Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

AS/400 & iSeries: A Comprehensive Guide to Setting System Values to Common Best Practice Securit

The purpose of this document is to assist anyone configuring or auditing iSeries (formerly known as AS/400) system values. This document should only serve as an informational guide and represents a security consultant's opinion on what the "Best Practice" setting should be in a typical corporate environment. Appropriate system value settings for the reader's environment may differ due to varying circumstances. This paper begins with a brief introduction of the iSeries platform. Next, a high level overview of how an iSe...

Copyright SANS Institute

Author Retains Full Rights

AD

AS/400 & iSeries:

A comprehensive guide to setting system values to common Best Practice security settings

(Version 1)

© SANS Institute 2001, Author retains full rights

Matthew R. Smith

July 16, 2001

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Introduction

The purpose of this document is to assist anyone configuring or auditing iSeries (formerly known as AS/400) system values. This document should only serve as an informational guide and represents a security consultant's opinion on what the "Best Practice" setting should be in a typical corporate environment. Appropriate system value settings for the reader's environment may differ due to varying circumstances.

This paper begins with a brief introduction of the iSeries platform. Next, a high level overview of how an iSeries machine functions is given, which leads into specifically discussing the system values. Fifteen of the most important system values have been chosen and will be analyzed in the following paper. Although system values from all areas of the iSeries platform are analyzed, an emphasis has been placed on system values related to iSeries security. Each system value bullet point contains a description of what that value controls and an explanation for each option associated with the system value. Last, a Best Practice setting is suggested in addition to the reasoning behind such a suggestion.

iSeries Overview

The IBM AS/400 (short for Application System/400), is a line of minicomputers that was introduced in 1988 and is still a popular choice today among IT Professionals and a wide range of companies. However, the AS/400 has recently become known as the iSeries. All models of the iSeries are run on a version of the Motorola/IBM 64 bit RISC (Reduced Instruction Set Computer) PowerPC processor specifically optimized for the OS/400 operating system. The iSeries is IBM's midrange series of computer systems used primarily for business applications, most of which are written in RPG III. There are 25,000 applications and 3,000 client/server applications that run on the iSeries machines. The iSeries serves in a variety of networking configurations: as a host or intermediate node to other AS/400s and System/3x machines, as a remote system to mainframe-controlled networks and as a network server to PCs. It is capable of supporting up to sixteen area networks, each with hundreds of clients.

On the iSeries, all user and system data structures are held in objects (files, folders, libraries, menus, programs, user profiles, etc.). It is possible to see in the objects only via their defined interfaces. iSeries operates on object-level security. The iSeries comes with four major operating system components: Integrated Communications, Integrated Database, Integrated Work Management, and Integrated Security. The functions within the Integrated Security component protect all objects and data from unauthorized access. The iSeries has default values known as system values, which can be used to control the operations of the system. System values are a part of iSeries and cannot be created by a user. However, most can be changed to customize your system according to your requirements. System values are used as default parameters in many commands and object descriptions. Other system values control the operation of certain parts of the operating system.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Changing System Values

In order to access the complete list of system values for viewing or editing purposes, enter the command "WRKSYSVAL" at the command line prompt. If the user is authorized to access this menu, the "Work with System Values" menu will appear. The matrix of values contains the system value, the category that the value fits under (Security, Storage, System control, etc.), and a description of the value. The values can be changed by entering option 2 or just displayed by entering option 5. Once option 2 is selected to edit a particular value, the menu may allow the user to choose from the different options available to that value or the user will be able to type the value in a provided space. If option 5 is selected for viewing, the user typically will see the option currently set for the value, as well as all the options available with a short description. If the user edits the system value, a confirmation notice is displayed at the bottom of the screen upon returning to the "Work with System Values" menu.

System Value Definitions and Best Practices

- **QDSPSGNINF** – The Display Sign-on Information system value determines whether the sign-on information display is shown after signing on. The sign-on information display shows:
  - The date of a user's last sign-on.
  - Any sign-on attempts that were not valid.
  - The number of days until the user's password expires (if the password is due to expire in 7 days or less).

