Technical Paper

SAS® User ID and Password Usage Rules

Introduction

An authenticated account ID for a SAS® user is a requirement.

In general, each SAS user has identity information in two distinct realms:

- In an authentication provider, the user has an account that can access the SAS Metadata Server.
- In SAS metadata, the user has a definition that includes a copy of the account ID with which the user accesses the metadata server.

An internal account uses the SAS Metadata Server as an authentication provider. An external account uses authentication from other authentication providers such as operating system and Lightweight Directory Access Protocol (LDAP) server.

This document is a high-level guide. It provides definitions and comparisons of user identity characteristics for internal and external authentication account rules.

User ID and Password Summarization Rules

	User Name	Internal Account	Operating System External Account					
			Windows 2003	Windows 2008	AIX	Linux	HP-UX	Solaris
Minimum length	1	7[1]	1	1	1	1	1	1
Maximum length	60	67[1]	104[2]	104	8[3]	8	8	8
Digits allowed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Special characters allowed	Characters except for / \ and control characters	Characters except for / \ and control characters	Characters except for “\/[]:;|=+*?< >	Characters except for “\/[]:;|=+*?< >	No	No	No	No
Case sensitive	No	No	No	No	Yes	Yes	Yes	Yes

Table 1. User Name and Account ID Rules and Parameters

[1] SAS internal accounts have a special suffix (@saspw).

[2] On Windows NT this value is 20

[3] For AIX 5.3 and later, this can be configured to be 255.

	Internal Account	Operating System External Account					
		Windows 2003	Windows 2008	AIX	Linux	HP-UX	Solaris
Minimum length	6	7	7	0	0	0	0
Maximum length	255	127	127	255[4]	8	8	8
Digits allowed	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Special characters allowed	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Case sensitive	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Encrypted (algorithm)	SHA-256[5]	LM or NTLM Hash	LM or NTLM Hash	MD5[6]	MD5	MD5	MD5
Age limits (force change)	No	No	No	Yes	Yes	Yes	Yes
History kept	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password complexity rules	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expire	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 2. Password Rules

Users

Each SAS user has a user name which is the identity in the SAS metadata. The SAS user is defined in the SAS metadata and corresponds to an account login. The authentication of SAS users access is performed by the authentication of its corresponding account ID and there is no password stored in the SAS metadata server for the SAS user itself.

Refer to *SAS® 9.3 Management Console Guide to Users and Permissions* for more information about creating user names using the SAS Management Console

Internal Accounts

An internal account is a SAS account that the metadata server authenticates independently, without relying on an external authentication provider such as the operating system and LDAP servers. Use internal accounts for only metadata administrators and certain service identities. These accounts are always list in this format: *name@saspw*. For more information about strengthening password policies refer to *SAS 9.3 Intelligence Platform Security Administration Guide, Chapter 11 Authentication Tasks for How to Change Internal Account Policies.* Internal accounts are locked after three unsuccessful login attempts. For more information about unlocking accounts refer to SAS 9.3 Intelligence Platform Security Administration Guide, *Chapter 4 Selected Tasks for Unlock an Internal Account.*

External Accounts

External accounts are defined outside of the SAS metadata. These accounts are local to a machine or network directory service with the machine is a member. External accounts are implemented for most SAS environmental users. In addition to common user access, external accounts are required to operate server processes. All of these accounts are controlled by the external authentication provider. External accounts are required to align with the policies of the authentication provider such as the operating system and LDAP server.

The user ID and passwords stored in the SAS metadata repository have a maximum length of 128 characters. The length of the corresponding account ID and password in operating systems or LDAP server should be less than 128 characters. For more information refer to SAS® 9.3 Metadata Model: Reference, Login section.

The following sub-topics provide brief descriptions of the User ID and Password usage rules when using Microsoft Windows, UNIX and or LINUX operating systems as the external authentication authority.

Microsoft Windows

On the Windows operating system, the passwords are controlled by operating system policies. The operating system passwords policies are used for domain and local user accounts. The default settings for passwords can be changed to meet site requirements. For example: enforcing password history, lifetimes, maximum or minimum age, and complexity requirements.

In Windows Server 2008, a fine-grained password policy can be used to specify multiple policies and apply different restrictions. Account lockout policies for users within a single domain can be set. For example, to increase the privileged account security stricter can be applied.

