Table of Contents

Summary:

1. NETLOGON_VALIDATION_SAM_INFO4 Structure Member Derivations and References

Items shown in **red bold** (with the exception of **Note**s) are pending additional verification. Items in **green bold** are used in policy checks (Security Settings / Account Policy).

[MS-NRPC] 2.2.1.4.13 NETLOGON_VALIDATION_SAM_INFO4

Data Type	Member Name	Derivation / Notes	User Account Object	References
OLD_LARGE_INTEGER	LogonTime	Time of logon (0x7FFFFFFF'FFFFFFFF for NULL session)	none	Time of validation completion.
OLD_LARGE_INTEGER	LogoffTime	<User Account Object>.lastLogoff (0x7FFFFFFF'FFFFFFFF for NULL session)	lastLogoff	[MS-ADA1] 2.349 Attribute lastLogoff
OLD_LARGE_INTEGER	KickOffTime	Time of logon start (0x7FFFFFFF'FFFFFFFF for NULL session)	none	Time of validation start.
OLD_LARGE_INTEGER	PasswordLastSet		pwdLastSet	[MS-ADA3] 2.174 Attribute pwdLastSet
OLD_LARGE_INTEGER	PasswordCanChange			**[MS-SAMR] 3.1.5.14.3 PasswordCanChange Generation (per user account control)**
OLD_LARGE_INTEGER	PasswordMustChange			**[MS-SAMR] 3.1.5.14.4 PasswordMustChange Generation**

				(per user account control)
UNICODE_STRING	EffectiveName		sAMAccountName	[MS-ADA3] 2.221 Attribute sAMAccountName
UNICODE_STRING	FullName		displayName	[MS-ADA1] 2.175 Attribute displayName
UNICODE_STRING	LogonScript		scriptPath	[MS-ADA3] 2.231 Attribute scriptPath
UNICODE_STRING	ProfilePath		profilePath	[MS-ADA3] 2.166 Attribute profilePath
UNICODE_STRING	HomeDirectory		homeDirectory	[MS-ADA1] 2.295 Attribute homeDirectory
UNICODE_STRING	HomeDirectoryDrive		homeDrive	[MS-ADA1] 2.296 Attribute homeDrive
unsigned short	LogonCount		logonCount	[MS-ADA1] 2.374 Attribute logonCount
unsigned short	BadPasswordCount		badPwdCount	[MS-ADA1] 2.83 Attribute badPwdCount
unsigned long	UserId	RID value from:	objectSid	[MS-ADA3] 2.44 Attribute objectSid
unsigned long	PrimaryGroupId		primaryGroupID	[MS-ADA3] 2.119 Attribute primaryGroupID
unsigned long	GroupCount	Computed like:	memberOf	[MS-ADA2] 2.45 Attribute memberOf
PGROUP_MEMBERSHIP	GroupIds	Computed like:	memberOf	[MS-ADA2] 2.45 Attribute memberOf
unsigned long	UserFlags			[MS-PAC] 2.5 KERB_VALIDATION_INFO
USER_SESSION_KEY	UserSessionKey	DataLength is normally 8		**[MS-NRPC] 2.2.1.4.9 USER_SESSION_KEY**
UNICODE_STRING	LogonServer	Name of the validating domain controller		
UNICODE_STRING	LogonDomainName	Name of the validating domain		
PRPC_SID	LogonDomainId	SID of the validating domain		
unsigned long	ExpansionRoom[10]			**[MS-NRPC] 2.2.1.4.9 USER_SESSION_KEY**
unsigned long	SidCount		sIDHistory	[MS- ADA3] 2.266 Attribute sIDHistory, [SID-History], [UsingSIDHistory]
PNETLOGON_SID_AND_ATTRIBUTES	ExtraSids		sIDHistory	[MS- ADA3] 2.266 Attribute sIDHistory, [SID-History], [UsingSIDHistory]
UNICODE_STRING	DnsLogonDomainNam e	DNS name of the validating domain		
UNICODE_STRING	Upn	sAMAccountName + "@DOMAIN.COM"	sAMAccountName	[MS- ADA3] 2.221 Attribute sAMAccountName
UNICODE_STRING	ExpansionString1			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString2			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString3			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString4			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString5			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString6			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString7			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString8			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString9			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures
UNICODE_STRING	ExpansionString10			[MS-NRPC] 1.3.8.1.3 Using Dummy Fields in Structures