  There are two possible values for QDSPSGNINF which are 0 (display is not shown) and 1 (display is shown). Also, this particular system value can be set different in a user's individual profile than the system value. The shipped value, or default value, for this setting is 0 (display is not shown). The preferred value is 1 (display is shown) because it is a good mechanism for users to monitor their system usage and notify I/S if something does not appear reasonable. It is also a warning to users that their password will expire soon.

- **QSECURITY** – The Security Level system value is perhaps the most important system value on the iSeries machines. The QSECURITY setting allows the system administrator to determine what level of security the system should enforce. Here's a review of the security levels available with OS/400:
  • Level 10: No Security (Discontinued in OS/400 Version 4, Release 2)
  • Level 20: Sign-on security
  • Level 30: Sign-on and resource security
  • Level 40: Sign-on and resource security; integrity protection
  • Level 50: Sign-on and resource security; enhanced integrity protection

  The iSeries are shipped with a default setting of 40. The system can only be set to one level for all users at any given time. The recommended setting for a secure iSeries machine is 40. This level of security is highly recommended for those locations that have complex processing that includes non-IBM system interfaces, network connectivity and processing of external tapes. One may think using 50 would be even better because it would be even more secure. This statement is true, however, there is a 5 to 15 percent performance decrease in going from level 40 to 50 and also a level of 40 provides an adequate level of security for typical companies.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **QINACTITV** – The Inactive Job Time-out system value controls the amount of time a terminal can remain signed-on without any activity. Once the inactive threshold is reached, the system automatically performs the action specified in the QINACTMSGQ system value. The QINACTITV and QINACTMSGQ system values provide security by preventing users from leaving inactive workstations signed-on. An inactive workstation might allow an unauthorized person access to the system. The possible values are *NONE or an interval in minutes between 5 and 300. The QINACTITV is shipped with a default value of *NONE, which means an inactive threshold cannot be reached because it doesn't exist. The recommended value is 60 minutes to prevent users from leaving inactive workstations signed-on.

- **QINACTMSGQ** – The Inactive Job Message Queue system value specifies the action the system takes when an interactive job has been inactive for the specified interval of time indicated by the QINACTITV system value. There are three possible values which include *ENDJOB, *DSCJOB, and the message-queue-name. The *ENDJOB option ends the dormant job, while the *DSCJOB merely disconnects the job. If the *DSCJOB value is used, the disconnected job time-out interval (QDSCJOBITV) system value controls whether the system eventually ends the disconnected job. If the message-queue-name value is used, a message is sent to the specified queue instead of canceling the job when the system determines a job is inactive. The iSeries default setting is *ENDJOB. The recommended Best Practice setting for the QINACTMSGQ system value is *DSCJOB in order to prevent an unauthorized user access to the system.

- **QDSCJOBITV** – The Disconnected Job Time-Out Interval system value determines, in terms of minutes, if and when the system ends a disconnected job. If the QINACTMSGQ is set to *DSCJOB, it is important to set a time limit to disconnect the job by specifying a value for QDSCJOBITV. This system value can either be a numeric value between 5 and 1,440 minutes or *NONE for no time limit. QDSCJOBITV is shipped with a system value of 240 minutes. However, a lower amount of time (90 to 120 minutes) is the preferred value because a disconnected job uses up system resources, as well as retaining any locks on objects.

