



CCAPRINT

A Newsletter Excerpt for Model 204 Users

March 2008

USE OF AND ACCESS TO PRODUCTS AND FEATURES ARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE USER'S SOFTWARE LICENSE. THE PRESENTATION OF MATERIAL HEREIN DOES NOT, IN ANY MANNER, MODIFY SUCH TERMS AND CONDITIONS.

Password Expiration and Other Security Features in V6R1.0

By James Damon

Most Model 204 installations require users to logon to a Model 204 Online or Batch204 system to gain access to the organization's data. Logon requires a valid User ID and password, which must be validated either by native Model 204 security or an external security interface: ACF2, RACF or TOPSECRET. CCASTAT is the file used in Model 204 security validation.

Many organizations have started to implement stricter logon security consisting of the following minimum requirements:

- Password expiration
- Revocation of user IDs after some number of unsuccessful logon attempts
- Password assignment that follows certain minimal rules of construction

V6R1.0 of Model 204 satisfies these requirements with an enhanced CCASTAT security file, as well as other enhancements to LOGON processing. File and group passwords are unaffected by these enhancements.

Converting Existing CCASTAT files

The enhanced security features available in V6R1.0 require you to convert your existing CCASTAT file to a new format. (This conversion is optional and need not be performed if you have no requirement for enhanced logon security.) A new utility, ZCTLTAB, converts CCASTAT, which enables the password expiration feature with the following configuration parameters:

- EXP, the number of days (0-255) before a password expires
- WARN, the number of days (0-255) prior to password expiration when the following warning message will be issued at every logon:

```
M204.2634: YOUR PASSWORD WILL EXPIRE IN 4 DAYS
```
- PURGE, the number of days (0-255) a user ID/password entry remains in CCASTAT, following password expiration, before it is purged

Following execution of the utility, each user ID/password entry in CCASTAT will increase in length from 26 to 34 bytes. This increase is generally not significant unless you have many thousands of user IDs. In that case, CCASTAT may require additional disk space.

Enhanced Logon Security in Operation

After CCASTAT has been converted with the ZCTLTAB utility, the parameters used to configure password expiration, are viewable with the VIEW command shown in Figure 1.

Figure1. Viewing password expiration parameters in CCASTAT

```
VIEW PWDEXP, PWDWARD, PWDPURGE
PWDEXP      30          PASSWORD EXPIRATION DAYS
PWDWARD     5           PASSWORD WARNING DAYS
PWDPURGE    180        PASSWORD PURGE DAYS
```

If the value of any of these parameters is equal to -1, then CCASTAT has not been converted to the new format.

After the conversion, a LOGLST command will show something similar to the following:

```
USER01      X'FF'      NONE  04/20/08  10/17/08  0      ALL
USER02      X'FF'      NONE  04/20/08  10/17/08  0      ALL
USER03      X'FF'      NONE  04/20/08  10/17/08  0      ALL
USER04      X'FF'      NONE  04/20/08  10/17/08  0      ALL
USER05      X'FF'      NONE  04/20/08  10/17/08  0      ALL
```

Assuming the conversion was run on 03/21/08 with the parameter values listed in Figure 1, the first date column is the date the user ID will expire. The second date column is the date, 180 days from the expiration date, that the user ID/password entry will be purged (deleted) from CCASTAT unless the password is reset. The column after that is a count of the number of unsuccessful logon attempts using this user ID.

Assuming these parameters are in effect, when a user, whose password has not been changed for 25 days, logs in that user will see the following message:

```
LOGON USERID
*** M204.0347: PASSWORD
*** M204.2634: YOUR PASSWORD WILL EXPIRE IN 5 DAYS
```

When a user's password expires, the following message is produced at logon:

```
LOGON USERID
*** M204.0347: PASSWORD
*** M204.2639: YOUR PASSWORD HAS EXPIRED
```

At this point, the user ID and password can be reactivated by only the system manager using the LOGCTL command. If this does not occur within the 180 days purge time, the user ID/password will be purged from CCASTAT.

Other Enhanced Security Features

Several other security features are also available when CCASTAT has been converted with the ZCTLTAB utility.

Revoking a User ID

When a user has attempted to logon more than three consecutive times with an incorrect password and has failed each time, the userid/password entry is in the same state as an

expired entry. In that case, the following message is produced and the user ID/password is made inactive:

```
LOGON USERID
*** M204.0347: PASSWORD
*** M204.0345: CCASTAT UPDATED
*** M204.2642: YOUR USERID HAS BEEN REVOKED: EXCESSIVE FAILED LOGON
ATTEMPTS
*** 3 M204.0349: LOGON FAILED
```

A new password must be set by the system manager using the LOGCTL command to reactivate the entry.

Password Assignment

User's may change their passwords during logon processing, if their logon privileges are set to X'10'. The following dialogue with Model 204 security will change a user's password:

```
LOGON USERID
*** M204.0347: PASSWORD
oldpass:newpass
*** M204.2633: RE-ENTER NEW PASSWORD
newpass
*** M204.0353: USERID      USERID      LOGON  08 MAR 20  17.40
*** M204.0350: NEW PASSWORD ACCEPTED
*** M204.0345: CCASTAT UPDATED
```

Password assignment, under CCASTAT enhanced security, must adhere to the following rules. The new password must:

1. Not be the same as the USERID, the current password, or the previous password.
2. Be six, seven or eight characters long.
3. Begin with an alphabetic character.
4. Include at least one numeric character.

In Summary

If your organization has begun imposing enhanced security requirements, the changes to native Model 204 security may satisfy those requirements. The conversion to the new CCASTAT format is very easy and, once done, can be redone with new security parameters whenever requirements change.

These enhanced security features are available under all operating systems. Additional information regarding ZCTLTAB, JCL and parameter settings can be found in the *Model 204 System Manager's Guide* in the chapter entitled "Storing Security Information (CCASTAT)."

© 2008 Computer Corporation of America
200 West Street, 3rd Floor West, Waltham, MA 02451