

---

# z/OS Communications Server

## Password phrase support in FTP and TN3270E



© 2011 IBM Corporation

This presentation provides an overview of the password phrase support added in z/OS® V1R13 Communications Server for FTP and TN3270E.

## Background

- Password
  - One to eight characters
  - Limited range of characters allowed (for example, no blanks in the password)
- Password phrase
  - Nine to one hundred characters
  - Can contain any characters allowed in the EBCDIC 1047 code page
  - Must contain at least two alphabetic characters (case sensitive)
  - Must contain at least two non-alphabetic characters (numeric, punctuation, special, blank)
  - Cannot have more than two consecutive identical characters or NUL character
  - Every user ID with a password phrase also has a password

By V1R10, z/OS RACF® had introduced and improved support for password phrases. A password phrase is optional when defining a user ID. Any user ID that is assigned a password phrase also has a password. Some elements of z/OS support the use of either a password phrase or a password.

A traditional password is limited to eight characters, but a password phrase can contain up to one hundred characters. It can also include spaces, punctuation marks, and is always case sensitive, even if RACF is configured for NOMIXEDCASE. Several additional rules for password phrases are listed on this slide.

## FTP server

- Accept password phrases on the PASS command
- Support changing password phrases on PASS command
- Pass password phrase to FTCHKPWD

<i>Length</i>	<i>Password or password phrase</i>
---------------	------------------------------------

Beginning in z/OS V1R13, the Communications Server FTP server accepts password phrases in addition to passwords.

If you provide a password phrase on the PASS subcommand, it is used to authenticate you.

The FTP server supports changing the password phrase on the PASS subcommand. However, you can only change a password phrase to another password phrase, and you can change a password only to another password. You cannot change a password to a password phrase, and you cannot change a password phrase to a password.

The interface to the FTCHKPWD FTP user exit is changed to pass an additional parameter. Because password phrases are longer than eight bytes, the existing password parameter is not long enough to pass the full passphrase. The new parameter is set to either the password or the password phrase. The first two bytes of this parameter are the length of the password or password phrase that follows. You can inspect the length field to determine which is which: passwords are up to eight characters, and password phrases are nine to one hundred characters in length. Note that when the connection is secured with TLS or Kerberos, logging in with a password is not always necessary. When the server doesn't require a password, the password is set to EBCDIC blanks, and the password phrase will have a length of zero. Additionally, if you log in as the anonymous user and have not coded a user ID on the ANONYMOUS statement in FTP.DATA, both the password and the password phrase are set to a single asterisk.

## FTP server restrictions

- Excluded characters
  - carriage return (<CR>) or line feed (<LF>)
  - forward slash (/) or colon (:)
  - leading or trailing blanks
  - Interpret as command (IAC or X'FF') and telnet characters
- Anonymous user ID
  - You can assign a password phrase to the anonymous user ID
  - You cannot specify a password phrase when configuring the server for anonymous FTP:
    - FTP daemon start option
    - ANONYMOUS statement in FTP.DATA

z/OS V1R13 Communications Server's FTP server restricts the allowed characters for password phrases used to log into the z/OS Communications Server FTP server. If you assign these characters to a password phrase, you cannot use that password phrase to log into the FTP server. These characters have special meaning to the FTP server in some circumstances.

FTP has many configuration options for anonymous FTP, and some configurations require you to enter a password when logging in anonymously. When the server replies to a USER anonymous command with a "331 please enter password", you can specify either a password or password phrase on the PASS command. However, you cannot explicitly configure a password phrase for anonymous login. The only way to allow password phrases for anonymous login is to assign a password phrase to the anonymous user id.

## FTP client and FTP client API

- NAME (user ID) prompt

```
220-FTP 21:22 on 2010-02-09.  
220 Connec will close if idle for more than 5 minutes.  
NAME (via USER2):  
user1 "user1 secret password"
```

- PASSWORD prompt
- USER subcommand

```
Command:  
user user1 "user1 secret password"
```

- PASS subcommand

You can type multiple-token passwords at the FTP client name prompt by enclosing them in single or double quotation marks. This support is not new in V1R13.

You can type multiple-token passwords at the FTP client password prompt. This support is not new in V1R13.

You can type multiple-token passwords using the FTP client USER subcommand by enclosing them in single or double quotation marks. This support is not new in V1R13.

You can type multiple-token passwords using the FTP client PASS subcommand by enclosing them in single or double quotation marks. The PASS subcommand is typically only used by applications using the FTP client API. This support is not new in V1R13.

## NETRC

- Already supported double-quoted password phrases
- Now supports single-quoted password phrases

```
machine mvs099 login user3
machine 127.0.0.1 login user4 password usr4longpassphrase account acctpass
machine ::1 login user2 password "user2's password phrase"
```

The NETRC data set or file can be used by the FTP client to allow for login without prompting for username and password.

Before V1R13, the FTP client supported the use of double quotation marks to enclose multiple-token password phrases in the NETRC file.

Beginning in V1R13, the FTP client also supports the use of single quotation marks to enclose multiple-token password phrases in the NETRC file.

## FTP client guidelines

- Enclose password phrases with blanks in quotation marks

```
'My multi-token password'  
"My multi-token password"
```

- Do not mix single and double quotation marks within a password phrase

```
My cat's mother said "meow"
```

- If you code user data, and either the data contains blanks or the password phrase contains blanks, enclose both in quotation marks

```
"Mypasswørd:My user data"  
'my multi-token password:userdata'
```

You must enter quotation marks to enclose multi-token password phrases. You can use single or double quotation marks. If the password phrase itself contains a quotation mark, use the other style of quotation mark to enclose the password phrase. However, do not use quotation marks if they are not required. Password phrases containing only letters, numerals, or the characters @ # \$ - { . ( ) \* % + do not require quotation marks.

Also, you cannot mix single and double quotation marks within a password phrase.

When entering user data, and the data or the password phrase contains blanks, enclose them both in quotation marks.

## TN3270E background

- RestrictAppl requires user ID and password
- Used by the server to allow or block session initiation
- A solicitor panel is presented

```
Enter Your Userid:
Password:
Application:
Application Required. No Installation Default
New password:
```

- This is not used as the session user ID or password:  
The application might provide its own login screens

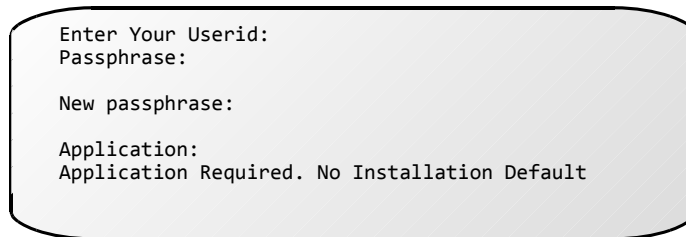
The TN3270E server RestrictAppl statement requires user verification before the server allows access to SNA applications. If RestrictAppl is configured, the server will send a solicitor screen to you asking for user ID, password, and the target application. If you supply a valid user ID, password, and target application combination the server will continue with session initiation with the target application. If your user ID and password are not valid, the server will not allow session initiation.

Note that, after you pass the server validity check and session initiation begins, the application might send its own log on screen. Your user ID and password required by the application are different from what you entered earlier during the server validity check.



## TN3270E server solicitor panel

- Password phrase can be up to 100 characters
- Enter eight characters or less and password is assumed



```
Enter Your Userid:  
Passphrase:  
  
New passphrase:  
  
Application:  
Application Required. No Installation Default
```

- New password or new password phrase confirmation required
- Supports both 80 column and 132 column displays

The TN3270E telnet server has been enhanced to optionally send a solicitor screen that allows a password phrase up to 100 characters. This new screen also accepts passwords. If the length is eight or less, the entry is considered a password. If the length is between nine and 100, the entry is considered a password phrase. Additionally, if you change your password or password phrase, you are prompted to retype your new password or password phrase to confirm the change. The old solicitor panel does not ask for confirmation which can lead to a lock-out if you mistype your new password or password phrase. Confirmation of a new password has not been added to the old solicitor screen in case automation has been set up and certain screen sequences are assumed.

Like the old solicitor screen, the new screen supports both 80 character and 132 character wide display formats.

## TN3270E function externals

Configure at all levels

- TelnetGlobals – All ports for the server
- TelnetParms – A single port
- ParmsGroup – Specific connections

A new statement, `PASSWORDPHRASE`, must be specified if you want to receive the new format solicitor screen and have the server ask for confirmation of a new password or password phrase. `PASSWORDPHRASE` can be specified in the `TELNETGLOBALS` block to affect all ports for the server, or specified in the `TELNETPARMS` block to affect a single port. If you want to send the new solicitor screen to a specific set of users based on IP address, host name, or SSL certificate user ID, you should use the `PARMSGROUP` statement within the `BEGINVTAM` block.

## Diagnosis

- Ensure your SAF product supports password phrases
- Check that you entered the correct case
- Try an alternate means of login

If you have a password phrase you can't log in with but which you think is correct, you should perform these steps. First, ensure that your SAF product supports password phrases and be aware of your SAF product's password phrase restrictions. For example, RACF has restrictions on characters that must be included and how many repeated characters are allowed. Second, check that you entered the correct case; password phrases are always case sensitive. Finally, try an alternate means of login to verify your password phrase, such as TSO or an alternate FTP client.

## Diagnosis for FTP

- Check that no forbidden characters are used, including leading or trailing spaces
- Check how single and double quotations marks are used
- Check the code pages between the client and the server
- Check if you have an FTCHKPWD user exit that has restrictions
- Be aware of your FTP client's password restrictions

For FTP, you should also check that your password phrase does not include characters disallowed by FTP, including leading or trailing spaces. Also, check that you are making proper use of single and double quotation marks. Because FTP translates password phrases to ASCII or UTF-8 for transmission, you should check that your code pages are consistent between your client and the server. Finally, you should check your FTCHKPWD exit and your FTP client to see if they are enforcing any restrictions.

---

## Diagnosis for TN3270E

- For TN3270E, turn on Telnet Debug for SAF return code data

For TN3270E, if there is a problem, you can turn on Debug detail in the server configuration to see the SAF return code and reason code for the login attempt.

## Things to think about

- FTP
  - Ensure your FTCHKPWD user exit can process the new parameter
  - For z/OS FTP client in batch mode, the password phrase and optional user data must fit on a single line of the batch file
  - Using only printable characters will reduce the likelihood of code page issues
- TN3270E
  - New solicitor panel format requires password change confirmation
  - New solicitor panel format might affect automation

For FTP, even if you do not intend to use password phrases, you should verify your FTCHKPWD user exit can handle the additional parameter. When using the z/OS FTP client in batch mode, note that the password phrase and optional user data must fit on a single line of the batch file. Finally, you can reduce the likelihood of code-page issues if you use only printable characters in your password phrases.

For TN3270E, the new solicitor panel format has the advantage of requiring confirmation for password changes. This reduces the likelihood of typing errors. However, you should take care to investigate how using the new solicitor panel format might affect any screen-scraping or automation that you are using.

---

## Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

[mailto:iea@us.ibm.com?subject=Feedback\\_about\\_passwordphrase.ppt](mailto:iea@us.ibm.com?subject=Feedback_about_passwordphrase.ppt)

This module is also available in PDF format at: [../passwordphrase.pdf](..../passwordphrase.pdf)

You can help improve the quality of IBM Education Assistant content by providing feedback.



## Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, RACF, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2011. All rights reserved.