- **QLMTSECOFR** – The Limit Security Officer system value restricts privileged users who have all-object (*ALLOBJ) or service (*SERVICE) special authorities to specified workstations. The two possible values for QLMTSECOFR are 1 and 0. A setting of 1 means a user with all-object or service special authority can sign-on at a workstation only if that user is specifically authorized to the display station or if the user profile QSECOFR is authorized to the display station. A setting of 0 means users with special authorities can sign-on to any workstation. Note that a user can always sign-on at the system console with the QSECOFR, QSRV, and QSRVBAS profiles, no matter how the QLMTSECOFR value is set. The iSeries default setting of 1 (privileged users are restricted to specified workstations) is the Best Practice value because a privileged user could potentially leave a workstation (not the secured console) unattended and that represents a considerable security exposure.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **QLMTDEVSSN** – The Limit Device Sessions system value determines whether a user is allowed to be signed-on to more than one device at a time. The possible values for QLMTDEVSSN are 0 and 1. A value of 0 means the system allows an unlimited number of sign-on sessions and a value of 1 means users are limited to one device session. Also, this particular system value can be set different in a user's individual profile than the system value. The default value for QLMTDEVSSN is 0 (unlimited number of sign-on sessions allowed). The QLMTDEVSSN value should be set to a value of 1, so that users can only be signed-on to one device at any given time. Having the users restricted as such reduces the risk that an unattended terminal would be left signed-on or that users will share their user-IDs and passwords.

- **QMAXSIGN** – The Maximum Number of Sign-on Attempts system value specifies the maximum number of invalid sign-on attempts permitted (for both local and remote users) by the system. The two possible values for QMAXSIGN are *NOMAX and any number between 1 and 25. If a number is specified, this indicates the amount of attempts a user may have to get the user name and password combination correct. If *NOMAX is used for this system value, an unlimited number of failed sign-in attempts is permitted on the iSeries machine. QMAXSIGN has a default value of 3. The Maximum Number of Sign-on Attempts system value should be set to the shipped value of 3. Having the users restricted as such reduces the risk that an intruder could repeatedly attempt user ID and password combinations without being detected.

- **QMAXSGNACN** – The Action When Sign-On Attempts Reached system value determines the action taken when the user violates the QMAXSIGN system value described above. It has three possible values numbered 1, 2, and 3. A value of 1 disables the device only. A value of 2 disables the user profile only. A value of 3 (the default setting) disables both the device and the user profile. Best Practices require the iSeries QMAXSGNACN system value be set on a value of 3 so that an intruder cannot attempt to access multiple profiles from one physical location.

- **QRMTSIGN** – The Remote Sign-On Control specifies how the system handles remote sign-on requests. The QRMTSIGN value can be set to *FRCSIGNON, *SAMEPRF, *VERIFY, *REJECT, or a custom program name. A value of * FRCSIGNON requires the user go through the normal sign-on procedure when accessing resources from a remote location. Both the *SAMEPRF and *VERIFY allow the remote user to bypass the sign-on display under certain sets of conditions. The *REJECT option does not allow remote connections to be established under any conditions. Finally, any custom program name used for this system value indicates that a custom application will run at the start and finish of any remote connection. The iSeries is shipped with a default setting of *FRCSIGNON for QRMTSIGN. The *FRCSIGNON option is also the preferred value if it is necessary for the machine to establish remote connections. If the machine does not require any type of remote connection, the *REJECT option is the preferred option.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **QPWDEXPITV** – The Password Expiration Interval specifies the number of days allowed before a password must be changed. The possible values for QPWDEXPITV are *NOMAX or a value between 1 and 366 days. The *NOMAX value indicates that users are not required to change their passwords. It should be noted that this particular system value could be set different in a user's individual profile than the system value. The default value for the Password Expiration Interval is *NOMAX, or users are not required to change their passwords at any period in time. It is definitely recommended that the QPWDEXPITV default value be changed to a value between 60 and 90 days. Having a password parameter that forces users to periodically change their password strengthens a company's security infrastructure.

- **QPWDRQDDGT** – The Requirement for Numeric Character in Passwords system value can require a user to have a numeric character in their new password. The possible values for QPWDRQDDGT are 0 (numeric characters are not required in passwords) and 1 (one or more numeric characters are required in passwords). The iSeries default setting for QPWDRQDDGT is 0 (numeric characters are not required in passwords). That setting provides for weak passwords – QPWDRQDDGT should be set to 1 (one or more numeric characters are required in passwords) to strengthen passwords so that they will not be easily guessed by an unauthorized user or attempted intruder.

