 1px 0; /* padding is calculated to center the picture verticaly
                     in the 32x32 allocated area (1+30+1 = 32) without any
                     horizontaly padding */
 }
```

Example custom.css to manage a toolbar icon with a non standard size

1.1.1.6.7. Removing 3D/hover effects on the toolbar buttons

This example shows how to remove the 3D/hover effects on toolbar buttons by adding orders in the custom.css file:

```
/*
 * VIRTEL Web Access style sheet customisation for removing 3D/hover effects
 * (c)Copyright SysperTec Communication 2014 All Rights Reserved
 */

 #toolbar td .tbButton,
 #toolbar td .tbButton:hover,
 #toolbar td .tbButton:active {
  background-color: inherit;
  border: inherit;
  box-shadow: inherit;
 }
```

Example custom.css for removing 3D/hover effects on buttons

1.1.1.6.8. File Transfer Icons

1.1.1.6.8.1. Add or remove File Transfer icons

The File Transfer icons are present in the toolbar only for access to TSO and if the transaction includes an INPUT and/or OUTPUT scenario with a call to the INDSCEN$ macro (See "TSO File Transfer" in "Virtel Web Access User Guide").

1.1.1.6.8.2. Removing file transfer icons

VIRTEL Web Access supports transfer of files between the browser and a TSO session using the IND$FILE protocol. The function is activated displayed only for the transaction defined with the SCENINDT scenario entered in Input and Output scenario fields. For some specific users, it may be necessary to remove the file transfer icons from the toolbar. This can be done by using the removetoolbarbutton function using the appropriate variable name.(see “Removing unwanted toolbar icons”, page 9.)

1.1.1.6.9. Macro Icons

1.1.1.6.9.1. Removing Macro icons

(See “Removing unwanted toolbar icons”, page 9.)

1.1.1.6.10. Troubleshooting

1.1.1.6.10.1. Icon display troubleshooting

If some icons on the toolbar are displayed with some parasites on the border, please check that the browser is not in a zoom mode greater than 100%.

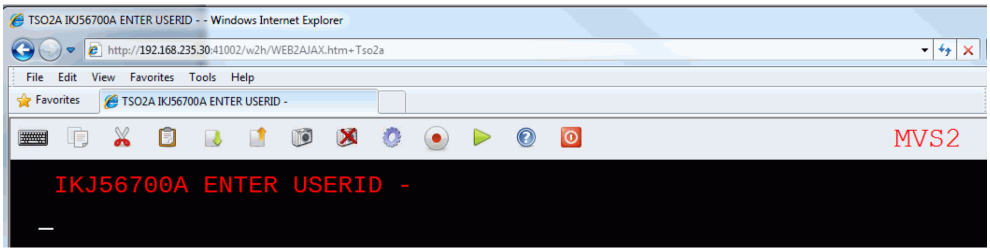
1.1.1.7. Background information

1.1.1.7.1. Adding custom text by application to the toolbar

Another way of providing a clear visual indication of which application the user is logged on to is to add a text label to the toolbar. In this example the text “MVS1” is displayed when logged on to application TSO1A, and “MVS2” is displayed for application TSO2A.

```
/*
* VIRTEL Web Access style sheet for site customisation
* (c)Copyright SysperTec Communication 2007,2010 All Rights Reserved
*/
.toolbarLast{
text-align: right; /* Text alignement */
}
.TSO1A .toolbarLast:before {
content: "MVS1";
opacity: 0.25;
font-size: 30px;
width: 100%;
z-index: 1000;
-webkit-text-stroke: 1px blue; /* Select color */
padding-right: 5px;            /* To separate cells */
}

.TSO2A .toolbarLast:before {
content: "MVS2";
opacity: 0.25;
font-size: 30px;
width: 100%;
z-index: 1000;
-webkit-text-stroke: 1px red;  /* Select color */
padding-right: 5px;            /* To separate cells */
}
```

Example custom.css for adding custom text to the toolbar


TSO2A IKJ56700A ENTER USERID - - Windows Internet Explorer
http://192.168.235.30:41002/w2h/WEB2AJAX.htm+Tso2a
File
Edit
View
Favorites
Tools
Help
Favorites
TSO2A IKJ56700A ENTER USERID -
MVS2

```
IKJ56700A ENTER USERID -
_
```

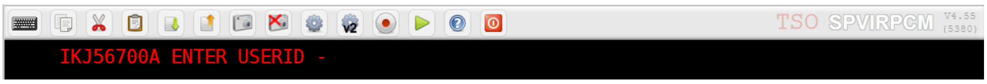
Web Access screen with custom text in the toolbar

1.1.1.7.2. Adding application name to the toolbar

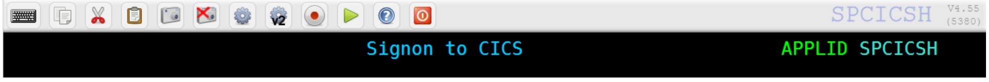
Another way of providing a clear visual indication of which application the user is logged on to is to add the application name label to the toolbar. In this example the text “TSO” is displayed when logged on to application TSO, and “SPCICSH” is displayed for application SPCICSH.

```
/*
* VIRTEL Web Access style sheet for site customisation
* (c)Copyright SysperTec Communication 2007,2010 All Rights Reserved
*/
.toolbarLast{
text-align: right; /* Text alignement */
}
.TSO .toolbarLast:before {
content: "TSO";
opacity: 0.25;
font-size: 30px;
width: 100%;
z-index: 1000;
-webkit-text-stroke: 1px red; /* Select color */
padding-right: 5px;           /* To separate cells */
}

.SPCICSH .toolbarLast:before {
content: "SPCICSH";
opacity: 0.25;
font-size: 30px;
width: 100%;
z-index: 1000;
-webkit-text-stroke: 1px blue; /* Select color */
padding-right: 5px;            /* To separate cells */
}
```

Example custom.css for adding custom text to the toolbar



IKJ56700A ENTER USERID -

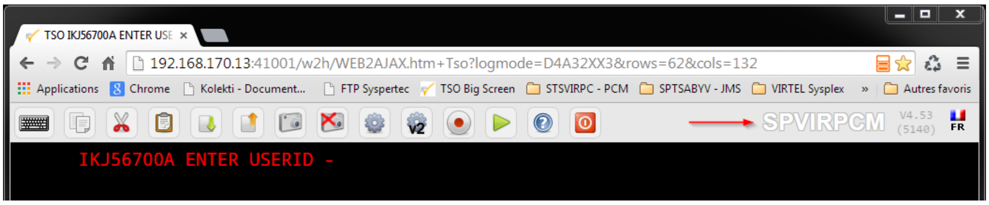


Signon to CICS APPLID SPCICSH

Web Access screen with custom application name in the toolbar

1.1.1.7.3. Showing / Hiding server informations

It is sometimes useful to have a clear visual indication of which server a user is logged on to, its version and the maintenace level applied on the system. By default, the value specified into the APPLID parameter of the VIRTCT is displayed at the top-right of the toolbar as shown below. This information is followed by the running version number and the Virtel Web access level of maintenance used. This last information is enclosed in parentheses.



IKJ56700A ENTER USERID -

The running version and the level of maintenance cannot be hidden, only the server name can be **permanently** removed by modifying the w2hparm.hideinfo attribut present in the customized w2hparms.js file:

```
/*
 * Configuration of the server name connected to.
 */

 w2hparm.hideinfo = true;
```

Example w2hparm.js for hiding the mainframe application name on which a user is connected to.

If the default value is preserved, the user can hide this information for his own usage by checking "Hide Virtel information in toolbar" in the Display tab of the settings panel.

1.1.1.7.4. Showing / Hiding running version and maintenance level

On the right side of the toolbar, the running version and the level of maintenance of VIRTEL is shown. As this information is important and very helpful in case of troubleshooting, those information cannot be hidden.

1.1.1.8. Language

1.1.1.8.1. Hide the langage icon

You can hide the language icon by using the following orders included in a custom.css file:

```
#toolbar td#toolbar-lang { width: 1px; }
#toolbar td#toolbar-lang a { display: none; }
```

Example to hide the language icon.

1.1.1.8.2. Assign a default language

You can force default language and leave to the customer the possibility to select another one if necessary by using the following order included in a custom.js file:

```
function after_standardInit() {
    /* Will force default language to Croatian and will leave to the customer
       the possibility to select another one if necessary */
    oVWAmsg.changeLang("hr");
}
```

Example to assign a default langage.

Possible values for the language code are:

- DE for Deutsch
- EN for English
- ES for Spanish
- FR for French
- HR for Croatian
- IT for Italian

They must be entered in lowercase.

1.1.1.8.3. Assign a permanent default language

You can force default language and not allow the customer to select another one. You can do it by using the following order included in a custom.js file:

```
function after_standardInit() {
   /* Will force default language to Croatian and will not allow the customer
      to select another one if necessary */
   oVWAmsgVWAmsg.restrictLanguages("hr");
}
```

Example to assign a permanent default langage.

Possible values for the language code are:

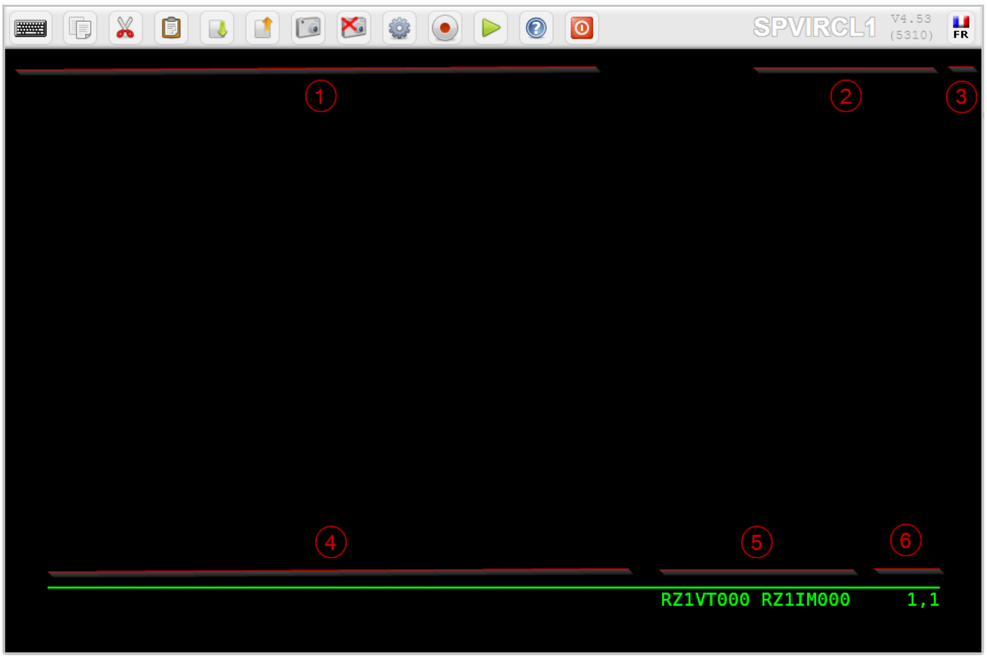
- DE for Deutsch
- EN for English
- ES for Spanish
- FR for French

- HR for Croatian
- IT for Italian

They must be entered in lowercase.

1.1.2. Status line

The status line of the VWA user interface is located at the bottom and includes the monitiring zone (4), particulars of the terminals associated with the session (5), mode and cursor position (6).



The VWA 3270 screen's areas.

1.1.2.1. Realy and Printer name

1.1.2.1.1. Managing Relay and Printer name area

The area (5) of the VWA user interface contains information about the terminals used during the session. The name of the 3270 relay terminal is shown in the leftmost portion of the area while the name of the virtual printer terminal is shown in the rightmost portion of the area. The presence of a printer device is optional and depends on the terminal definition itself.

The information in this area can be managed using the following functions:

- Editing functions
  - vwaStatusBar.setRelay("some txt") to customize the 3270 relay area
  - vwaStatusBar.setPrintRelay("some txt") to customize the print relay area
- Retrieval functions
  - vwaStatusBar.getRelay(P1) to retrieve the content of the 3270 relay area
  - vwaStatusBar.getPrintRelay(P1) to retrieve the content of the print relay area

For the retrieval function, if the value of the parameter P1 is "true" (without the double quotes), the information returned is the value of "Relay or Printer" as valued at the time the command executes. If the P1 is undefined or if its value is different from "true" the information returned is the value of "Relay or Printer" as existed at the time the page was sent by VWA to the browser.

1.1.2.1.2. Relay name area

You can manage the content of the relay name area by adding appropriate orders in after_responseHandle function.

1.1.2.1.2.1. Modify Relay name area content

```
/*
 * (c)Copyright SysperTec Communication 2012 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions
 */

function after_responseHandle(httpXmlObj, url, xmitTimestamp) {
  vwaStatusBar.setRelay();                      // Clears relay field
  vwaStatusBar.setRelay("Relay: " +             // Adds some text
               vwaStatusBar.getRelay());        // Get the relay name
}
```

Example custom.js to customize the content of the relay name area

1.1.2.1.2.2. Hide Relay name area content

You can hide the content of the realy name by replacing its content by spaces.

```
/*
 * (c)Copyright SysperTec Communication 2012 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions
 */

function after_responseHandle(httpXmlObj, url, xmitTimestamp) {
  vwaStatusBar.setRelay();                      // Clears relay field
}
```

Example custom.js to hide the content of the relay name area

1.1.2.1.3. Printer name area

You can manage the content of the printer name area by adding appropriate orders in after_responseHandle function.

1.1.2.1.3.1. Modify Printer name area content

```
/*
 * (c)Copyright SysperTec Communication 2012 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions
 */

function after_responseHandle(httpXmlObj, url, xmitTimestamp) {
  vwaStatusBar.setPrintRelay();                 // Clears printer field
  vwaStatusBar.setPrintRelay("CICS printer: " + // Adds some text
               vwaStatusBar.getPrintRelay());   // Get the printer name
}
```

Example custom.js to customize the content of the printer name area

1.1.2.1.3.2. Hide Printer name area content

You can hide the content of the printer name by replacing its content by spaces.

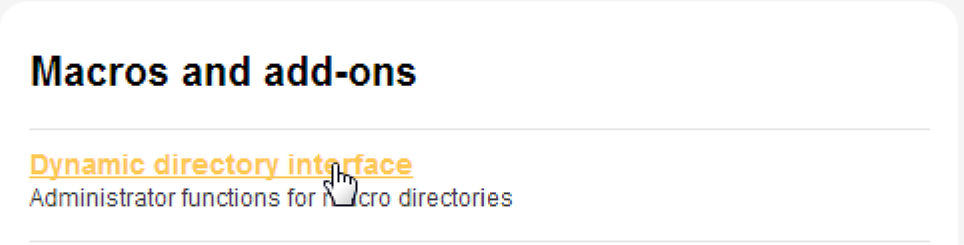
```
/*
 * (c)Copyright SysperTec Communication 2012 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions
 */

function after_responseHandle(httpXmlObj, url, xmitTimestamp) {
  vwaStatusBar.setPrintRelay();                 // Clears printer field
}
```

Example custom.js to hide the content of the printer name area

1.2. Dynamic Directory Interface (DDI)

The Dynamic Directory Interface is intended for the administator, to enable the users to deal with dynamic directories including those dedicated to various users and groups.

- The DDI application is accessible from the link "Dynamic directory interface" present in the main page associated with the W- HTTP line.



Macros and add-ons

Dynamic directory interface

Administrator functions for macro directories

Accessing the Dynamic Directory Interface.

1.2.1. "Your VIRTEL is not configured for dynamic directories"

To access the DDI, the administrator must use a Virtel Web Access session in which he has authority to manage at least one of the GLOBAL, GROUP or USER directory. To do this, the list of the transaction avalaible to the administrator must contains at least one of the following :

```
W2H-80A  uplglb   Upload macros (GLB-DIR directory)                  VIR0041C
W2H-80G  uplgrp   Upload macros (GRP-DIR directory)                  VIR0041C
W2H-80U  uplusr   Upload macros (USR-DIR directory)                  VIR0041C
```

Example of a custom.js file content to allow access to the DDI.

The internal name must be in agreement with the prefix of the transactions associated with the used entry-point. The external name must conform to one of the values presented above and need to be lowercase.

Necessary environnement to access DDI can be setup running the ARBOLOAD job present in the SAMPLIB wit the VMACRO parameter set to YES.

1.2.2. HTTP 404 or 406 while accessing directory

Once connected to the DDI, the administrator may experienced some HTTP 404 or 406 failure. This is generaly due to a lack of ressources in his profile associated with the following type of messages at the console :

```
VIRHT54E INVALID REQUEST ON HTTP-WZ1 ENTRY POINT 'ZEB2HOST' DIRECTORY 'W2H      '
       PAGE 'CAPABILITYCODE.JSON' URL '/w2h/capabilityCode.json+USRCAP'
       TRANSACTION 'USRCAP  ' CALLER  192.168.092.053:63319
       rejected transaction :USRCAP
```

This issue can be solved by adding the following transaction in the entry point :

```
TRANSACTION DETAIL DEFINITION ---------------------- Applid: SPVIRCL1 11:00:03

Internal name ===> W2H-66                 To associate with an entry point name
External name ===> usrcap                 Name displayed on user menu
Description   ===> Generate administrator upload capability token
Application   ===> $NONE$                 Application to be called
PassTicket    ===>    Name ===>           0=no 1=yes 2=unsigned
Application type   ===> 2                 1=VTAM 2=VIRTEL 3=SERV 4=PAGE 5=LINE
Pseudo-terminals   ===> DELOC             Prefix of name of partner terminals
Logmode            ===>                   Specify when LOGMODE must be changed
How started        ===> 2                 1=menu 2=sub-menu 3=auto
Security           ===> 1                 0=none 1=basic 2=NTLM 3=TLS 4=HTML
H4W commands ?     ===> 0                 0=no 1=yes 2=if2VIRTEL 4=auto
Logon message      ===>

TIOA at logon      ===> &/S OK &/T

TIOA at logoff     ===>

Initial Scenario   ===> SCENUCAP          Final Scenario      ===>
Input Scenario     ===>                   Output Scenario     ===>

P1=Update                          P3=Return                       P12=Server
```

Example of transation to avoid USER CAPABILITY error.

```
VIRHT54E INVALID REQUEST ON HTTP-WZ1 ENTRY POINT 'ZEB2HOST' DIRECTORY 'W2H      '
       PAGE 'DYNAMIC_DIR_ADMIN.JSON' URL '/w2h/dynamic_dir_admin.json+dynadmin'
       TRANSACTION 'DYNADMIN' CALLER  192.168.092.053:64074
       rejected transaction :DYNADMIN
```

This issue can be solved by adding the following transaction in the entry point :

```
TRANSACTION DETAIL DEFINITION ---------------------- Applid: SPVIRCL1 11:00:03

Internal name ===> W2H-07                 To associate with an entry point name
External name ===> dynadmin               Name displayed on user menu
Description   ===> Dynamic Directory Interface
Application   ===> VIR0022                Application to be called
```

```
PassTicket    ===>    Name ===>           0=no 1=yes 2=unsigned
Application type   ===> 2                 1=VTAM 2=VIRTEL 3=SERV 4=PAGE 5=LINE
Pseudo-terminals   ===> DELOC             Prefix of name of partner terminals
Logmode            ===>                   Specify when LOGMODE must be changed
How started        ===> 2                 1=menu 2=sub-menu 3=auto
Security           ===> 1                 0=none 1=basic 2=NTLM 3=TLS 4=HTML
H4W commands ?     ===>                   0=no 1=yes 2=if2VIRTEL 4=auto
Logon message      ===>

TIOA at logon      ===>

TIOA at logoff     ===>

Initial Scenario   ===>                   Final Scenario      ===>
Input Scenario     ===> SCDYNADM          Output Scenario     ===> SCDYNADM

P1=Update                          P3=Return                          P12=Server
```

Example of transation to authorize access to the diretory.

Necessary environnement to access DDI can be setup running the ARBOLOAD job present in the SAMPLIB wit the VMACRO parameter set to YES.

1.2.3. User have no access to the macro stored in DD

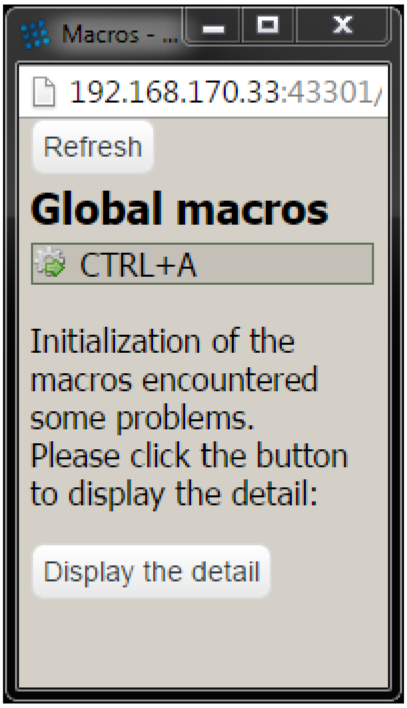
To access any of the GLOBAL, GROUP or USER dynamic directory, the user must use a Virtel Web Access session in which w2hparm.useVirtelMacros parameter is set to true. This can be done by including the following code in a custom.js file.

```
/*======================================================================
 * (c)Copyright SysperTec Communication 2012-2015 All Rights Reserved
 * VIRTEL Web Access customer-specific javascript functions & settings
 *====================================================================*/

/*
 * The macros are fetched/stored from/into Virtel directories if this property
 * is set to 'true'. Otherwise they are only saved in the Browser's local storage.
 *
 *  Default value (if unspecified) : false
 */
w2hparm.useVirtelMacros = true;
```

Example of a custom.js file content to allow access to the DDI.

1.2.4. GLOBAL macros are avalaible but not to the GROUP or USER

To access any of the GLOBAL, GROUP or USER dynamic directory, the user must use a Virtel Web Access session in which w2hparm.useVirtelMacros parameter is set to true. This can be done by including the code above. In some cases a user may encounter an error message such as : "Initialization of the macros encountered some problems. Please click the button to display the detail":



Global macros

Initialization of the macros encountered some problems. Please click the button to display the detail:

This situation mainly occurs if the user is not signed on, or does not have access to transactions targeting GRP-DIR and USR-DIR directories. To solve this situation, you must make sure that all the following conditions are met:

- The user is connected thru a session that requires to be signed on,
- The entry-point contains two transaction targetting GRP-DIR and USR-DIR. (See transaction WH2-03G and W2H-03U in the ARBOLOAD job present in the samplib for a sample),
- The GRP-DIR and USR-DIR transaction MUST BE in security mode 1 or 2 or 3 or 4 according your choice.

1.2.5. No access to the Local Storage when using Dynamic Directories

If a user is connected to VWA through a session configured to use macros stored in dynamic directories, it is no longer allowed to store macros in the Local Storage. However Local Storage will be used by VIRTEL transiently if synchronization macros is required between several VIRTEL running in a SYSPLEX environment. This can be done by including the following code inside the custom.js file associated to the connection.

```
/* The macros are synchronized between Sysplex Virtels (and-or Local Storage)
 * if this property is set to 'true' (AND w2hparm.useVirtelMacros is also 'true').
 *
 *  Default value (if unspecified) : false
 */
w2hparm.synchronizeVirtelMacros = true;
```

Example of a custom.js file content to allow synchronization in SYSPLEX environment.

2. Lines

2.0.6. Starting and stopping a line

By default, a line is automatically initialized at Virtel startup, and is terminated when Virtel stops.

In some cases, the handling of line initialization/termination needs to be managed differently:

Initialization conditioned by the “Possible Calls” parameter

- 0: the line is not initialized at Virtel startup. It must be started manually.
- 1, 2, 3: except in the cases described below, the line is initialized automatically at Virtel startup. The value of this field indicates the possible directions allowed for communication.

Initialization completely inhibited

Whatever the value of the “Possible calls” field, if the VIRTCT contains a parameter IGNLU that references the line, then this line shall not be initialized automatically at Virtel startup. In this case it will no longer be possible to start this line manually after Virtel has started.

Conditional initialization of a line

It is possible to condition the initialization of a line to that of another line. This can be necessary for example when an application communicates with Virtel via MQ/Series, with one line that accepts inbound messages and another line that handles outbound messages. In this case, it is useful to wait until the communication with the partner has been established before accepting inbound messages.

```
LINE     ID=M-MQ1,                                                -
         NAME=MQ-IN,                                              -
         LOCADDR=REQ.INPUT.QUEUE,                                 -
         DESC='MQ - REQUEST',                                     -
         TERMINAL=MQINT,                                          -
         ENTRY=MQINEP,                                            -
         TYPE=MQ1,                                                -
         INOUT=1,                                                 -
         COND='MIMIC-LINE(M-MQ0)',                                -
         PROTOCOL=PREFIXED,                                       -
         RULESET=M-MQ1

LINE     ID=M-MQ2,                                                -
         NAME=MQ-OUT,                                             -
         LOCADDR=REQ.OUTPUT.QUEUE,                                -
         DESC='MQ - OUTPUT REQUETE',                              -
         TERMINAL=MQOUT,                                          -
         TYPE=MQ1,                                                -
```

```
               INOUT=2,                                                 -
               PROTOCOL=PREFIXED,                                       -
               RULESET=M-MQ2
```

Deferred initialization

The “Possible calls” field must be set to 0. The line may subsequently be started by a START command. It must not be referenced by an IGNLU parameter in the VIRTCT.

Using commands at the system console

Lines can be started or stopped by entering the appropriate command at the console. For further information on how to issue Virtel commands, see "Audit And Performance" reference manuel.

```
LINE=linename,START (or L=linename,S)
LINE=linename,STOP (or L=linename,P)
```

linename

> internal or external name of the line

The LINE START and LINE STOP commands perform the same function as using the “S” and “P” commands on the “Status of lines”. These commands may only be issued for line types AntiGATE, AntiPCNE, AntiFASTC, and TCP/IP.

3. Terminal

3.1. Controling LU Names

When a user connects to a 3270 application through VIRTEL Web Access, VIRTEL makes it appear to the application as if the user is connecting from a virtual 3270 terminal. In VTAM terms a virtual 3270 terminal is called a Logical Unit or LU, and each LU has a unique eight character name (LU name). VIRTEL has at its disposal a pool of LUs known to VTAM, whose names are specified in the VIRTEL configuration file (the VIRARBO file). Normally when a user connects to a 3270 application, VIRTEL chooses any available LU from the pool.

While most mainframe applications will accept a connection from any LU name, certain applications (particularly applications which run under IMS) are sensitive to the LU name because they assign permissions to the user based upon the LU name of the user’s terminal. LU nailing allows VIRTEL to assign a particular LU name to a user based upon the user’s IP address or upon a cookie presented by the user’s browser.

This chapter describes the following types of LU nailing:

- LU nailing by work station name
- LU nailing by LU (Pre-defined terminal)
- LU nailing by LU (Non-predefined terminal)
- LU nailing by IP address
- LU nailing by cookie
- LU nailing by URL

3.1.1. LU nailing using the work station name (Predefined terminals)

In this example we use a batch job on the user’s PC to initiate a session with Virtel. The batch job obtains the terminal name of the work station, opens a browser window and passes the work station name through to Virtel. With a Virtel RULE we can test the name of the workstation and assign a particular relay LUNAME from a Virtel terminal POOL.

```
RULE ID=ESH0000,                                         -
     RULESET=E-HTTP,                                     -
     STATUS=ACTIVE,                                      -
     DESC='Rule for terminal EHPMA00',                   -
     ENTRY=EDSWHOST,                                     -
     PARAM=EHPMA000,         /* Or EHPMA00* */           -
     NETMASK=255.255.255.255,                            -
     USERDATA=(EQUAL,HOLT-W)
```

Example of a Virtel RULE to be activated with a user data.

The rule instructs Virtel to test the user data field passed in a URL and if it matches the string POOL-W than to assign an LU name prefix of EHPMA00 and direct the terminal call to use an entry point of EDSWHOST. A static rule would have to be built for each unique work station name.

The EDSWHOST entry point looks like:

```
ENTRY ID=EDSWHOST,                                      -
      DESC='EDS WEB ENTRY POINT (USERS WITH USERDATA)', -
      TRANSACT=EDSW,                                    -
      TIMEOUT=0720,                                     -
      ACTION=0,                                         -
      EMUL=HTML,                                        -
      SIGNON=VIR0020H,                                  -
      MENU=VIR0021A,                                    -
      EXTCOLOR=X,                                       -
      ENDPAGE=CLOSE.HTM
```

In this entry point you would define the relevant transactions. In our case we have defined the following:

- A transaction using EHLOC terminals to access the /w2h directory
- A Virtel transaction using EHLOC terminals to support the application menu list
- VTAM transaction using EHVTS terminal to establish a relationship with the VTAM application

```
TRANSACT ID=EDSW-00,                                    -
         NAME=EDSWHOST,                                 -
         DESC='HTML page directory (default access)',   -
         APPL=W2H-DIR,                                  -
         TYPE=4,                                        -
         TERMINAL=EHLOC,                                -
         STARTUP=2,                                     -
         SECURITY=0
TRANSACT ID=EDSW-20,                                    -
         NAME='w2h',                                    -
         DESC='W2H toolkit directory (/w2h)',           -
         APPL=W2H-DIR,                                  -
         TYPE=4,                                        -
         TERMINAL=EHLOC,                                -
         STARTUP=2,                                     -
         SECURITY=0
TRANSACT ID=EDSW-41,                                    -
         NAME=IMS,                                      -
         DESC='IMS access with userdata',               -
         APPL=IMS3270,                                  -
         PASSTCKT=0,                                    -
         TYPE=1,                                        -
         TERMINAL=EHVTS,                                -
         STARTUP=1,                                     -
         SECURITY=0
TRANSACT ID=EDSW-42,                                    -
         NAME=TSO,                                      -
         DESC='TSO access with userdata',               -
         APPL=TSO,                                      -
         PASSTCKT=0,                                    -
         TYPE=1,                                        -
         TERMINAL=EHVTS,                                -
         STARTUP=1,                                     -
         SECURITY=0
TRANSACT ID=EDSW-90,                                    -
         NAME='applist',                                -
         DESC='List of applications for appmenu.htm',   -
         APPL=VIR0021S,                                 -
         TYPE=2,                                        -
         TERMINAL=EHLOC,                                -
         STARTUP=2,                                     -
         SECURITY=1
```

In VTAM we would have the following definition:

```
* ------------------------------------------------------------------ *
* LU Test : VTAM application relays with user data. *
* ------------------------------------------------------------------ *
EHPMA000 APPL AUTH=(ACQ,PASS),MODETAB=ISTINCLM,DLOGMOD=SNX32702,EAS=1
Or for EHPMA00*
* ------------------------------------------------------------------ *
* LU Test : VTAM application relays with user data. *
* ------------------------------------------------------------------ *
EHPMA00? APPL AUTH=(ACQ,PASS),MODETAB=ISTINCLM,DLOGMOD=SNX32702,EAS=1
```

Example of VTAM APPL definitions.

We also need a terminal and pool definition. Here is the pool definition:

```
TERMINAL ID=EHPMA000,                                    -
         RELAY=EHPMA000, /* Or EHPMA00* */               -
         POOL=*STAPOOL,                                  -
         DESC='Terminal definition for EHPMA000',        -
         TYPE=3,                                         -
         COMPRESS=2,                                     -
         INOUT=3,                                        -
         STATS=26,                                       -
         REPEAT=
```

…and a pool definition for out static pool:

```
TERMINAL ID=EHVTS000,                                    -
         RELAY=*STAPOOL,                                 -
         DESC='Static definition pool',                  -
         TYPE=3,                                         -
         COMPRESS=2,                                     -
         INOUT=3,                                        -
         STATS=26,                                       -
         REPEAT=0010
```

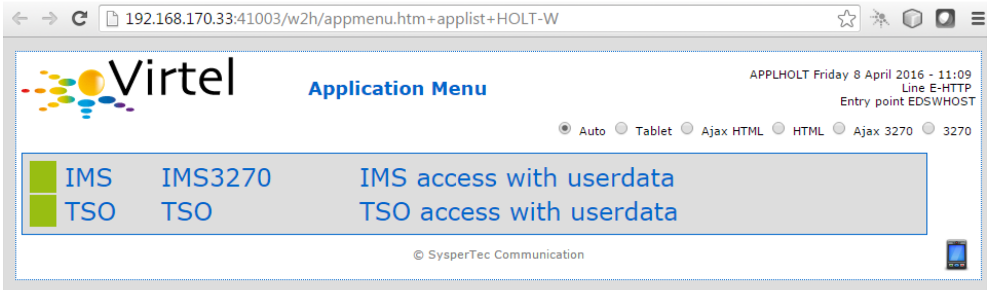
This setup will support up to 10 predefined terminal definitions. For each terminal we have to provide a static definition. Of course we could have used a generic terminal definition of EHPMA00* but this would only work for numerically sequenced terminal names – EHPMA000 – EHPMA009.

Getting the PC workstation name to Virtel is through a batch job which fires up the default browser and passes the work station name as a user data parameter. Here is an example:

```
title Test Propagation of Userdata Parameter
@echo on
color 1f
cls
SET P1=%COMPUTERNAME:~0,6%
start http://192.168.170.33:41003/w2h/appmenu.htm+applist+%P1% &goto:eof
:exit
```

The SET command takes the first six characters of the work station name and passes it into the start command. Following the Virtel transaction I wish to execute which in this case is an APPLIST menu list.

The start command will open a default browser window and connect to Virtel:



192.168.170.33:41003/w2h/appmenu.htm+applist+HOLT-W

Application Menu

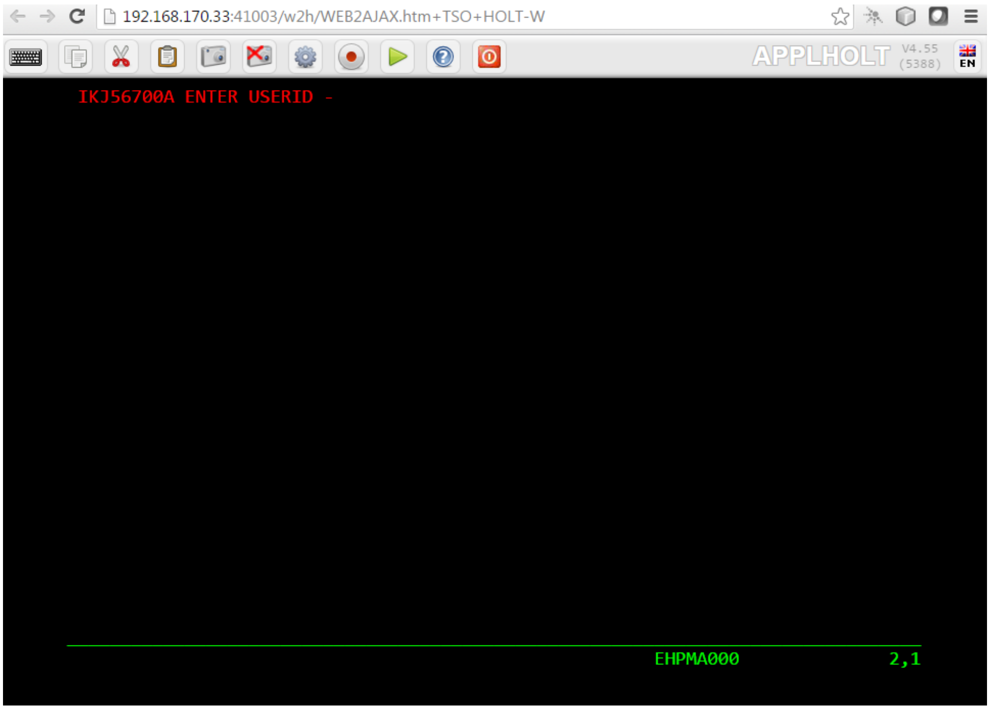
APPLHOLT Friday 8 April 2016 - 11:09
Line E-HTTP
Entry point EDSWHOST

● Auto ○ Tablet ○ Ajax HTML ○ HTML ○ Ajax 3270 ○ 3270

IMS	IMS3270	IMS access with userdata
TSO	TSO	TSO access with userdata

© SysperTec Communication

When a transaction is selected from the menu list the RULE will be invoked to allocate the correct LUNAME.



192.168.170.33:41003/w2h/WEB2AJAX.htm+TSO+HOLT-W

```
IKJ56700A ENTER USERID -

                                              EHPMA000              2,1
```

The Virtel RULE has forced an LU name prefixed EHPMA00* to be used from the the VIRTEL terminal pool associated with the Virtel line. In this case relay LUNAME EHPMA000 has been allocated.

In the VTAM display we can see that a session has been set up using that LU name:

```
D NET,ID=EHPMA000,E
  IST097I DISPLAY ACCEPTED
  IST075I NAME = SPNET.EHPMA000, TYPE = DYNAMIC APPL 073
  IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
  IST1447I REGISTRATION TYPE = CDSERVR
  IST1629I MODSRCH = NEVER
  IST977I MDLTAB=***NA*** ASLTAB=***NA***
  IST861I MODETAB=ISTINCLM USSTAB=***NA*** LOGTAB=***NA***
  IST934I DLOGMOD=SNX32702 USS LANGTAB=***NA***
  IST1632I VPACING = 7
  IST1938I APPC = NO
  IST597I CAPABILITY-PLU ENABLED ,SLU ENABLED ,SESSION LIMIT NONE
  IST231I APPL MAJOR NODE = APPLSPEH
  IST1425I DEFINED USING MODEL EHPMA???
  IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
  IST1500I STATE TRACE = OFF
  IST271I JOBNAME = SPVIREH, STEPNAME = SPVIREH, DSPNAME = IST217EE
  IST228I ENCRYPTION = OPTIONAL , TYPE = DES
  IST1563I CKEYNAME = EHPMA000 CKEY = PRIMARY CERTIFY = NO
  IST1552I MAC = NONE MACTYPE = NONE
  IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
  IST1633I ASRCVLM = 1000000
```

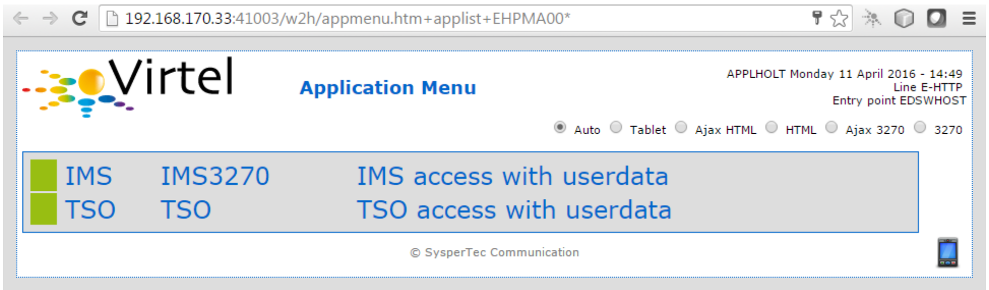
```
      IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
      IST1669I IPADDR..PORT 192.168.92.65..50027
      IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
      IST206I SESSIONS:
      IST634I NAME STATUS SID SEND RECV VR TP NETID
      IST635I TSO1A005 ACTIV-P CA7B8B52114E7A85 0000 0002 SPNET
      IST314I END
```

3.1.2. LU nailing using an LU name (Predefined Terminal)

Instead of passing a work station name in the user data field of the URL in this example we are passing an LU name. Again with a Virtel RULE we can extract the user data parameter from the URL and use that as the Virtel relay LUNAME name. For this example the rule looks like:

```
RULE ID=ESH0001,                                         -
     RULESET=E-HTTP,                                     -
     STATUS=ACTIVE,                                      -
     DESC='Rule for terminal EHPMA00',                   -
     ENTRY=EDSWHOST,                                     -
     PARAM=$URL$,                                        -
     NETMASK=255.255.255.255
```

We use the special PARAM=URL which indicates that the VTAM LU Name to be used is the user data passed in the URL.



192.168.170.33:41003/w2h/appmenu.htm+applist+EHPMA00*

Virtel

Application Menu

APPLHOLT Monday 11 April 2016 - 14:49
Line E-HTTP
Entry point EDSWHOST

● Auto ○ Tablet ○ Ajax HTML ○ HTML ○ Ajax 3270 ○ 3270

IMS	IMS3270	IMS access with userdata
TSO	TSO	TSO access with userdata

© SysperTec Communication

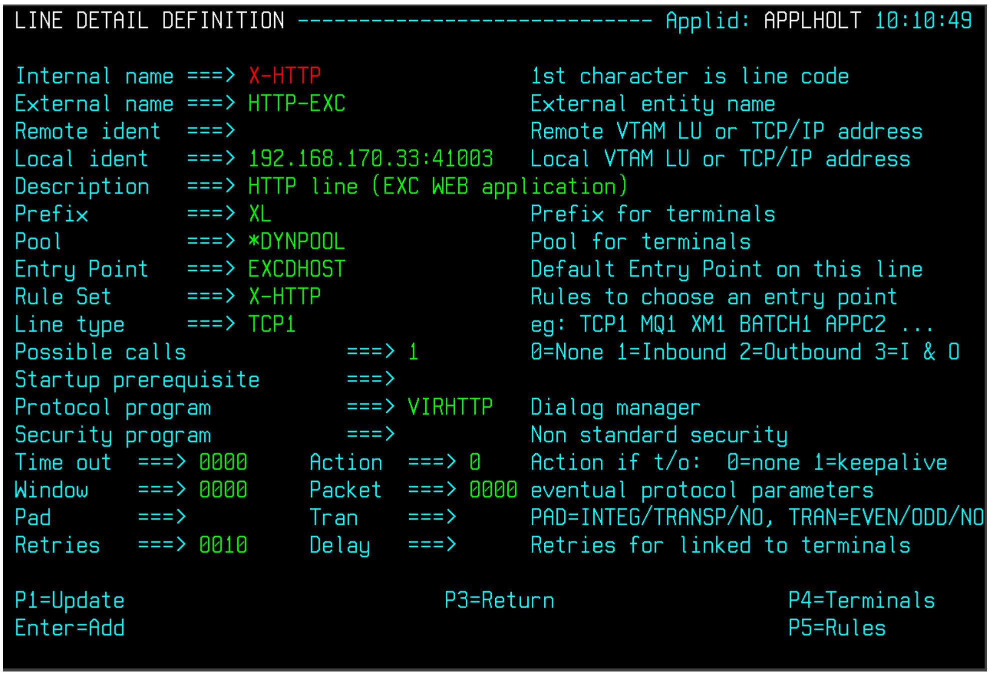
The user data in the URL, in this case EHPMA00*, will be added to each transaction in the APPLIST menu and used as the Virtel relay LUNAME. When connecting to an application VIRTEL will use the LU name defined in the URL. In this example we are using a generic LUNAME (This could support a range from EHPMA000 through to EHPMA009

3.1.3. Lu Nailing using an LU Name (No predefined terminal)

Both of the above techniques require that a relay terminal be predefined for each terminal. For some installations this could be a maintenance headache and doesn't scale up very well. Virtel provides a feature whereby predefined names are not necessary. In this next example we look at a technique that doesn't require terminal predefinition. Virtel will grab a terminal entry from a pool and use the LU name passed in the URL as the relay LU name. To use this setup certain conditions must be in place. Also note that no rules are required. Those definitions required are:

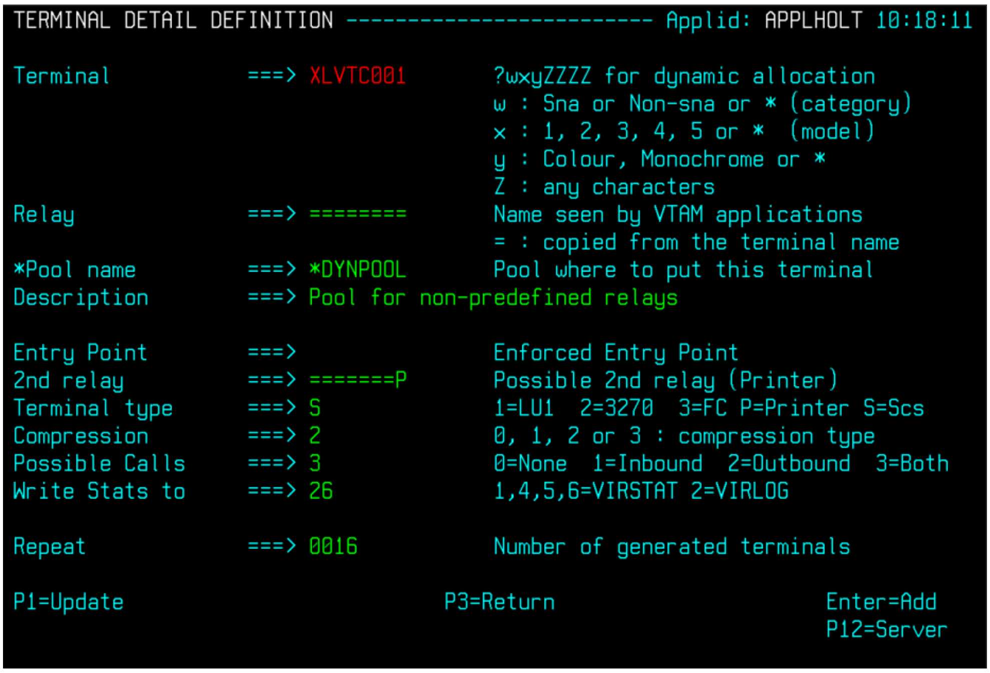
- The HTTP Line must specify a pool name,
- A pool name needs to be defined,
- Transactions must specify $LINE$ in the "Pseudo-terminals" field.

Line définition



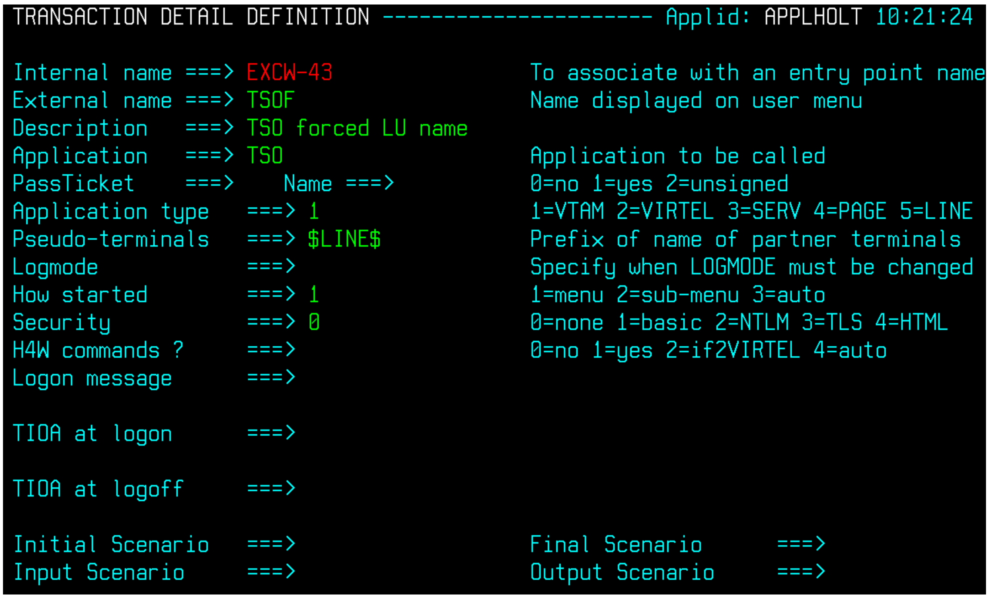
```
LINE DETAIL DEFINITION ---------------------------- Applid: APPLHOLT 10:10:49

Internal name ===> X-HTTP                    1st character is line code
External name ===> HTTP-EXC                  External entity name
Remote ident  ===>                           Remote VTAM LU or TCP/IP address
Local ident   ===> 192.168.170.33:41003      Local VTAM LU or TCP/IP address
Description   ===> HTTP line (EXC WEB application)
Prefix        ===> XL                        Prefix for terminals
Pool          ===> *DYNPOOL                  Pool for terminals
Entry Point   ===> EXCDHOST                  Default Entry Point on this line
Rule Set      ===> X-HTTP                    Rules to choose an entry point
Line type     ===> TCP1                      eg: TCP1 MQ1 XM1 BATCH1 APPC2 ...
Possible calls             ===> 1            0=None 1=Inbound 2=Outbound 3=I & O
Startup prerequisite       ===>
Protocol program           ===> VIRHTTP      Dialog manager
Security program           ===>              Non standard security
Time out    ===> 0000     Action   ===> 0    Action if t/o:  0=none 1=keepalive
Window      ===> 0000     Packet   ===> 0000 eventual protocol parameters
Pad         ===>          Tran     ===>      PAD=INTEG/TRANSP/NO, TRAN=EVEN/ODD/NO
Retries     ===> 0010     Delay    ===>      Retries for linked to terminals

P1=Update                          P3=Return                   P4=Terminals
Enter=Add                                                      P5=Rules
```

Pool definition for non-predefined LU Names



```
TERMINAL DETAIL DEFINITION ------------------------ Applid: APPLHOLT 10:18:11

Terminal            ===> XLVTC001       ?wxyZZZZ for dynamic allocation
                                        w : Sna or Non-sna or * (category)
                                        x : 1, 2, 3, 4, 5 or *  (model)
                                        y : Colour, Monochrome or *
                                        Z : any characters
Relay               ===> ========       Name seen by VTAM applications
                                        = : copied from the terminal name
*Pool name          ===> *DYNPOOL       Pool where to put this terminal
Description         ===> Pool for non-predefined relays

Entry Point         ===>                Enforced Entry Point
2nd relay           ===> =======P       Possible 2nd relay (Printer)
Terminal type       ===> S              1=LU1  2=3270  3=FC P=Printer S=Scs
Compression         ===> 2              0, 1, 2 or 3 : compression type
Possible Calls      ===> 3              0=None  1=Inbound  2=Outbound  3=Both
Write Stats to      ===> 26             1,4,5,6=VIRSTAT 2=VIRLOG

Repeat              ===> 0016           Number of generated terminals

P1=Update                          P3=Return                      Enter=Add
                                                                  P12=Server
```

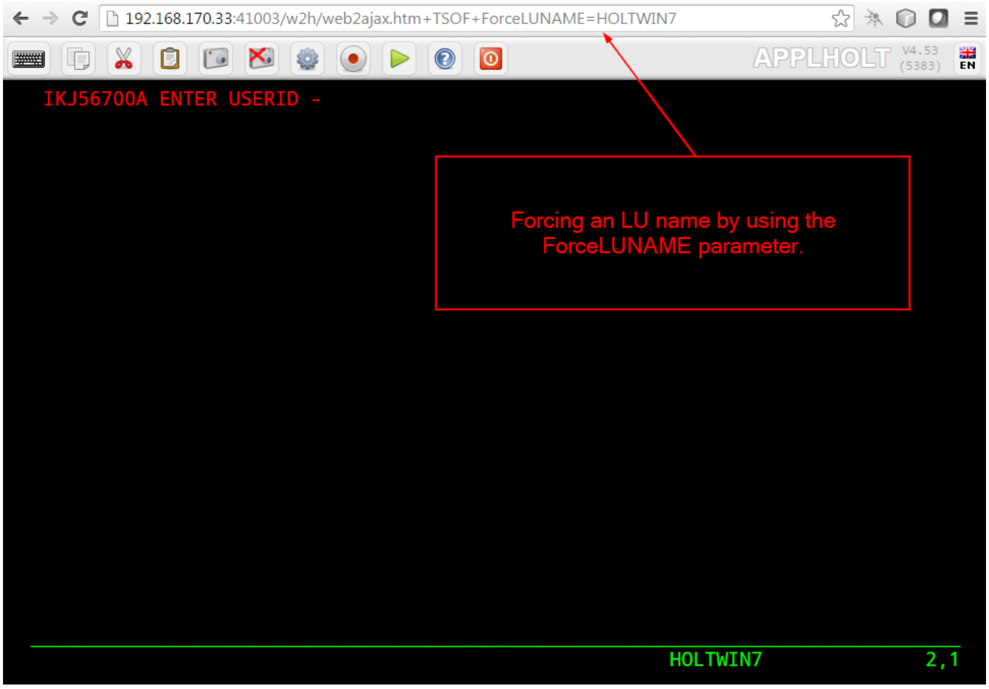
Transaction defintion



```
TRANSACTION DETAIL DEFINITION ---------------------- Applid: APPLHOLT 10:21:24

Internal name ===> EXCW-43                    To associate with an entry point name
External name ===> TSOF                       Name displayed on user menu
Description   ===> TSO forced LU name
Application   ===> TSO                        Application to be called
PassTicket    ===>    Name ===>               0=no 1=yes 2=unsigned
Application type   ===> 1                     1=VTAM 2=VIRTEL 3=SERV 4=PAGE 5=LINE
Pseudo-terminals   ===> $LINE$                Prefix of name of partner terminals
Logmode            ===>                       Specify when LOGMODE must be changed
How started        ===> 1                     1=menu 2=sub-menu 3=auto
Security           ===> 0                     0=none 1=basic 2=NTLM 3=TLS 4=HTML
H4W commands ?     ===>                       0=no 1=yes 2=if2VIRTEL 4=auto
Logon message      ===>

TIOA at logon      ===>

TIOA at logoff     ===>

Initial Scenario   ===>                       Final Scenario     ===>
Input Scenario     ===>                       Output Scenario    ===>
```

Note that the Psuedo-Terminal is defined as $LINE$. We have also assign a printer definition to this setup. So if our LU relay name was HOLTWIN7 then our associated printer LU would be HOLTWINP.

Accessing the transaction TSOF would be through the following URL forcing the relay LU NAME to HOLTWIN7. We would still have to define a terminal pool for *DYNPOOL, but we avoid having to define individual terminal definitions, or ranges of, for every static terminals.



```
192.168.170.33:41003/w2h/web2ajax.htm+TSOF+ForceLUNAME=HOLTWIN7
```

```
IKJ56700A ENTER USERID -

                                                   HOLTWIN7          2,1
```

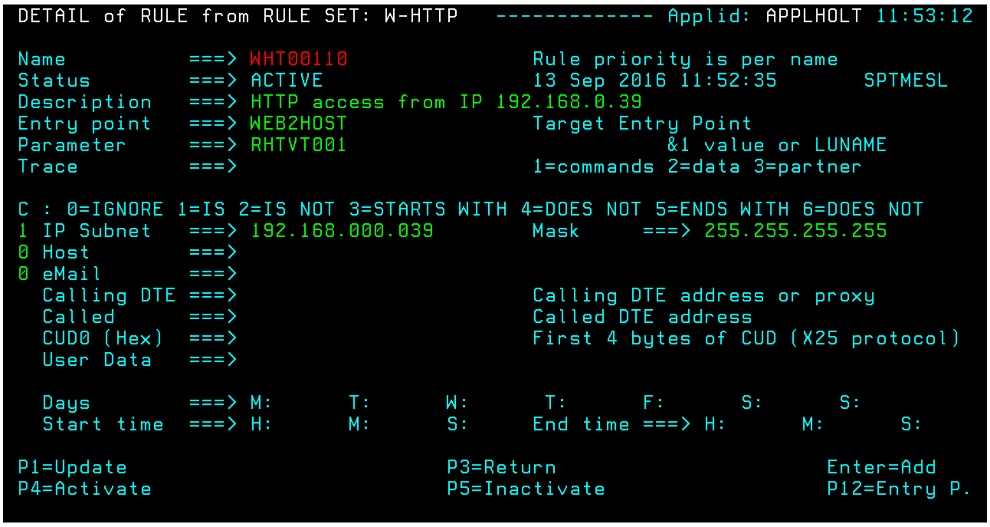
Forcing an LU name by using the ForceLUNAME parameter.

3.1.4. Lu Nailing using a cookie (Correspondent Sub Application)

Virtel also can use cookies to select a relay LU name. Virtel uses a cookie as a part of the “Correspondence Sub Application’. Within the cookie sent to Virtel is a security token. This token is used to identify a user and their associated VTAM LU relay name. A Correspondent file is used to maintain the user details. The cookie can be sent to the use as part of an Email from which the User selects a link to access Virtel or it can be part of the ‘self-registration’ process. For further information see Virtel – How to Activate LU Nailing.

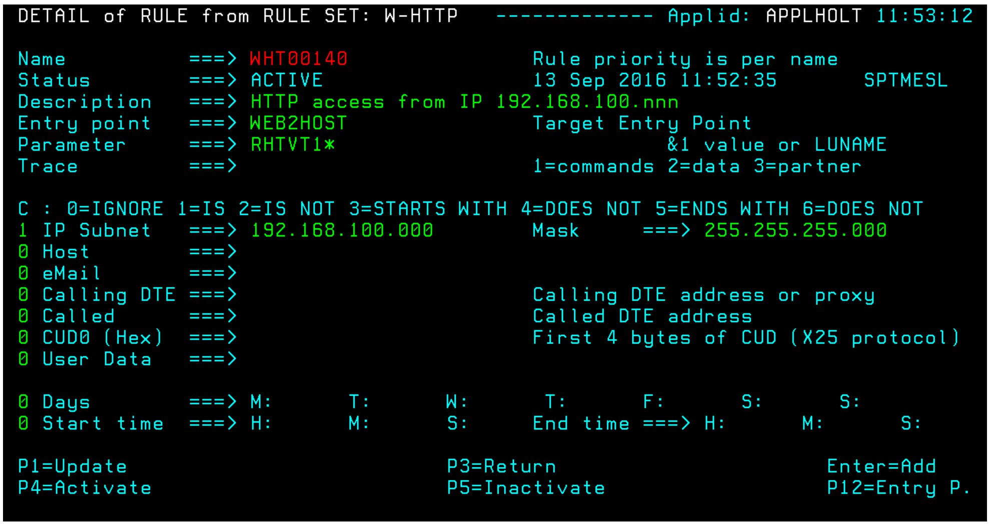
3.1.5. LU Nailing by IP

This technique uses a rule to associate an IP address with an LU Name. The rule is associated with a line. In the example below we define a rule on line W-HTTP which will force a terminal connecting with IP address 192.168.000.039 to use LU name RHTVT001. The LU name must be pre-defined in a Virtel terminal pool.



```
DETAIL of RULE from RULE SET: W-HTTP   ------------- Applid: APPLHOLT 11:53:12

Name           ===> WHT00110                 Rule priority is per name
Status         ===> ACTIVE                   13 Sep 2016 11:52:35       SPTMESL
Description    ===> HTTP access from IP 192.168.0.39
Entry point    ===> WEB2HOST                 Target Entry Point
Parameter      ===> RHTVT001                            &1 value or LUNAME
Trace          ===>                          1=commands 2=data 3=partner

C : 0=IGNORE 1=IS 2=IS NOT 3=STARTS WITH 4=DOES NOT 5=ENDS WITH 6=DOES NOT
1 IP Subnet    ===> 192.168.000.039          Mask     ===> 255.255.255.255
0 Host         ===>
0 eMail        ===>
  Calling DTE  ===>                          Calling DTE address or proxy
  Called       ===>                          Called DTE address
  CUD0 (Hex)   ===>                          First 4 bytes of CUD (X25 protocol)
  User Data    ===>

  Days         ===> M:      T:      W:      T:      F:      S:      S:
  Start time   ===> H:      M:      S:       End time ===> H:      M:      S:

P1=Update                          P3=Return                      Enter=Add
P4=Activate                        P5=Inactivate                  P12=Entry P.
```

Multiple terminals can be defined with a rule by using the * suffix. In the following example a range of IP address is mapped to a pool of LU names. Address range 192.168.100.0 through to 192.168.100.255 will be assigned the next unused LU name in the range RHTVT1xx.



```
DETAIL of RULE from RULE SET: W-HTTP   ------------- Applid: APPLHOLT 11:53:12

Name           ===> WHT00140                 Rule priority is per name
Status         ===> ACTIVE                   13 Sep 2016 11:52:35       SPTMESL
Description    ===> HTTP access from IP 192.168.100.nnn
Entry point    ===> WEB2HOST                 Target Entry Point
Parameter      ===> RHTVT1*                             &1 value or LUNAME
Trace          ===>                          1=commands 2=data 3=partner

C : 0=IGNORE 1=IS 2=IS NOT 3=STARTS WITH 4=DOES NOT 5=ENDS WITH 6=DOES NOT
1 IP Subnet    ===> 192.168.100.000          Mask     ===> 255.255.255.000
0 Host         ===>
0 eMail        ===>
0 Calling DTE  ===>                          Calling DTE address or proxy
0 Called       ===>                          Called DTE address
0 CUD0 (Hex)   ===>                          First 4 bytes of CUD (X25 protocol)
0 User Data    ===>

0 Days         ===> M:      T:      W:      T:      F:      S:      S:
0 Start time   ===> H:      M:      S:       End time ===> H:      M:      S:

P1=Update                          P3=Return                      Enter=Add
P4=Activate                        P5=Inactivate                  P12=Entry P.
```

The new rule is named WHT00140, the "IP Subnet" field specifies the IP address 192.168.100.000, and the "Mask" is set to 255.255.255.000 to indicate that only the first three octets of the IP address are tested to determine whether the rule matches the IP address of the client browser. The "parameter" field specifies a generic LU name RHTVT1* which signifies that any LU whose name begins with RHTVT1 may be assigned to clients whose IP address matches this rule.

Comparison Table

	Rule definition	Terminal definition	Cookies Used
By Work Station Name in URL	**Yes. 1 per work station**	**Yes. Individual or Group**	No
By LUNAME in URL	**Yes. 1 generic rule**	**Yes. Individual or Group**	No
By using Forced LU	No	**Pool Only**	No

Correspondant	**Yes**	**Yes**	**Yes**
By IP	**Yes**	**Yes**	No

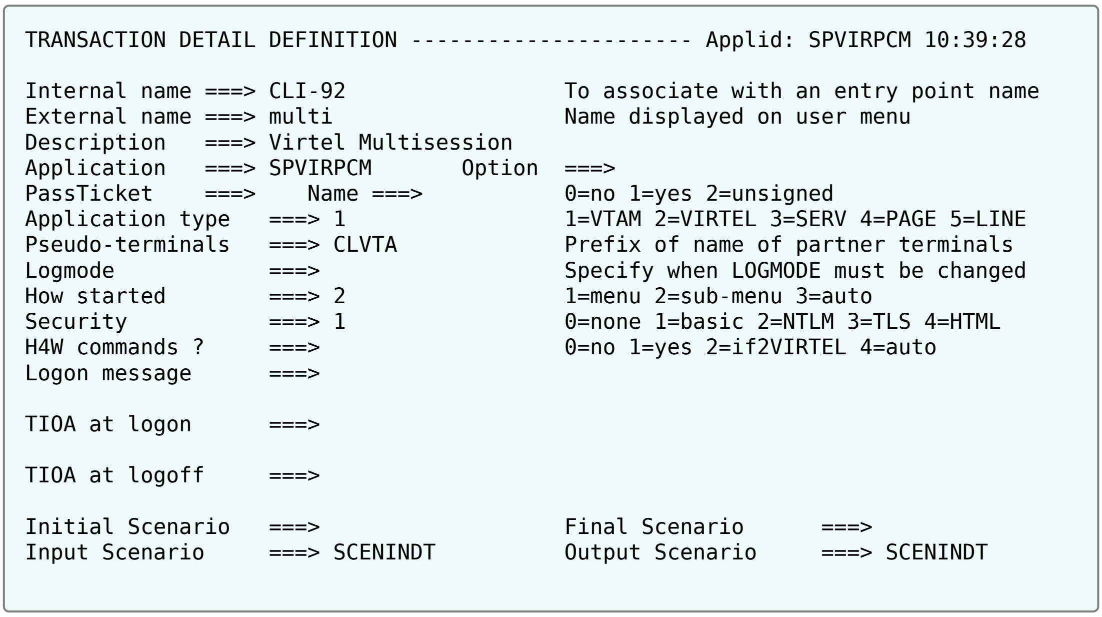
4. Transactions & Applications

4.1. Virtel Multisession Within Virtel Web Access

In some situations, it is necessary to allow a group of users to simultaneously access several distinct 3270 applications. This can be solved by using the "appmenu.htm" associated with the "applist" transaction, or by using the 3270 Multisession function of Virtel.

In the first situation, for a same original calling terminal, Virtel uses as many relays as VTAM open sessions, in the second configuration, a single relay is used for all sessions, Virtel ensuring the swapping between the opened session.

To access the Multisession function of Virtel, you must define a transaction whose application name is the same as the main Virtel ACB name. This transaction is accessible in the same way as any other VTAM appplication. As the first screen shown is a signature screen, the transaction does not necessarily need to be secured. The lists of applications presented to the user depends on the selected parameter setting (See the Virtel Multisession documented section for further information on this subject). Use of the multisession Virtel module, even in a VWA context, requires an appropriate license agreement.



```
TRANSACTION DETAIL DEFINITION ---------------------- Applid: SPVIRPCM 10:39:28

Internal name ===> CLI-92                 To associate with an entry point name
External name ===> multi                  Name displayed on user menu
Description   ===> Virtel Multisession
Application   ===> SPVIRPCM       Option  ===>
PassTicket    ===>    Name ===>           0=no 1=yes 2=unsigned
Application type   ===> 1                 1=VTAM 2=VIRTEL 3=SERV 4=PAGE 5=LINE
Pseudo-terminals   ===> CLVTA             Prefix of name of partner terminals
Logmode            ===>                   Specify when LOGMODE must be changed
How started        ===> 2                 1=menu 2=sub-menu 3=auto
Security           ===> 1                 0=none 1=basic 2=NTLM 3=TLS 4=HTML
H4W commands ?     ===>                   0=no 1=yes 2=if2VIRTEL 4=auto
Logon message      ===>

TIOA at logon      ===>

TIOA at logoff     ===>

Initial Scenario   ===>                   Final Scenario      ===>
Input Scenario     ===> SCENINDT          Output Scenario     ===> SCENINDT
```

```
 P1=Update                          P3=Return                      P12=Server
```

Transaction definition for the Virtel Multisession module

4.2. How To Access A Host Application Directly

It is not always necessary to pass via an application selection menu to connect to a host application. A host application may be accessed directly by opening the URL containing the complete path to the application. This URL may result in the display of the host signon screen, the first application screen, or possibly (if a script or scenario is used), a subsequent screen sent by the application. For more information about how VIRTEL can be used to automate the process of connection to a host application, see Virtel URL formats in the Virtel Web Access Reference manual, and "Connection/Disconnection Scripts" in the VIRTEL Connectivity Reference manual.

4.2.1. Full path URL

For example, you can access the VIRTEL transaction whose external name is "Cics" by pointing the browser at a URL of the following format:

```
http://n.n.n.n:41001/w2h/WEB2AJAX.htm+Cics
```

At the end of the session with the host application, VIRTEL examines the "Last page" field (see previous section) to decide whether to return to the desktop or to redisplay the application selection menu.

4.2.2. Default URL for the entry point

An application URL may be coded in the "TIOA at logon" field of the default transaction for the entry point (the default transaction is the transaction whose external name is the same as the entry point name). This allows the user to go directly to the host application simply by entering a URL of the format:

```
http://n.n.n.n:41001
```

The example below shows the default transaction for the WEB2HOST entry point set up to go directly to the transaction whose external name is "Cics":

```
 TRANSACTION DETAIL DEFINITION ---------------------- Applid: VIRTEL   15:01:02

 Internal name ===> W2H-00                 To associate with an entry point name
 External name ===> WEB2HOST               Name displayed on user menu
 Description   ===> Default directory = entry point name
 Application   ===> W2H-DIR                Application to be called
 PassTicket    ===> 0  Name ===>           0=no 1=yes 2=unsigned
 Application type   ===> 4                 1=VTAM 2=VIRTEL 3=SERV 4=PAGE 5=LINE
 Pseudo-terminals   ===> DELOC             Prefix of name of partner terminals
 Logmode            ===>                   Specify when LOGMODE must be changed
 How started        ===> 2                 1=menu 2=sub-menu 3=auto
 Security           ===> 0                 0=none 1=basic 2=NTLM 3=TLS 4=HTML
 H4W commands ?     ===>                   0=no 1=yes 2=if2VIRTEL 4=auto
 Check URL Prefix   ===>

 TIOA at logon      ===> /w2h/WEB2AJAX.htm+Cics

 TIOA at logoff     ===>

 Initial Scenario   ===>                   Final Scenario      ===>
 Input Scenario     ===>                     Output Scenario     ===>

 P1=Update                          P3=Return                       P12=Server
```

Example of default URL

For more information see Virtel URL formats in the Virtel Web Access Reference manual.

4.3. How To Use Different Screen Sizes

Although the standard 3270 screen size is 24 rows by 80 columns, certain applications benefit from the use of terminals with larger screen sizes. The screen size is determined by the LOGMODE used for the session between VIRTEL and the host application. VTAM offers logmodes for the following standard screen sizes:

- model 2 : 24x80 (logmode SNX32702)
- model 3 : 32x80 (logmode SNX32703)
- model 4 : 43x80 (logmode SNX32704)
- model 5 : 27x132 (logmode SNX32705)

There are two different ways that the VIRTEL administrator can set up the configuration to allow the VIRTEL Web Access user to select the desired logmode:

- define a separate VIRTEL transaction for each screen size, and allow the user to select the appropriate transaction
- group the VTAM relay LUs into pools, each pool having a different logmode, and allow the user to select the pool by coding an appropriate parameter on the URL

4.3.1. LOGMODE defined by the transaction

With this method, the administrator defines multiple VIRTEL transactions for a single application, each transaction specifying a different logmode. For example, transactions Tso2 and Tso5 delivered in the sample configuration both define TSO as the target application, but specify different logmodes SNX32702 and SNX32705 respectively. The user selects the desired transaction from the applist menu displayed by the “Other applications” link in the VIRTEL Web Access menu.

The figure below shows the definition of the Tso5 transaction defined under the WEB2HOST entry point:

```
 TRANSACTION DETAIL DEFINITION ---------------------- Applid: VIRTEL   17:12:54

 Internal name ===> W2H-13M5                 To associate with an entry point name
 External name ===> Tso5                     Name displayed on user menu
 Description   ===> Logon to Tso (3270 model 5)
 Application   ===> TSO                      Application to be called
 PassTicket    ===> 0  Name ===>             0=no 1=yes 2=unsigned
 Application type   ===> 1                   1=VTAM 2=VIRTEL 3=SERV 4=PAGE 5=LINE
 Pseudo-terminals   ===> DEVT                Prefix of name of partner terminals
 Logmode            ===> SNX32705            Specify when LOGMODE must be changed
 How started        ===> 1                   1=menu 2=sub-menu 3=auto
 Security           ===> 0                   0=none 1=basic 2=NTLM 3=TLS 4=HTML
 H4W commands ?     ===>                     0=no 1=yes 2=if2VIRTEL 4=auto
 Logon message      ===>

 TIOA at logon      ===>

 TIOA at logoff     ===>

 Initial Scenario   ===>                     Final Scenario     ===>
 Input Scenario     ===>                     Output Scenario    ===>
```

```
P1=Update                          P3=Return                       P12=Server
```

Example of TSO transaction TSO specifying logmode SNX32705

The URL to access this transaction could be of the format:

```
http://n.n.n.n:41001/w2h/WEB3270.htm+Tso5
```

4.3.2. Assigning a LOGMODE by URL parameter

The URL which allows the browser to connect to a host application via VIRTEL may contain a parameter, such as “model5” as shown in this example:

```
http://n.n.n.n:41001/w2h/WEB3270.htm+Tso+model5
```

This form of a VIRTEL URL is described in the section “Dynamic URL with user data”, page 1.

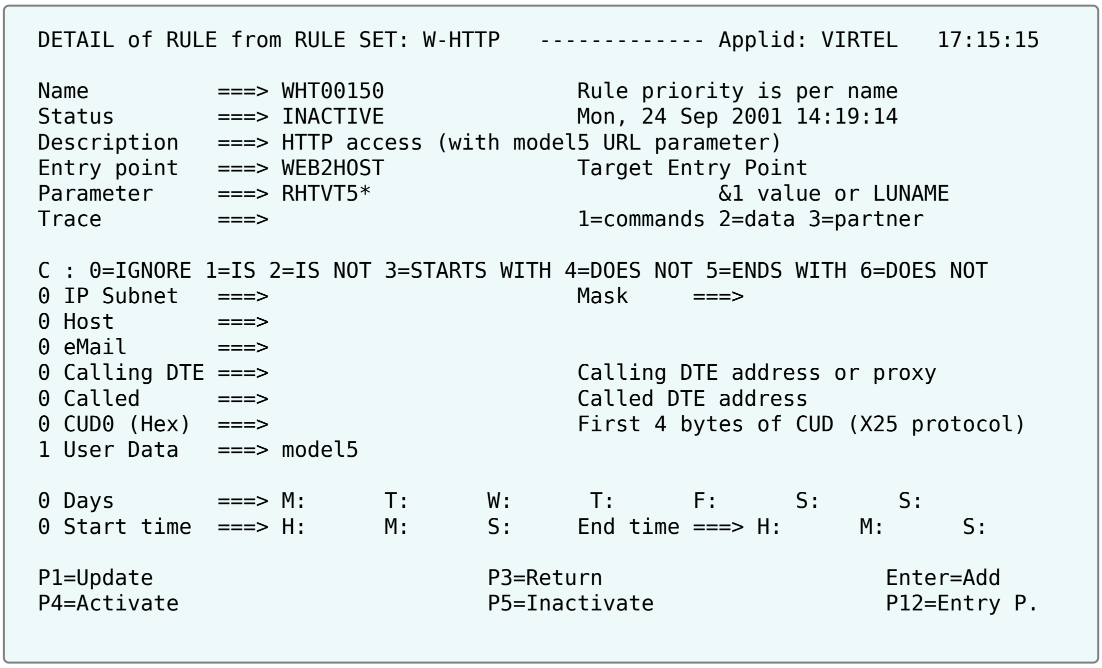
This form of URL is processed by VIRTEL with reference to the “rule set” associated with the HTTP line. VIRTEL looks for a rule whose “User Data” field matches the value of the parameter (model5). The “Parameter” field of the selected rule assigns a relay LU name from the pool defined with logmode SNX32705.

The VTAM definition of the relay pool is shown in the example below. In this example, LU names in the range RHTVT5nn are defined to have the model5 logmode SNX32705:

```
VIRTAPPL VBUILD TYPE=APPL
* ------------------------------------------------------------------ *
* RHTVTxxx    : Relay for VTAM applications acceded by WEB to HOST   *
* ------------------------------------------------------------------ *
* 3270 model 2 terminals
RHTVT0?? APPL  AUTH=(ACQ,PASS),MODETAB=ISTINCLM,DLOGMOD=SNX32702,EAS=1
* 3270 model 5 terminals
RHTVT5?? APPL  AUTH=(ACQ,PASS),MODETAB=ISTINCLM,DLOGMOD=SNX32705,EAS=1
```

VTAM definition of terminal groups

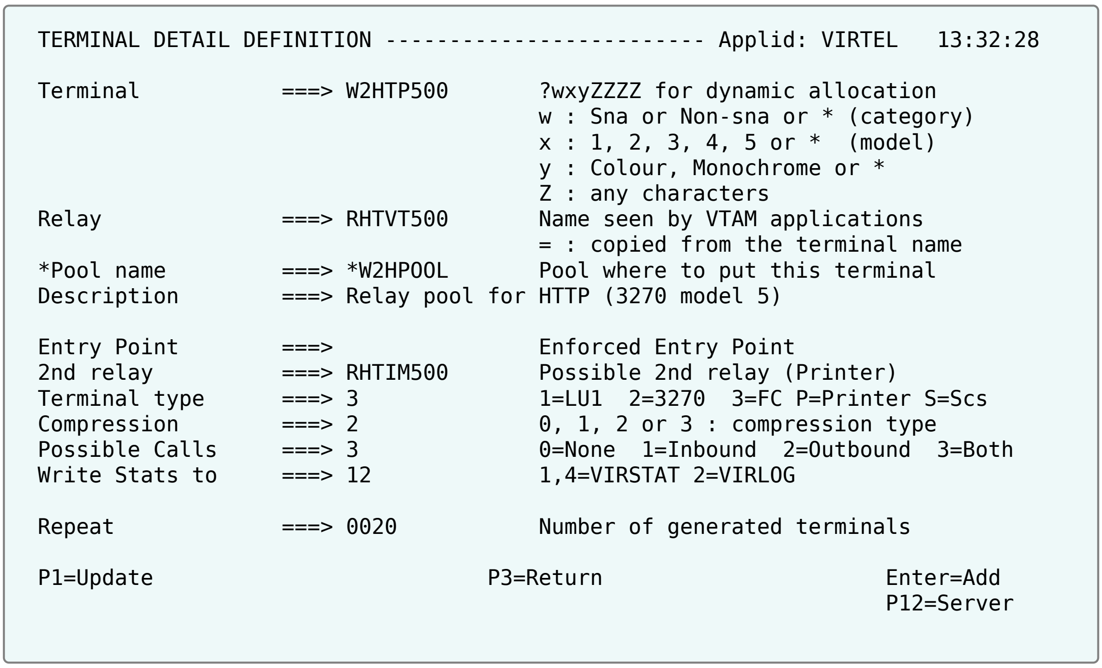
The screen below shows an example rule which assigns a relay LU from the range RHTVT5nn when the URL contains the parameter model5:



```
DETAIL of RULE from RULE SET: W-HTTP   ------------- Applid: VIRTEL   17:15:15

Name          ===> WHT00150               Rule priority is per name
Status        ===> INACTIVE               Mon, 24 Sep 2001 14:19:14
Description   ===> HTTP access (with model5 URL parameter)
Entry point   ===> WEB2HOST               Target Entry Point
Parameter     ===> RHTVT5*                           &1 value or LUNAME
Trace         ===>                        1=commands 2=data 3=partner

C : 0=IGNORE 1=IS 2=IS NOT 3=STARTS WITH 4=DOES NOT 5=ENDS WITH 6=DOES NOT
0 IP Subnet   ===>                        Mask     ===>
0 Host        ===>
0 eMail       ===>
0 Calling DTE ===>                        Calling DTE address or proxy
0 Called      ===>                        Called DTE address
0 CUD0 (Hex)  ===>                        First 4 bytes of CUD (X25 protocol)
1 User Data   ===> model5

0 Days        ===> M:      T:      W:      T:      F:      S:      S:
0 Start time  ===> H:      M:      S:     End time ===> H:      M:      S:

P1=Update                          P3=Return                      Enter=Add
P4=Activate                        P5=Inactivate                  P12=Entry P.
```

Example rule for selection of logmode by URL

The LU name (RHTVT5nn) assigned by the rule must belong to the LU pool shared assigned to the HTTP line, as shown in the example below:



```
TERMINAL DETAIL DEFINITION ------------------------- Applid: VIRTEL   13:32:28

Terminal          ===> W2HTP500       ?wxyZZZZ for dynamic allocation
                                      w : Sna or Non-sna or * (category)
                                      x : 1, 2, 3, 4, 5 or *  (model)
                                      y : Colour, Monochrome or *
                                      Z : any characters
Relay             ===> RHTVT500       Name seen by VTAM applications
                                      = : copied from the terminal name
*Pool name        ===> *W2HPOOL       Pool where to put this terminal
Description       ===> Relay pool for HTTP (3270 model 5)

Entry Point       ===>                Enforced Entry Point
2nd relay         ===> RHTIM500       Possible 2nd relay (Printer)
Terminal type     ===> 3              1=LU1  2=3270  3=FC P=Printer S=Scs
Compression       ===> 2              0, 1, 2 or 3 : compression type
Possible Calls    ===> 3              0=None  1=Inbound  2=Outbound  3=Both
Write Stats to    ===> 12             1,4=VIRSTAT 2=VIRLOG

Repeat            ===> 0020           Number of generated terminals

P1=Update                          P3=Return                      Enter=Add
                                                                  P12=Server
```

Definition of model 5 terminals in the W2HPOOL pool

4.3.3. User-specified LOGMODE

When the entry point definition specifies SCENLOGM in the “Identification scenario” field, the user may override the default logmode by appending an additional parameter LOGMODE=modename to the URL, as shown in this example:

```
http://n.n.n.n:41001/w2h/WEB3270.htm+Tso?logmode=SNX32705
```

The source code for the SCENLOGM scenario is supplied in the VIRTEL SAMPLIB.

Note: To activate this functionality, SCENLOGM must be specified in the “Identification scenario” field of the ENTRY POINT (not the transaction definition)

4.3.4. Dynamic logmode with user-specified screen size

VIRTEL Web Access also supports the use of “dynamic” logmodes, such as D4A32XX3, which allow the user to specify a non-standard alternate screen size. When the entry point definition specifies SCENLOGM in the “Identification scenario” field, the user may also append ROWS and COLS parameters to the URL, as shown in this example:

```
http://n.n.n.n:41001/w2h/WEB3270.htm+Tso?logmode=D4A32XX3&rows=54&cols=132
```

VIRTEL allows a maximum screen size of 62 rows by 160 columns. The host application must also support the use of non-standard screen sizes.

4.4. Session Management In The Application Menu List

When the user connects to the "Application Selection Menu" described ine the "Virtel Web Access User Guide", by default, clicking on an available application will open the session in the current tab replacing the APPMENU application list. You may want to operate differently.

4.4.1. Open session in separate tab

To open each session in separate tabs and keep the application menu available, add the following code in a "custom.js" file:

```
/* To open an application (issued from applist transaction) in a new TAB instead of the same window */
 function before_launchApplink(href) {
   return {
         url: href,          // Return received URL
         target: '_blank'    // Target is a new TAB
   };
}
```

Example of Javascript code to open different sessions in separate tabs

4.4.1.1. Restrictions

Opening simultaneous sessions in different tabs imposes certain restrictions:

- Browsers deliberately limit the opening of multiple simultaneous HTTP sessions on the same domain. This number varies depending on the browser itself and the version used. A detailed census is available on the BrowserScope website.
- Each new session gives rise to the opening of a specific IP socket, and therefore the use of a separate relay terminal for each session. The LU Nailing is therefore not always possible or easy to implement in such situation.

4.5. How To Handle Host Session Termination

When the user terminates the application session by pressing the “Disconnect” button in the browser, various options are available:

- Return to the application selection menu
- Display a specific HTML page
- Close the browser window and return to the desktop

Remember that it is always best to exit cleanly from the host application by pressing the “Disconnect” button, rather than closing the browser window. If the browser window is closed abruptly, the host session resources may not be freed until the expiry of the timeout period specified in the entry point definition.

4.5.1. Return to the application selection menu

When a “Disconnect” request is received, VIRTEL returns to the root URL and displays the default page for the line, which will normally be an application selection menu. For detailed information, see “Virtel URL formats”, page 1.

The user can then choose to connect to the same or a different application by clicking on the appropriate link in the application selection menu.

4.5.2. Displaying a specific page on disconnection

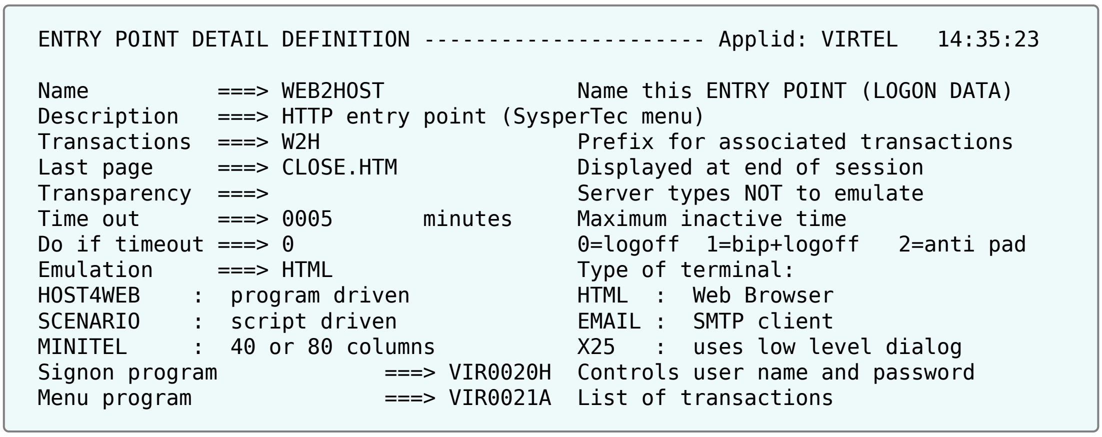
Those sites wishing to display a specific page at the end of a session may use the “Last page” field in the definition of the entry point associated with the HTTP line or the entry point selected by the rules of the line. The “Last page” field indicates the name of the page to be displayed following disconnection from the host application. The indicated file must be uploaded to the same directory as specified in the URL for the host application (for example W2H-DIR if the URL specifies /w2h/WEB3270.htm).

The “Last page” may contain instructions to the user and may include system information provided by VIRTEL (such as the application and terminal name, date and time, etc.)

4.5.3. Closing the browser window automatically

Sites who wish to close the browser window and return to the desktop when the user disconnects from the host application may specify close.htm in the “Last page” field of the entry point definition. This page contains JavaScript code which will attempt to close the current browser window. Depending on the browser version and security settings, the window may close, a prompt may be issued, or the window may remain open. The close.htm page is delivered as standard in the W2H-DIR directory but may be copied to another directory if required.

The figure below shows an example of an entry point definition with close.htm specified as the “Last page”:



```
ENTRY POINT DETAIL DEFINITION ---------------------- Applid: VIRTEL   14:35:23

Name          ===> WEB2HOST                Name this ENTRY POINT (LOGON DATA)
Description   ===> HTTP entry point (SysperTec menu)
Transactions  ===> W2H                     Prefix for associated transactions
Last page     ===> CLOSE.HTM               Displayed at end of session
Transparency  ===>                         Server types NOT to emulate
Time out      ===> 0005        minutes     Maximum inactive time
Do if timeout ===> 0                       0=logoff  1=bip+logoff   2=anti pad
Emulation     ===> HTML                    Type of terminal:
HOST4WEB    :  program driven              HTML  :  Web Browser
SCENARIO    :  script driven               EMAIL :  SMTP client
MINITEL     :  40 or 80 columns            X25   :  uses low level dialog
Signon program             ===> VIR0020H  Controls user name and password
Menu program               ===> VIR0021A  List of transactions
```

```
Identification scenario    ===>           eg XML identification
Type 3 compression         ===>           Discover typical screens  (Virtel/PC)
Mandatory identification   ===>                                 (PC or minitel)
3270 swap key              ===>           eg P24
Extended colors            ===> X         E: extended  X: extended + DBCS

P1=Update                          P3=Return                   P4=Transactions
Enter=Add
```

Example of entry point with last page

5. Security

5.1. How To Activate SSL Using AT-TLS

To provide secure HTTP (https) sessions to client browsers, VIRTEL uses the Application Transparent Transport Layer Security (AT-TLS) feature of z/OS Communication Server. AT-TLS is included with z/OS V1R7 and later releases.

AT-TLS allows socket applications to access encrypted sessions by invoking system SSL within the transport layer of the TCP/IP stack. The Policy Agent decides which connections are to use AT-TLS, and provides system SSL configuration for those connections. The application continues to send and receive clear text over the socket, but data sent over the network is protected by system SSL. The supported protocols are TLS, SSLv3, and SSLv2.

5.1.1. Installation steps

Install Policy Agent procedure

If you do not already have the Communications Server Policy Agent (PAGENT) active in your z/OS system, copy the cataloged procedure EZAPAGSP from TCPIP.SEZAINST into your proclib, renaming it as PAGENT.

Create the Policy Agent configuration file

If you do not already run the Policy Agent, you will need to create a configuration file /etc/pagent.conf using z/OS Unix System Services. If you already run Policy Agent, you will need to find the existing configuration file and add the TTLS definitions to it.

Step PCONFIG in the SSLSETUP sample job contains a starter configuration. The following changes should be made:

- Replace %virtjob% by the name of your VIRTEL started task (SSLSETUP line 70)
- Replace 41000-41002 by 41002 in the LocalPortRange parameter (SSLSETUP line 71) to activate AT-TLS for VIRTEL line C-HTTP
- Replace ServerWithClientAuth by Server in the HandshakeRole parameter (SSLSETUP line 82) as we will not be using Client Certificates.

Allow the Policy Agent to run during TCP/IP initialization

The Policy Agent must be given READ access to the resource EZB.INITSTACK.* in RACF class SERVAUTH. See step EZBAUTH in the SSLSETUP sample job (delivered in VIRTEL SAMPLIB).

Create the server certificate

A server certificate for VIRTEL must be created, signed by a certificate authority, and stored in the RACF database. In the SSLSETUP sample job we create a signing certificate and use RACF itself as the certificate authority. Alternatively, you may use an external certificate authority such as Verisign to create and sign the certificate, then import it into RACF.

At SSLSETUP line 228, replace %virtssl% by the DNS name assigned to the VIRTEL host (for example, virtssl.syspertec.com)

Add the certificate to the keyring

The server certificate must be added to the VIRTRING keyring. See step CCERTIF in the SSLSETUP sample job.

Allow VIRTEL to access its own certificate

To allow VIRTEL to access its own keyring and server certificate, the VIRTEL started task must have READ access to the resource IRR.DIGTCERT.LISTRING in the RACF class FACILITY. See step IRRAUTH in the SSLSETUP sample job.

Activate AT-TLS

To activate AT-TLS, add the following statements to TCPIP PROFILE:

```
TCPCONFIG TTLS
AUTOLOG 5 PAGENT ENDAUTOLOG
```

Stop and restart TCP/IP to activate the TCPCONFIG TTLS profile statement. The AUTOLOG statement will cause the PAGENT procedure to be started automatically during TCP/IP initialization.

5.1.2. Operations

Starting the Policy Agent

The AUTOLOG statement in the TCP/IP profile will start the PAGENT procedure automatically at TCP/IP initialization. Alternatively you can issue the MVS command S PAGENT.

Note: if this is the first time you have activated the SERVAUTH class, you are likely to see RACF failure messages during TCP/IP initialization indicating that other applications are unable to access the resource EZB.INITSTACK. This is normal, because Communications Server uses this mechanism to prevent applications from accessing TCP/IP before the Policy Agent is started. Do not be tempted to authorize applications to use this RACF resource. Either ignore the messages (they will go away once PAGENT has started), or ensure that PAGENT starts before all other applications.

Altering the Policy Agent configuration

To make changes to the Policy Agent configuration file, either edit and resubmit the PCONFIG step of the SSLSETUP sample job, or use the TSO ISHELL command to edit the file /etc/pagent.conf directly from ISPF.

After you make changes to the Policy Agent configuration, use the MVS command F PAGENT,REFRESH to force PAGENT to reread the file.

Logon to VIRTEL using secure session

To access VIRTEL line C-HTTP you must now use URL https://n.n.n.n:41002 instead of http://n.n.n.n:41002 (where n.n.n.n is the IP address of the z/OS host running VIRTEL).

5.1.3. Problem determination

Policy Agent log file

Policy Agent startup messages are written to the /tmp/pagent.log file of z/OS Unix System Services. You can use the TSO ISHELL command to browse this file from ISPF.

Common error messages

Error messages relating to session setup are written to the MVS SYSLOG. The most common error message is:

```
EZD1287I TTLS Error RC: nnn event
```

where nnn represents a return code. Return codes under 5000 are generated by System SSL and are defined in the System SSL Programming manual. Return codes over 5000 are generated by AT-TLS and are defined in the IP Diagnosis Guide. Some commonly encountered return codes are:

- **7** No certificate
- **8** Certificate not trusted
- **109** No certification authority certificates
- **202** Keyring does not exist
- **401** Certificate expired or not yet valid
- **402** or **412** Client and server cannot agree on cipher suite
- **416** VIRTEL does not have permission to list the keyring
- **431** Certificate is revoked
- **434** Certificate key not compatible with cipher suite
- **435** Certificate authority unknown
- **5003** Browser sent clear text (http instead of https)

Cipher suite

The client and server cipher specifications must contain at least one value in common. The TTLSEnvironmentAdvancedParms parameter of the Policy Agent configuration file allows you to turn on or off the SSLv2, SSLv3, and TLSv1 protocols at the server end. The list of supported cipher suites for each protocol is in the TTLSCipherParms parameter. Check the /tmp/pagent.log file to determine whether any cipher suites were discarded at startup time.

In Microsoft Internet Explorer, follow the menu Tools – Internet Options – Advanced. Under the security heading there are three options which allow you to enable or disable the SSL 2.0, SSL 3.0, and TLS 1.0 protocols. You cannot enable or disable individual cipher suites.

In Firefox the cipher specifications are accessed by typing about:config in the address bar and typing security in the filter box. By default, ssl2 is disabled, and ssl3 and tls are enabled. By default, all weak encryption cipher suites are disabled, and 128-bit or higher cipher suites are enabled.

5.1.4. Bibliography

- ***SA22-7683-07 z/OS V1R7 Security Server: RACF Security Administrator's Guide*** Chapter 21. RACF and Digital Certificates
- ***SC24-5901-04 z/OS V1R6 Cryptographic Services: System SSL Programming*** Chapter 12. Messages and Codes
- ***SC31-8775-07 z/OS V1R7 Communications Server: IP Configuration Guide*** Chapter 14. Policy-based networking Chapter 18. Application Transparent Transport Layer Security (AT-TLS) data protection
- ***SC31-8776-08 z/OS V1R7 Communications Server: IP Configuration Reference*** Chapter 21. Policy Agent and policy applications
- ***GC31-8782-06 z/OS V1R7 Communications Server: IP Diagnosis Guide*** Chapter 28. Diagnosing Application Transparent Transport Layer Security (AT-TLS)
- ***SC31-8784-05 z/OS V1R7 Communications Server: IP Messages: Volume 2 (EZB, EZD)*** Chapter 10. EZD1xxxx messages

5.2. SSL - Signing On Using Server And Client Certificates

In this section we look at setting up Virtel to work with client and user certificates and to effectively remove the need for a user to provide a user id and password. This is equivalent to the Express Logon Feature (ELF) provided by Host on Demand and other Telnet clients.

First, let’s review what is going on behind the scenes with certificate authentication and X.509 certificate validation within TLS/SSL. The guiding principle here is that Public Key Infrastructure (PKI) requires that data encrypted with a public key can only be decrypted with a private key and data encrypted with a private key can only be decrypted with a public key. The secure session (https) that runs between the browser and Virtel uses the Application Transparent Transport Layer Security feature of z/OS Communications Server, also known as AT-TLS. AT-TLS allows socket applications to access encrypted sessions by invoking Secure Socket Layer (SSL) within the transport layer of the TCP/IP stack. A policy agent (PAGENT) is used to configure AT-TLS using parameter statements which will determine which sessions are to use AT-TLS.

AT_TLS inserts itself in the connection between the application and browser. This means that the application will send and receive clear text over the socket interface, but data over the network is encrypted by system SSL. System SSL has three supported protocol levels:

- TLSv1
- SSLv2
- SSLv3

In this configuration we will be using SSLv3.

The server / client process, which in Virtel’s case is the Virtel started task (server) and the browser (client), implements the following SSL protocol or handshake during the “hello” phase of establishing a secure session:

1. The Client contacts the Server ;
2. The Server sends a certificate;
3. Server authentication is performed by the Client ;
4. Client sends the certificate;
5. Client authentication is performed by the Server ;
6. An encryption algorithm and single key is chosen to encrypt / decrypt data

The purpose of the authentication is to ensure that the server/client are in fact who they say they are. This is to ensure that they server/client private and public keys haven’t been stolen and are purporting to be an entity that they aren’t and thereby compromising security. Authentication uses X.509 digital certificates. Further details of this handshake and the certificate exchange can be found in Appendix B. TLS/SSL Security z/OS Communications Server: IP Configuration Guide.

5.2.1. Certificates

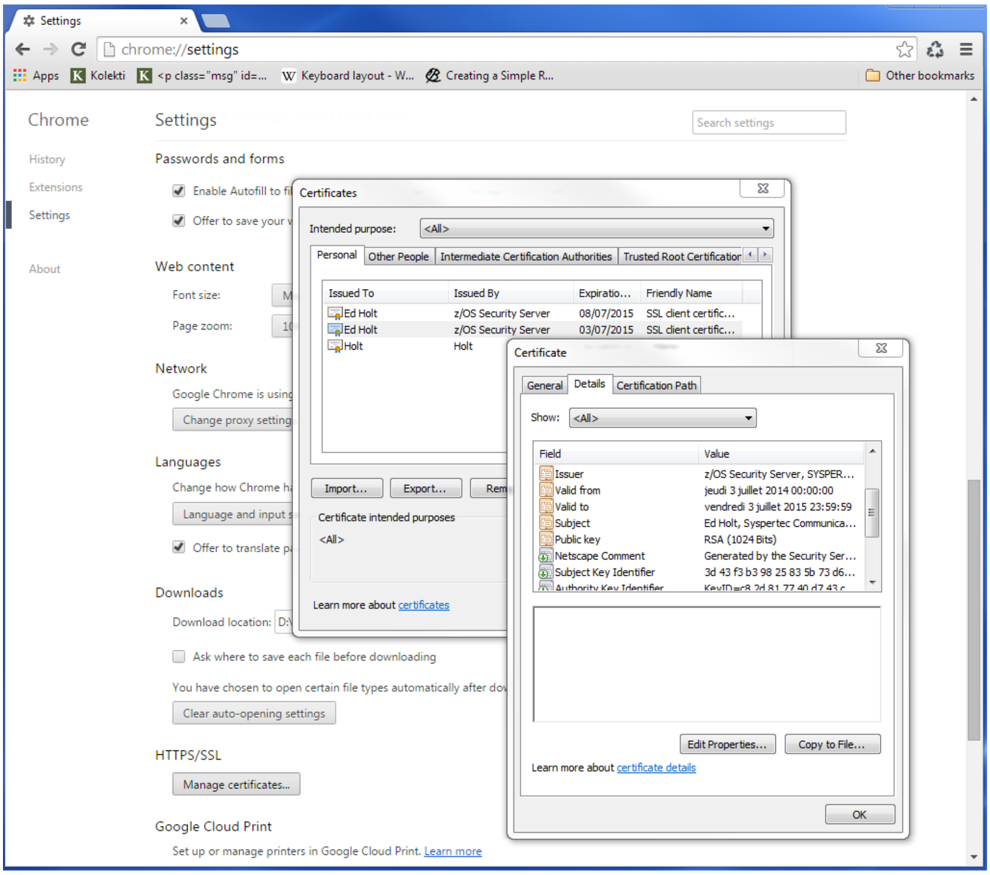
What’s in a X.509 certificate?

Amongst other things it includes the Distinguished Name of the Server (DNS), the public key of the Server, Distinguished Name of the Server organization issuing the certificate and the issuer’s signature. If we look at a certificate held with RACF we can see this information. Certificates are identified by a combination of LABEL, USERID or Certification Authority (CA).

```
READY
  RACDCERT ID(SPVIRSTC) LIST(LABEL('VIRTEL SSL DEMO'))
Digital certificate information for user SPVIRSTC:

  Label: VIRTEL SSL DEMO
  Certificate ID: 2Qji1+XJ2eLjw+XJ2ePF00Di4tNAxMXU1kBA
```

```
Status: TRUST
Start Date: 2014/07/08 00:00:00
End Date: 2015/07/08 23:59:59
Serial Number:
     >05<
Issuer's Name:
     >CN=z/OS Security Server.O=SYSPERTEC.C=FR<
Subject's Name:
     >CN=RECETTE VIRTEL.T=VIRTEL Web Access.O=SYSPERTEC.C=FR<

Key Usage: HANDSHAKE, DATAENCRYPT
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
  Ring Owner: SPVIRSTC
  Ring:
     >VIRTRING<
```

Similar details can be found in the browser settings. For example here is what Chrome displays in the HTTPS/SSL certificate database.



Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Ed Holt	z/OS Security Server	08/07/2015	SSL client certific...
Ed Holt	z/OS Security Server	03/07/2015	SSL client certific...
Holt	Holt		

Show: <All>

Field	Value
Issuer	z/OS Security Server, SYSPER...
Valid from	jeudi 3 juillet 2014 00:00:00
Valid to	vendredi 3 juillet 2015 23:59:59
Subject	Ed Holt, Syspertec Communica...
Public key	RSA (1024 Bits)
Netscape Comment	Generated by the Security Ser...
Subject Key Identifier	3d 43 f3 b3 98 25 83 5b 73 d6...
Authority Key Identifier	KeyID=c8 2d 81 77 40 d7 43 c

Types of certificates

- Client certificate
- Server certificate
- Well-known Certificate Authority (CA) Signing certificate
- RACF signing certificate

In this configuration we will be using self-signed server and client certificates. In most installation you would use server and client certificates signed by a well-known CA. These well-known CA certificates are normally available in the RACF and browser key data bases.

Configuring the certificates

The first step is to create the necessary certificates. We require a server certificate, a RACF signing certificate and a user certificate.

In the Virtel SAMPLIB there is a member called SSLSETUP. This will initialize the SSL environment and create the RACF signing certificate. Some of the steps may or may not be relevant so you will need to customize SSLSETUP accordingly. For example, you might already be running the PAGENT started task and have RACF definitions in place to support the required SSL access.

The following is the certificate generation statement for the RACF signing certificate.

```
//DCERTCA EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
/*-----------------------------------------------------------------*/
/* Delete previous signing certificate */
/*-----------------------------------------------------------------*/
  RACDCERT CERTAUTH +
  DELETE(LABEL('z/OS signing certificate'))
//*----------------------------------------------------------------*
//* CCERTCA : CREATE SIGNING CERTIFICATE *
//*----------------------------------------------------------------*
//CCERTCA EXEC PGM=IKJEFT1A
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
/*-----------------------------------------------------------------*/
/* Create a signing certificate */
/*-----------------------------------------------------------------*/
  RACDCERT CERTAUTH +
           GENCERT +
           WITHLABEL('z/OS signing certificate') +
           SUBJECTSDN( +
                   CN('z/OS Security Server') +
                    O('SYSPERTEC') +
                    C('FR')) +
           KEYUSAGE(CERTSIGN) SIZE(1024) +
           NOTAFTER(DATE(2026-06-30))
```

If we list the certificate after we have created it will get the following:

```
READY
  RACDCERT CERTAUTH LIST(LABEL('z/OS signing certificate'))

Digital certificate information for CERTAUTH:

  Label: z/OS signing certificate
  Certificate ID: 2QiJmZmDhZmjgalh1uJAoomHlYmVh0CDhZmjiYaJg4GjhUBA
  Status: TRUST
  Start Date: 2013/07/03 00:00:00
  End Date: 2026/06/30 23:59:59
  Serial Number:
       >00<
  Issuer's Name:
       >CN=z/OS Security Server.O=SYSPERTEC.C=FR<
  Subject's Name:
       >CN=z/OS Security Server.O=SYSPERTEC.C=FR<
  Key Usage: CERTSIGN
  Key Type: RSA
  Key Size: 1024
  Private Key: YES
  Ring Associations:
  Ring Owner: SPVIRSTC
  Ring:
     >VIRTRING<
```

The key usage identifies this certificate as a signing certificate. This certificate will be used to sign other certificates that we generate.

Next is the server certificate. Again we use RACF to generate the certificate and use the RACF signing certificate to "sign" it. The following extract is from the Virtel SAMPLIB member SSLUCERT.

```
//CCERTIF EXEC PGM=IKJEFT1A
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
/*-----------------------------------------------------------------*/
/* Create a digital certificate */
/*-----------------------------------------------------------------*/
  RACDCERT ID(SPVIRSTC)         /* VIRTEL userid */           +
           GENCERT                                            +
           WITHLABEL('VIRTEL SSL DEMO')                       +
           SIGNWITH(CERTAUTH LABEL('z/OS signing certificate')) +
           SUBJECTSDN(                                        +
                   CN('RECETTE VIRTEL')                       +
                    T('VIRTEL Web Access')                    +
                    O('SYSPERTEC')                            +
                    C('FR'))                                  +
           KEYUSAGE(HANDSHAKE DATAENCRYPT) SIZE(1024)
```

Note how we identify the signing certificate with the ***SIGNWITH*** *parameter using the same label information that we used when defining the RACF signing certificate.*

Key rings

Having generated two of our certificates we now need a place to keep them. We place the certificates on a key ring and associate the key ring with the VIRTEL server RACF user id (in our case SPVIRSTC). The member SSLSETUP has some RACF commands to perform the key ring generation. Here is an extract:

```
/*-----------------------------------------------------------------*/
/* Create a keyring */
/*-----------------------------------------------------------------*/
  RACDCERT ID(SPVIRSTC) /* VIRTEL userid */                   +
  ADDRING(VIRTRING)
/*-----------------------------------------------------------------*/
/* Add the certificate to the keyring */
/*-----------------------------------------------------------------*/
  RACDCERT ID(SPVIRSTC) /* VIRTEL userid */                   +
  CONNECT(                                                    +
  ID(SPVIRSTC)                                                +
  LABEL('VIRTEL SSL DEMO')                                    +
  RING(VIRTRING)                                              +
  DEFAULT)
```

Again it is the label that identifies the key(certificate) that we want to add to the key ring owned by user SPVIRSTC.

User Certificate

The next step is to create a user certificate which we will export and import into our browser's key data base. In the Virtel SAMPLIB member SSLUCERT performs the task of creating the user certificate and creating an "exportable" file.

```
//*----------------------------------------------------------------*
//* Associate certificate with user id *
//*----------------------------------------------------------------*
//UCERTIF EXEC PGM=IKJEFT1A
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
/*-----------------------------------------------------------------*/
/* Add certificate to Server ring */
/*-----------------------------------------------------------------*/
  RACDCERT ID(SPVIRSTC) /* client userid */                     +
  CONNECT (CERTAUTH                                             +
  LABEL('z/OS signing certificate')                             +
  RING(VIRTRING)                                                +
  USAGE(CERTAUTH))
/*-----------------------------------------------------------------*/
/* Add certificate to Server ring */
/*-----------------------------------------------------------------*/
  RACDCERT ID(SPVIRSTC) /* client userid */                     +
  CONNECT (ID(SPTHOLT)                                          +
  LABEL('SSL client certificate')                               +
  RING(VIRTRING)                                                +
  USAGE(CERTAUTH))
/*-----------------------------------------------------------------*/
/* Refresh the RACF profiles */
/*-----------------------------------------------------------------*/
  SETROPTS RACLIST(DIGTRING) REFRESH
  SETROPTS RACLIST(DIGTCERT) REFRESH
```

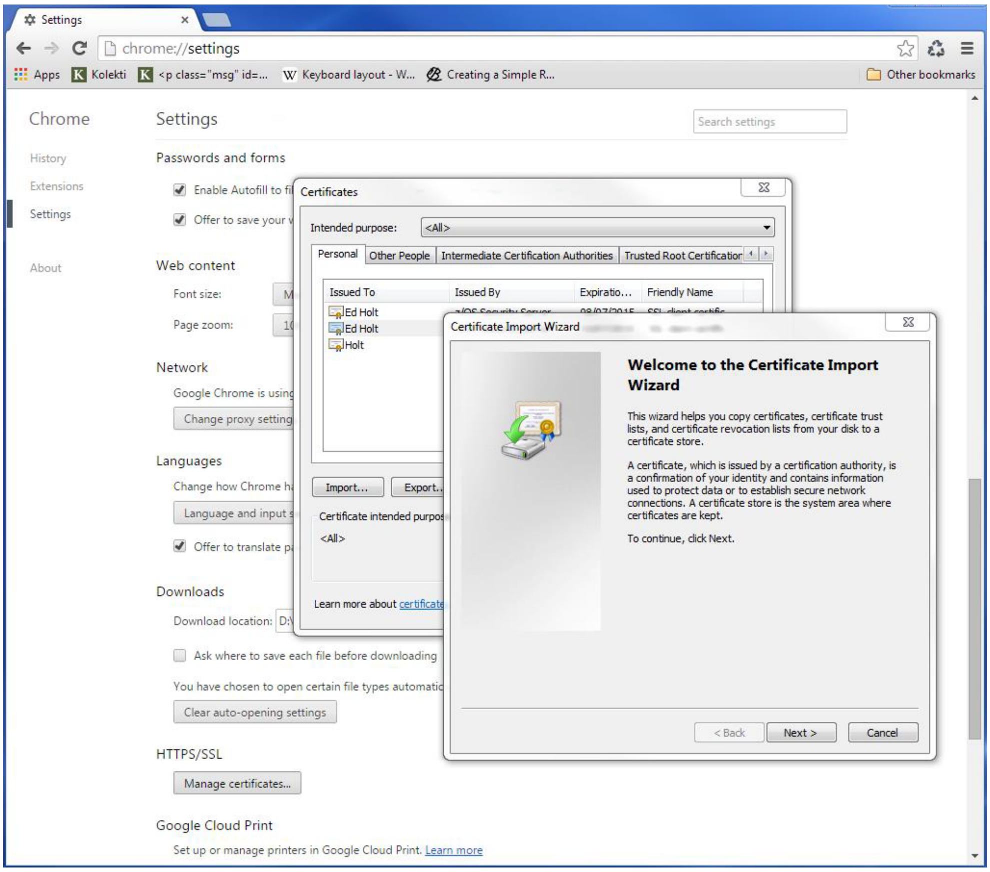
The "CONNECT CERTAUTH" tells RACF that this is a signing CA certificate and the "CONNECT ID(SPTHOLT) indicates that the certificate labelled 'SSL client certificate' is associated with USERID SPTHOLT. This is how Virtel obtains the USERID. Also, note that we refresh the RACF profiles related to certificates and key rings.

If we list our key ring for user SPVIRSTC we should have three certificates.

```
READY
RACDCERT ID(SPVIRSTC) LISTRING(VIRTRING)
Digital ring information for user SPVIRSTC:
Ring:
>VIRTRING<
Certificate Label Name Cert Owner USAGE DEFAULT
-------------------------------- ------------ -------- -------
VIRTEL SSL DEMO ID(SPVIRSTC) PERSONAL YES
z/OS signing certificate CERTAUTH CERTAUTH NO
SSL client certificate ID(SPTHOLT) CERTAUTH NO
```

Importing the certificate on the client work station.

To import the user certificate into the client workstation the P12 file must be downloaded in binary and then the certificate import wizard is run to import the certificate.



Settings

☑ Enable Autofill to fi

☑ Offer to save your

Google Chrome is using

Change how Chrome h

☑ Offer to translate p

□ Ask where to save each file before downloading

You have chosen to open certain file types automatic

Clear auto-opening settings

Set up or manage printers in Google Cloud Print. Learn more

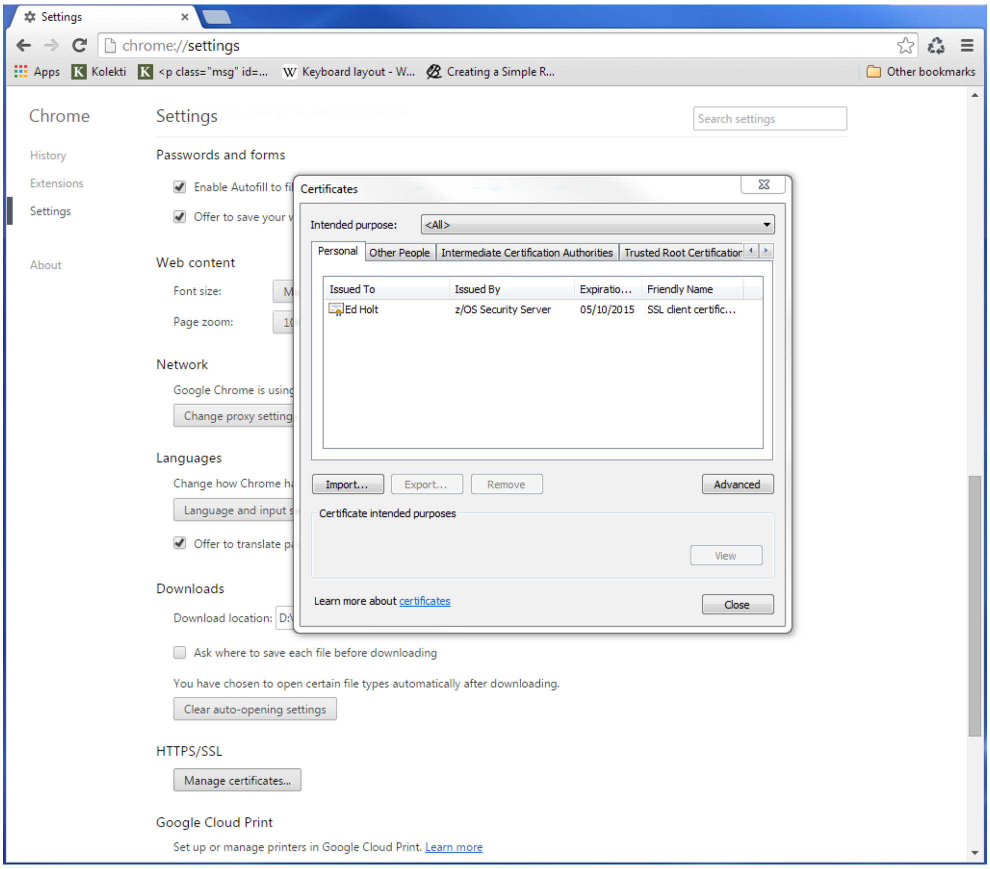
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

After importing the following panel is displayed:



Settings

☑ Enable Autofill to fi

☑ Offer to save your

Google Chrome is using

Change how Chrome h

☑ Offer to translate p

□ Ask where to save each file before downloading

You have chosen to open certain file types automatically after downloading.

Clear auto-opening settings

Set up or manage printers in Google Cloud Print. Learn more

Certificates

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Ed Holt	z/OS Security Server	05/10/2015	SSL client certific...

Certificate intended purposes

Learn more about certificates

At this stage we have completed our certificate generation. Through the use of the certificates we will be able to initiate a secure session (https) with an application and obtain a user id.

PassTicket support

The next step is to obtain a pass ticket in place of a password so that Virtel can log on to the target application and present a user id and password combination on behalf of the user. The following job will enable PassTicket support for our target application SPCICSH and using user id SPVIRSTC, out Virtel server user id. This job will have to be customized accordingly:

```
//STEP1 EXEC PGM=IKJEFT1A,DYNAMNBR=20
//* RDEFINE FACILITY IRR.RTICKETSERV
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
  SETROPTS CLASSACT(APPL)
  SETROPTS CLASSACT(PTKTDATA)
  SETROPTS RACLIST(PTKTDATA)
  SETROPTS GENERIC(PTKTDATA)
  RDELETE PTKTDATA SPCICSH
  RDELETE PTKTDATA IRRPTAUTH.SPCICSH.*
  RDEFINE PTKTDATA IRRPTAUTH.SPCICSH.* UACC(NONE)
  RDEFINE PTKTDATA SPCICSH SSIGNON(KEYMASKED(998A654FEBCDA123)) +
  UACC(NONE)
//STEP1 EXEC PGM=IKJEFT1A,DYNAMNBR=20
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
  PERMIT IRR.RTICKETSERV CL(FACILITY) ID(SPVIRSTC) ACC(READ)
  PERMIT IRRPTAUTH.SPCICSH.* CL(PTKTDATA) ID(SPVIRSTC) ACC(UPDATE)
  SETROPTS REFRESH RACLIST(PTKTDATA)
  SETROPTS REFRESH RACLIST(FACILITY)
```

In order for Virtel to generate PassTickets, you must also modify your VIRTCT to include the parameter PASSTCK=YES and then reassemble the VIRTCT. See chapter 6 of the Virtel Installation Guide for more details on the Virtel VIRTCT.

PAGENT Configuration

To enable system SSL sessions to take place between the browser and the application we have to tell AT-TLS and SSL which sockets to intercept. This is configured in the pagent configuration file which can be found in /etc/pagent.conf. The two areas that we are interested in are the TTLSEnvironmentAction section and the TTLSRule section.

```
TTLSEnvironmentAction             VIRTELenvir_inSec
{

         HandshakeRole            ServerWithClientAuth
         Trace                    7
         TTLSKeyringParms
         {
             Keyring              VIRTRING
         }
         TTLSEnvironmentAdvancedParms
         {
             SSLv2                On
             SSLv3                On
             TLSv1                On
             ClientAuthType       SAFCheck
         }
         TTLSCipherParmsRef       VIRTELcipher
}
```

```
../..
TTLSRule                          VIRTELrule_in_eh
{
         Jobname                  SPVIREH
         LocalPortRange           41002
         Direction                Inbound
         TTLSGroupActionRef       VIRTELgroup
         TTLSEnvironmentActionRef VIRTELenvir_inSec
}
```

The TTLS Rule identifies Virtel Started task name via the Jobname parameter and also the port number that can support secured sessions _ https. In this case it is port 41002.

The rules section also identifies the environmental section. In this case we have selected an environment section called VIRTELenvir_insec.

In VIRTELenvir_insec we identify that we want to use both server and client certificates

```
  HandShakeRole        ServerWithClientAuth
```

That the user certificate must be associated with a valid RACF userid

```
  ClientAuthType       SAFCheck
```

The name of the keyring that holds the keys(certificates)

```
  Keyring              VIRTRING
```

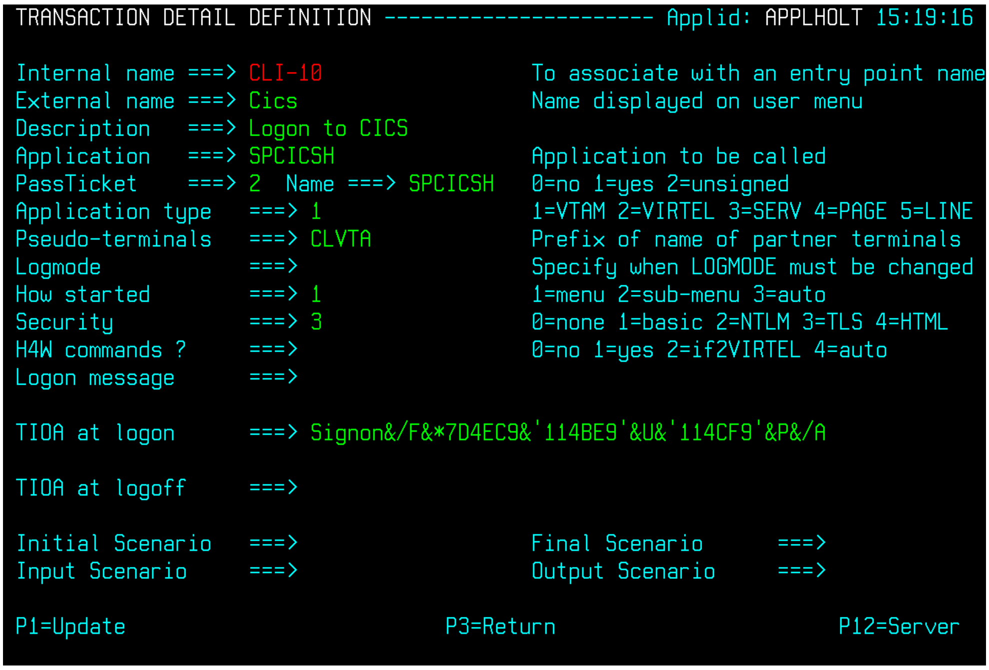
A default pagent.conf is shipped with the SAMPLIB member SSLSETUP which you can use to modify accordingly to define the above SSL sections.

To refresh a pagent.conf profile after you have made changes you can issue the following z/OS command:

```
F PAGENT,REFRESH
```

Virtel Configuration

The final part in our configuration is to configure Virtel to use SSL to obtain the user id and PassTicket support to create a password. We configure Virtel in the transaction associated with our target application, in this case the CICS application called SPCICSH.



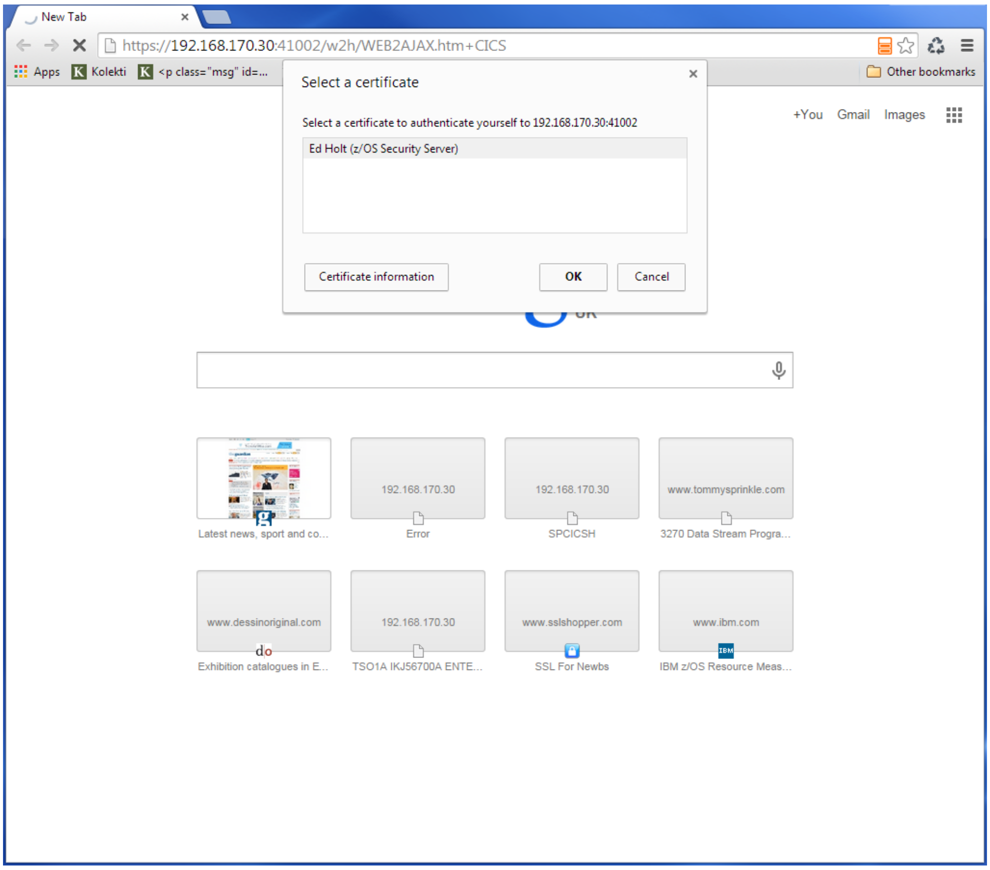
```
TRANSACTION DETAIL DEFINITION ---------------------- Applid: APPLHOLT 15:19:16

Internal name ===> CLI-10                     To associate with an entry point name
External name ===> Cics                       Name displayed on user menu
Description   ===> Logon to CICS
Application   ===> SPCICSH                    Application to be called
PassTicket    ===> 2  Name ===> SPCICSH       0=no 1=yes 2=unsigned
Application type    ===> 1                    1=VTAM 2=VIRTEL 3=SERV 4=PAGE 5=LINE
Pseudo-terminals    ===> CLVTA                Prefix of name of partner terminals
Logmode             ===>                      Specify when LOGMODE must be changed
How started         ===> 1                    1=menu 2=sub-menu 3=auto
Security            ===> 3                    0=none 1=basic 2=NTLM 3=TLS 4=HTML
H4W commands ?      ===>                      0=no 1=yes 2=if2VIRTEL 4=auto
Logon message       ===>

TIOA at logon       ===> Signon&/F&*7D4EC9&'114BE9'&U&'114CF9'&P&/A

TIOA at logoff      ===>

Initial Scenario    ===>                      Final Scenario      ===>
Input Scenario      ===>                      Output Scenario     ===>

P1=Update                          P3=Return                          P12=Server
```

Note that PassTicket is set to 2. This will enable Virtel to generate a temporary password. Security is set to 3. This indicates that Virtel will receive a USERID based upon the user certificate used in the authentication process. The TIOA at logon is a string that will logon to the CICS application using the user id and password values that Virtel has obtained.

With this configuration we can logon to our CICS application without the user presenting any user id or password. This is very much like the Express Logon Facility implemented in our Telnet clients.

Logon Example

In the following screen shots we demonstrate logging into a CICS application via a secure session (https) without specifying any user id/password. Our initial URL is https://192.168.170.30:41002/w2h/WEB2AJAX.htm+CICS; you will replace the IP address with your own installation IP address or domain name.



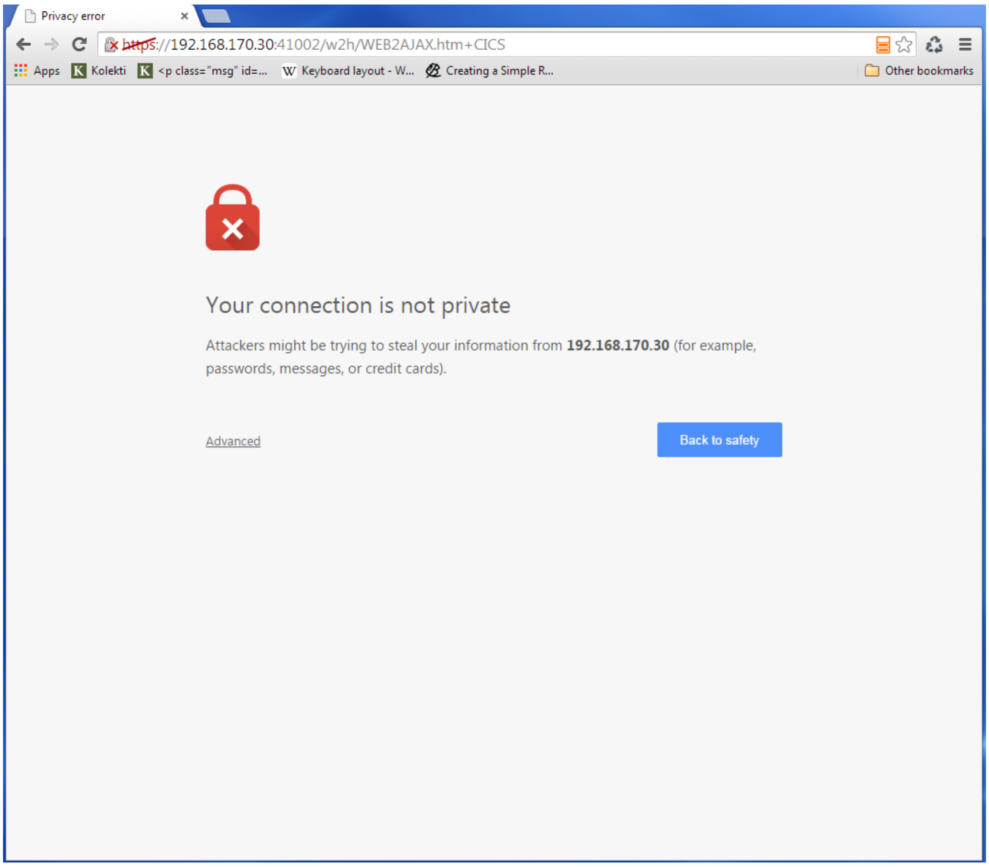
Select a certificate

Select a certificate to authenticate yourself to 192.168.170.30:41002

Ed Holt (z/OS Security Server)

We are presented with a « Select a certificate » window from the browser requesting the certificate we wish to user for authenication purposes. We select the certificate we downloaded.

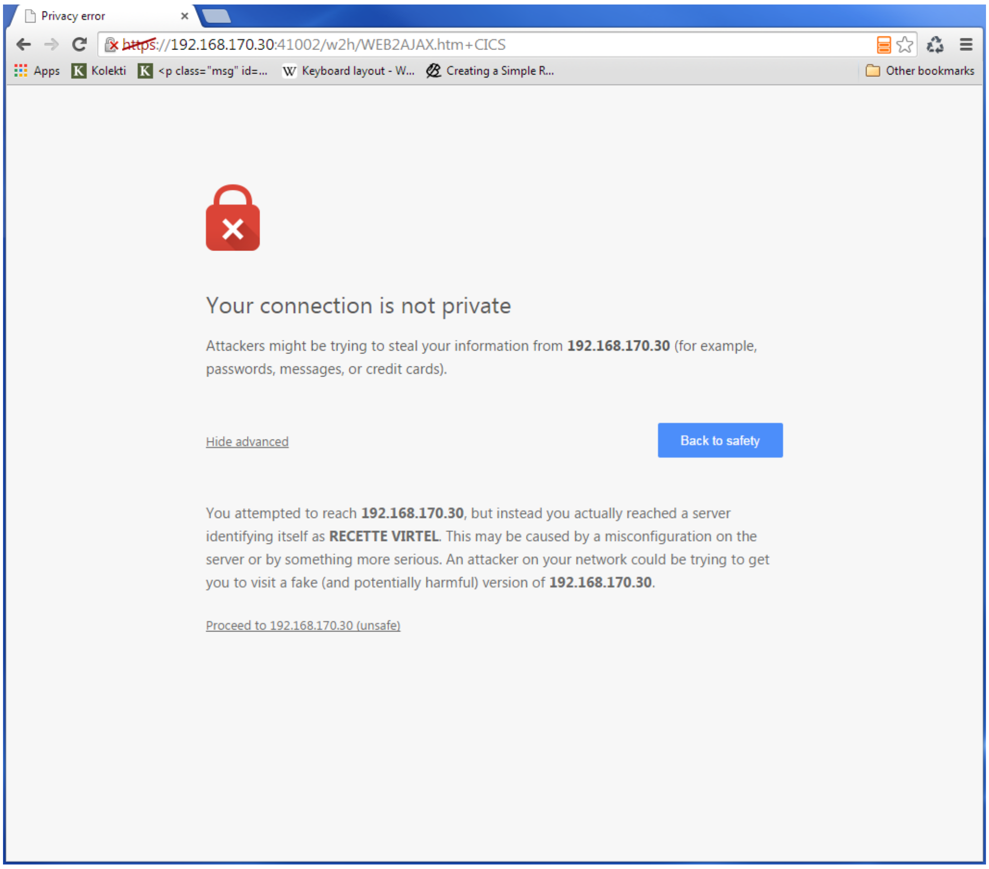
The next panel is a warning panel which identifes that the certificate we are using has not been authenticated by a well-known CA authority. We are of course aware of this as we are using a RACF self signed certifcate.



Your connection is not private

Attackers might be trying to steal your information from **192.168.170.30** (for example, passwords, messages, or credit cards).

We select Advanced and are then presented with information about the certificate.

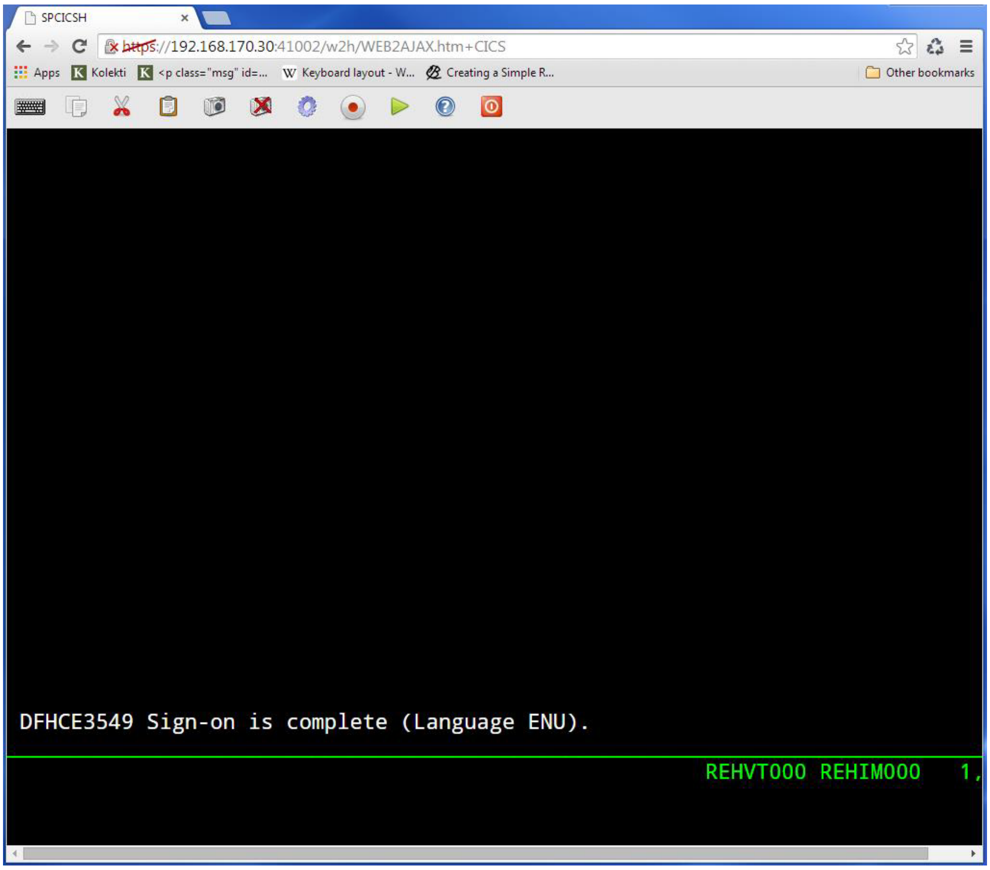


Your connection is not private

Attackers might be trying to steal your information from **192.168.170.30** (for example, passwords, messages, or credit cards).

You attempted to reach **192.168.170.30**, but instead you actually reached a server identifying itself as **RECETTE VIRTEL**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **192.168.170.30**.

We select the “Proceed” link.



```
DFHCE3549 Sign-on is complete (Language ENU).
                                                REHVT000 REHIM000    1,
```

We are signed into CICS without having to specify any user id or password.

Problems

It is easy to miss something when configuring user certificate sign on. Here are some general guidelines that should help in debugging configuration errors.

1. Is AT-TLS active.

   Issue the following z/OS command – D TCPIP,,N,TTLS

   The response should be :

```
EZD0101I NETSTAT CS V1R13 TCPIP 706
TTLSGRPACTION                       GROUP ID      CONNS
VIRTELGROUP                         00000002      3
1 OF 1 RECORDS DISPLAYED
END OF THE REPORT
```

2. PAGENT return codes

   Common session startup/handshake errors are reported through messqge EZD1287I. In the example below we can see that the handshake has failed with a return code of 5003. Return codes under 5000 are generated by System SSL and are defined in the System SSL Programming manual. Return codes over 5000 are generated by AT-TLS and are defined in the IP Diagnosis Guide. In the following the 5013 suggests that the browser has sent clear text; in other words, http was used instead of https in the URL.

```
BPXF024I (TCPIP) Oct 7 13:33:08 TTLS 83951769 : 15:33:08 TCPIP 367
EZD1281I TTLS Map CONNID: 000006A2 LOCAL: 192.168.170.30..41002
REMOTE: 192.168.92.62..57545 JOBNAME: SPVIREH USERID: SPVIRSTC TYPE:
```

```
InBound STATUS: Enabled RULE: VIRTELrule_in_eh ACTIONS: VIRTELgroup
VIRTELenvir_inSec **N/A**
BPXF024I (TCPIP) Oct 7 13:33:08 TTLS 83951769 : 15:33:08 TCPIP 368
EZD1286I TTLS Error GRPID: 00000002 ENVID: 00000000 CONNID: 000006A2
LOCAL: 192.168.170.30..41002
REMOTE: 192.168.92.62..57545
JOBNAME: SPVIREH USERID: SPVIRSTC
RULE: VIRTELrule_in_eh
RC: 5003 Data Decryption EZD1287I TTLS Error RC: 5003 Data Decryption 369
LOCAL: 192.168.170.30..41002
REMOTE: 192.168.92.62..57545
JOBNAME: SPVIREH RULE:
VIRTELrule_in_eh USERID:
SPVIRSTC GRPID: 00000002
ENVID: 00000000
CONNID: 000006A2
```

Common PAGENT return codes:

- **7** No certificate
- **8** Certificate not trusted
- **109** No certification authority certificates
- **202** Keyring does not exist
- **401** Certificate expired or not yet valid
- **402** or **412** Client and server cannot agree on cipher suite
- **416** VIRTEL does not have permission to list the keyring
- **431** Certificate is revoked
- **434** Certificate key not compatible with cipher suite
- **435** Certificate authority unknown
- **5003** Browser sent clear text (http instead of https)

3. Virtel messages

VIRHT57E LINE IS NOT SET UP FOR HTTPS

This means that the browser has sent encypted text (https) but that AT-TLS has not decrypted it before sending it to VIRTEL. The PAGENT rules haven't correctly identified this port as a SSL jobname/port. Check the /etc/pagent.conf member. The message is a bit misleading as there is no line setup required by Virtel.

Normally AT-TLS is transparent to VIRTEL. AT-TLS performs the decryption and transforms the https request into an http request before passing it to VIRTEL. The only case where VIRTEL is AT-TLS aware is when the VIRTEL transaction definition specifies SECURITY=3 (TLS) and in this case VIRTEL will check that the session has been processed by AT-TLS and will issue an IOCTL to obtain the userid associated with the certificate.

In the normal case, you should specify HandshakeRole Server, ClientAuthType Full, and ApplicationControlled Off in the AT-TLS rules, as in the example in VIRT447.SAMPLIB(SSLSETUP). VIRTEL does not issue an IOCTL to turn decryption on and off, so if you specified ApplicationControlled On then you would get VIRHT57E because AT-TLS has not been instructed to start decryption.

If you still get an error when you have ApplicationControlled Off then we will need to see the SYSLOG (for the EZD TTLS messages), the JESMSGLG from the VIRTEL started task, and the SYSPRINT resulting from a z/OS command F VIRTEL,SNAP immediately after the error occurs. We would also like to see the exact URL which was entered at the browser, as well as the AT-TLS pagent.conf file.

z/OS IBM References

- ***SA22-7683-07 z/OS V1R7 Security Server: RACF Security Administrator's Guide*** Chapter 21. RACF and Digital Certificates
- ***SC24-5901-04 z/OS V1R6 Cryptographic Services: System SSL Programming*** Chapter 12. Messages and Codes
- ***SC31-8775-07 z/OS V1R7 Communications Server: IP Configuration Guide*** Chapter 14. Policy-based networking Chapter 18. Application Transparent Transport Layer Security (AT-TLS) data protection
- ***SC31-8776-08 z/OS V1R7 Communications Server: IP Configuration Reference*** Chapter 21. Policy Agent and policy applications
- ***GC31-8782-06 z/OS V1R7 Communications Server: IP Diagnosis Guide*** Chapter 28. Diagnosing Application Transparent Transport Layer Security (AT-TLS)
- ***SC31-8784-05 z/OS V1R7 Communications Server: IP Messages: Volume 2 (EZB, EZD)*** Chapter 10. EZD1xxxx messages

Virtel References

- ***VIRTEL Installation Guide*** PASSTCK parameter
- ***VIRTEL Connectivity Reference*** Transactions – PassTicket Parameter / Transactions – Security Parameter
- ***VIRTEL Web Access Guide*** Security – Data encryption by SSL