UNIX

On UNIX, the length limit of an account or a group name can be configured. In AIX the user and group name length limit parameter default value is eight characters. AIX user names are case sensitive, must not begin with a -, +, @, or ~, and cannot contain the following characters: :“#,=\/?‘`. The keywords ALL or default cannot be used in a user name.

A user’s effective password is a mix of uppercase and lowercase letters; a combination of alphabetic, numeric, or punctuation characters; or meet other restrict conditions. AIX provides mechanisms to help enforce a stronger password policy, such as resetting values for the following parameters:

- Minimum and maximum number of weeks that can elapse before and after a password can be changed (default 0, 0).
- Minimum length of a password.
- Minimum number of alphabetic characters that can be used when selecting a password.

Password options and extended user attributes are located in the /etc/security/user file, a text file that contains attribute stanzas for users. These restrictions are enforced whenever a new password is defined for a user. All password restrictions are defined per user. The settings in default stanza are applied only when a value has not been provided in user-specific stanza. To maintain password security, all passwords must be similarly protected. There are recommended values for some security attributes related to user passwords in the /etc/security/user file. For more information refer to *AIX 5.3 Security, table 7* . Only the root user can change attributes for users with admin=true set in the /etc/security/user file.

AIX stores encrypted passwords in the /etc/security/passwd file, that readable by the root user. The /etc/passwd file is used to keep track of every registered user with system access. The /etc/passwd file is owned by root user and must be readable by all the users, but only the root user has writable permissions.

LINUX

Linux has a standard set of tools that can be used to increase account data security. The system can be configured to enforce account aging and password composition rules.

In Red Hat® Enterprise Linux, changes are made in multiple locations. They are:

- /etc/pam.d/system-auth
- /etc/login.defs
- /etc/default/useradd

In Linux, password changes are passed through Pluggable Authentication Modules (PAM). To satisfy those requirements the PAM entry that corresponds with the password must be modified. The PAM file, /etc/pam.d/system-auth, is responsible for authentication. Initial modifications are made in this file. Inside /etc/pam.d/system-auth there are entries based on a "type" that the rules apply to. For more information about passwords refer to *Red Hat Enterprise Linux 6 Security Guide.*

Suggested Reading and More Information

SAS Institute Inc. 2011. *SAS® 9.3 Intelligence Platform: Security Administration Guide* Cary, NC: SAS Institute Inc. available at: http://support.sas.com/documentation/cdl/en/bisecag/63082/PDF/default/bisecag.pdf

SAS Institute Inc. 2009. *SAS® 9.3 Management Console: Guide to Users and Permissions.* Cary, NC: SAS Institute Inc. available at:

http://support.sas.com/documentation/cdl/en/mcsecug/63190/PDF/default/mcsecug.pdf

SAS Institute Inc. 2011. SAS® 9.3 Metadata Model: Reference, Login section. . Cary, NC: SAS Institute Inc. available at: http://support.sas.com/documentation/cdl/en/bisecag/61133/HTML/default/viewer.htm#titlepage.htm

SAS Institute Inc. 2009. *SAS® 9.2 Intelligence Platform: Security Administration Guide*. Cary, NC: SAS Institute Inc. available at: http://support.sas.com/documentation/cdl/en/bisecag/61133/PDF/default/bisecag.pdf

SAS Institute Inc. 2009. *SAS® 9.2 Management Console: Guide to Users and Permissions.* Cary, NC: SAS Institute Inc. available at: http://support.sas.com/documentation/cdl/en/mcsecug/61708/PDF/default/mcsecug.pdf

Microsoft 2005. *Account Policies in Windows server 2003* available at: http://technet.microsoft.com/en-us/library/cc783512(WS.10).aspx

Microsoft 2011. *Account Policies in Windows server 2008* available at: http://technet.microsoft.com/en-us/library/dd349793(WS.10).aspx

IBM 2002, 2010. *AIX 5.3 Security* available at: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/topic/com.ibm.aix.security/doc/security/security_pdf.pdf

Red Hat, Inc. 2011. *Red Hat Enterprise Linux 6 Security Guide* available at: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

SAS Institute Inc. World Headquarters +1 919 677 8000
To contact your local SAS office, please visit: **sas.com/offices**