- **QPWDRQDDIF** – The Required Difference in Passwords system value indicates the number, if any, of previous passwords that are checked for duplicates. QPWDRQDDIF has eight possible values which are the following: 0 (0 duplicate passwords are allowed), 1 (32 previous passwords are checked for duplicates), 2 (24 previous passwords are checked for duplicates), 3 (18 previous passwords are checked for duplicates), 4 (12 previous passwords are checked for duplicates), 5 (10 previous passwords are checked for duplicates), 6 (8 previous passwords are checked for duplicates), 7 (6 previous passwords are checked for duplicates), and 8 (4 previous passwords are checked for duplicates). The iSeries ships with a value of 0 (0 duplicate passwords are allowed) for QPWDRQDDIF. The recommended setting for the Required Difference in Passwords system value is 1 (32 previous passwords are checked for duplicates), 2 (24 previous passwords are checked for duplicates), 3 (18 previous passwords are checked for duplicates), or 4 (12 previous passwords are checked for duplicates). By setting this system value to one of these values, this strengthens passwords and discourages users from using the same password each time they are required to change it.

- **QPWDMINLEN** – The Minimum Length of Passwords system value specifies, in terms of characters, the shortest length a user's password may be. This system value must be a number of characters between 1 and 10. Despite being shipped with a value of 6, the QPWDMINLEN system value should be set to 8 to increase security surrounding the iSeries. By increasing the minimum length of passwords, intruders are forced to spend exponentially more time in their efforts to crack passwords.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **QAUDCTL** – The Auditing Control system value is the determinate of whether the iSeries is performing auditing or not. For this particular system value, more than one option can be chosen, with the exception of the *NONE (no auditing of users' actions or objects is performed) option which must be used alone. Also, *NONE is the default value for QAUDCTL. The other available options for QAUDCTL include *OBJAUD, *AUDLVL, and *NOQTEMP. The *OBJAUD option specifies that auditing should be performed for objects that have been selected using the CHGOBJAUD, CHGDLOAUD, or CHGAUD commands. The *AUDLVL option specifies that auditing should be performed for any functions selected on the QAUDLVL system value and on the AUDLVL parameter of individual user profiles. The *NOQTEMP option specifies that auditing should not be performed for most actions if the object is in the QTEMP library. It is recommended that the Auditing Control system value be set to *OBJAUD, *AUDLVL, and *NOQTEMP to maximize monitoring of the iSeries. This will ensure that your organization is taking steps to keep a watchful eye out for suspicious activity taking place on the system.

Conclusion

In closing, the reader should note that there are many other system values that can strengthen or weaken the security surround an iSeries machine that the reader should take into consideration. There are over 130 system values and an almost endless amount of configurations for an iSeries machine. Hopefully, the brief review of the system values covered in this document will at least help one get a basic understanding of the function of some of the more important system values and maybe even benefit by strengthening the security in your iSeries environment. Remember, the suggested or recommended settings discussed in this paper are in reference to a more generic environment, so carefully research the effect of any changes you make to system values in your specific environment before making them. Good luck!

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

1. International Business Machines Corporation (IBM). "Tips and Tools for Securing Your AS/400 Version 4". 1999.
   URL: http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R5PDF/C4153004.PDF

2. International Business Machines Corporation (IBM). "Security – Reference Version 5". 2000. URL: http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R5PDF/C4153024.PDF

3. AS400JOURNAL.com. "Do you know the AS/400…". July 16, 2001.
   URL: http://www.geocities.com/alex_nubla/facts.htm

4. internet.com – Webopedia. "AS/400". September 1, 1997.
   URL: http://www.pcwebopedia.com/TERM/A/AS_400.html

5. AS/400 and iSeries Security -- Wayne O Evans Consulting. "View Security Questions and Answers". March 24, 2001.
   URL: http://woevans.freeyellow.com/Qst_Ans.pdf

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced