

Password Requirement Changes  
Frequently Asked Questions

Q: Why are we changing our password requirements?

A: The new password requirements will help keep BNSF's systems secure. Hackers often use tools designed to easily decrypt common passwords which in turn would give them the ability to compromise your identity and impact your work. Requiring passwords to use mixed-case letters and numbers increases the difficulty of cracking the password.

Q: What are the new requirements?

A: All new passwords will require at least one uppercase character, one lower case character and one number.

Q: Are there other changes?

A: Also new is password change synchronization from the Mainframe to the Windows and UNIX systems. Now the password sync service will automatically match your password for these systems, whenever you change your password on either Windows or the Mainframe.

Q: How do I create a strong password?

A: Avoid using words found in the dictionary, birth dates, sports teams, family or pet names and other easily identifiable words. Change some characters to numbers. For example, use the number "5" for the letter "s."

Q: What if I use a special character?

A: If you use a special character, your password might not synch correctly as some environments within BNSF can handle the special character while others cannot. The Windows password policy will accept special characters but the password would fail in the Mainframe if the three new requirements were not met. Syncing the mainframe with Windows will cause certain special characters to be replaced with zeroes. This is not a change from current behavior. However, if you only log into Windows, using special characters is fine and would increase the strength of your password.

Q: Is the password length changing?

A: The minimum password length is still eight characters. Some environments will support more than eight characters (e.g., Windows, Linux) while some environments either won't accept it (e.g. , eMesa) or will truncate the password (e.g. , AIX, RACF). If you create a password longer than eight characters, your password might not synch correctly across our different platforms and applications. Similarly with special character use, if you only log into Windows, using longer passwords is fine and would increase the strength of your password.

Q: When will the new requirements go into effect?

A: Jan. 11, 2012

Password Requirement Changes  
Frequently Asked Questions

Q: Will I have to change my password on Jan. 11, 2012?

A: Passwords expire on a 90-day cycle. You will have to change your password 90 days after your last password change, not on Jan. 11, 2012.

Q. What happens if I need to change my password through the Voice Response Unit (VRU)?

A. The VRU will change your password and will provide your new alpha-numeric password.

Q. Does the VRU support the new password requirements?

A. Yes. You'll just have to enter your new password as described below.

Q. How do I input my new password with capitals and small letters and numbers?

A. Just like you use your touchtone keypad to call 1-800-CARPETS, you'll enter your new password the same way. Regardless of capital letters or lower-case letters in your new password, you'll use the same touchtone number, just like you would to call either 1-800-carpets or 1-800-CARPETS. Numbers in your new password will be entered as the same number on the keypad. If you have a special character in your new password (like "\$" or "&"), enter the number zero ("0") on your keypad.

Q: How do I enter characters when dialing into the VRU with my BlackBerry? The BlackBerry does not show the characters that correspond to the number.

A: While the telephone keypads on iPhone and Android devices display the letters that correspond with the numbers to dial, the BlackBerry does not. Press the <alt> button on the BlackBerry and select the letter(s) in the dialing string. Pressing <alt> b will send the tone used for both the "B" and "b" character to the VRU.

Remember: never share your password with anyone requesting it, whether it is via phone, email or in person. Hackers often pose as authorized personnel in an attempt to obtain your logon credentials. Change your password immediately if you suspect it is compromised.

Contact the BNSF Service Desk at 8-593-HELP (817-593-4357) if you require assistance with your password.