References

[MS-NRPC]: Netlogon Remote Protocol Specification

2.2.1.4.9 USER_SESSION_KEY

2.2.1.4.13 NETLOGON_VALIDATION_SAM_INFO4

2.2.1.4.14 NETLOGON_VALIDATION

2.2.1.4.17 NETLOGON_VALIDATION_INFO_CLASS

6 Appendix A: Full IDL

[MS-APDS]: Authentication Protocol Domain Support Specification

3.1 NTLM Logon Details

3.1.5.1 NTLM Interactive Logon

3.1.5.2 NTLM Network Logon

4.1 NTLM Pass-Through Authentication

[MS-PAC]: Privilege Attribute Certificate Data Structure

2.5 KERB_VALIDATION_INFO

4.2.2 SID Filtering

[SID-History] "SID-History Attribute", http://msdn.microsoft.com/en-us/library/ms679833(VS.85).aspx

[UsingSIDHistory] "Using SID History to Preserve Resource Access", http://technet.microsoft.com/en-us/library/cc779590.aspx

Sample User Account Object

Dn: CN=Test,CN=Users,DC=DOMAIN,DC=COM
accountExpires: 9223372036854775807 (never);
badPasswordTime: 0 (never);
badPwdCount: 0;
cn: Test;
codePage: 0;
countryCode: 0;
displayName: Test;
distinguishedName: CN=Test,CN=Users,DC=DOMAIN,DC=COM;

dSCorePropagationData: 0x0 = ( );
givenName: Test;
homeDirectory: C:\Public;
instanceType: 0x4 = (WRITE);
lastLogoff: 0 (never);
lastLogon: 0 (never);
logonCount: 0;
logonHours: <ldp: Binary blob 21 bytes>; See Note 1
memberOf (2): CN=Remote Desktop Users,CN=Builtin,DC=DOMAIN,DC=COM; CN=Backup Operators,CN=Builtin,DC=DOMAIN,DC=COM;
name: Test;
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=DOMAIN,DC=COM;
objectClass (4): top; person; organizationalPerson; user;
objectGUID: 1da4e247-66da-40e1-b4a7-12a21e84df0c;
objectSid: S-1-5-21-2074671935-2981103931-2886920652-1124;
primaryGroupID: 513 = (GROUP_RID_USERS);
profilePath: \\DOMAINDC1.DOMAIN.COM\Public;
pwdLastSet: 9/18/2008 11:52:50 AM Eastern Daylight Time;
sAMAccountName: Test;
sAMAccountType: 805306368 = (NORMAL_USER_ACCOUNT);
scriptPath: \\DOMAINDC1.DOMAIN.COM\Public\Test.cmd;
userAccountControl: 0x10200 = (NORMAL_ACCOUNT | DONT_EXPIRE_PASSWD);
userPrincipalName: Test@DOMAIN.COM;
uSNChanged: 49221;
uSNCreated: 49207;
whenChanged: 9/18/2008 12:01:08 PM Eastern Daylight Time;
whenCreated: 9/18/2008 11:52:50 AM Eastern Daylight Time;

Note 1: [MS-ERREF](ntstatus, winerror): ERROR_INVALID_LOGON_HOURS, STATUS_INVALID_LOGON_HOURS

2. Password Policy Checks

The following account control flags shown in **blue bold** control security policy application to user logons. Control flags shown in **purple bold** apply to Kerberos authentication. Items shown in **orange bold** apply to [MS-SAMR] (Password Policy).

Password policy is constrained as described in [MS-SAMR] 3.1.1.7 Additional Update Constraints

Please see [MS-SAMR] for additional information on these flags:

[MS-SAMR]: Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)
- 3.1.1.7.1 General Password Policy
- 3.1.1.7.2 Cleartext Password Policy
- 3.1.1.8.10 userAccountControl
- 3.1.5.14.2 userAccountControl Mapping Table

USER_ACCOUNT Code		Description	Notes
USER_ACCOUNT_DISABLED (UF_NORMAL_ACCOUNT)	**UF_ACCOUNTDISABLE**	**Specifies that the account is not enabled for authentication.**	**[MS-ERREF] (ntstatus, winerror): STATUS_ACCOUNT_DISABLED, ERROR_ACCOUNT_DISABLED**
USER_HOME_DIRECTORY_REQUIRED	UF_HOMEDIR_REQUIRED	Specifies that the **homeDirectory** attribute is required.	**Note 2**
USER_PASSWORD_NOT_REQUIRED (UF_NORMAL_ACCOUNT)	**UF_PASSWD_NOTREQD**	**Specifies that the password-length policy does not apply to this user.**	**[MS-SAMR] 3.1.1.7.1 General Password Policy**
USER_ENCRYPTED_TEXT_PASSWORD_ALLOWED	**UF_ENCRYPTED_TEXT_PASSWORD_ALLOWED**	**Specifies that the cleartext password is to be persisted.**	**[MS-SAMR] 3.1.1.7.2 Cleartext Password Policy 3.1.1.8.11.5 CLEARTEXT Property**
USER_NORMAL_ACCOUNT	**UF_NORMAL_ACCOUNT**	**Specifies that the user is not a computer object.**	**[MS-SAMR] 3.1.5.14.1 distinguishedName Generation** [MS-SAMR] 3.1.5.14.4 PasswordMustChange Generation
USER_INTERDOMAIN_TRUST_ACCOUNT	UF_INTERDOMAIN_TRUST_ACCOUNT	Specifies that the object represents a trust object. For more information about trust objects, see [MS-LSAD].	[MS-SAMR] 3.1.5.14.4 PasswordMustChange Generation
USER_WORKSTATION_TRUST_ACCOUNT	UF_WORKSTATION_TRUST_ACCOUNT	Specifies that the object is a member workstation or server.	[MS-SAMR] 3.1.5.14.4 PasswordMustChange Generation

USER_SERVER_TRUST_ACCOUNT	UF_SERVER_TRUST_ACCOUNT	Specifies that the object is a DC.	[MS-SAMR] 3.1.5.14.4 PasswordMustChange Generation
USER_DONT_EXPIRE_PASSWORD	**UF_DONT_EXPIRE_PASSWD**	**Specifies that the maximum-password-age policy does not apply to this user.**	**[MS-SAMR] 3.1.5.14.4 PasswordMustChange Generation**
USER_ACCOUNT_AUTO_LOCKED	**UF_LOCKOUT**	**Specifies that the account has been locked out.**	**[MS-ERREF] (ntstatus, winerror): STATUS_ACCOUNT_LOCKED_OUT, ERROR_ACCOUNT_LOCKED_OUT**
USER_MNS_LOGON_ACCOUNT	**UF_MNS_LOGON_ACCOUNT**	**This bit is used by the Kerberos protocol. It indicates that the "OK as Delegate" ticket flag (described in [RFC4120] section 2.8) MUST be set.**	**[MS-KILE] 3.3.1.1 Account Database Extensions (Trusted for delegation:)**
USER_SMARTCARD_REQUIRED	**UF_SMARTCARD_REQUIRED**	**Specifies that the user can authenticate only with a smart card.**	**Note 3**
USER_TRUSTED_FOR_DELEGATION	**UF_TRUSTED_FOR_DELEGATION**	**This bit is used by the Kerberos protocol. It indicates that the "OK as Delegate" ticket flag (described in [RFC4120] section 2.8) MUST be set.**	**[MS-KILE] 3.3.1.1 Account Database Extensions (Trusted for delegation:)**
USER_NOT_DELEGATED	**UF_NOT_DELEGATED**	**This bit is used by the Kerberos protocol. It indicates that the ticket-granting tickets (TGTs) of this account and the service tickets obtained by this account are not marked as forwardable or proxiable when the forwardable or proxiable ticket flags are requested. For more information, see [RFC4120].**	**[MS-KILE] 3.2.1.1 Application Parameters (Delegate:)**
USER_USE_DES_KEY_ONLY	**UF_USE_DES_KEY_ONLY**	**This bit is used by the Kerberos protocol. It indicates that only des-cbc-md5 or des-cbc-crc keys (as defined in [RFC3961]) are used in the Kerberos protocols for this account**	**[MS-KILE] 3.3.1.1 Account Database Extensions (Use DES only:)**
USER_DONT_REQUIRE_PREAUTH	**UF_DONT_REQUIRE_PREAUTH**	**This bit is used by the Kerberos protocol. It indicates that the account is not required to present valid pre-authentication data, as described in [RFC4120] section 7.5.2.**	**[MS-KILE] 1.7.1 Pre-Authentication**
USER_PASSWORD_EXPIRED	**UF_PASSWORD_EXPIRED**	**Specifies that the password age on the user has exceeded the maximum password age policy.**	**[MS-ERREF] (ntstatus, winerror): STATUS_PASSWORD_EXPIRED, ERROR_PASSWORD_EXPIRED**
USER_NO_AUTH_DATA_REQUIRED	**UF_NO_AUTH_DATA_REQUIRED**	**This bit is used by the Kerberos protocol. It indicates that when the key distribution center (KDC) is issuing a service ticket for this account, the privilege attribute certificate (PAC) MUST NOT be included. For more information, see [RFC4120].**	**[MS-KILE] 3.1.5.1 Pre-authentication Data [MS-PAC] Privilege Attribute Certificate Data Structure [MS-SECO] 3.2.2.2 Notes**

Note 2: [MS-SAMR] 2.2.7.1 Common User Fields

HomeDirectory: A counted Unicode string of type RPC_UNICODE_STRING, indicating a directory in which an end-user interactive-logon application SHOULD start. This is user profile information.<15>

Note 3: [MS-SAMR] 3.1.1.8.10 userAccountControl

6. If the UF_SMARTCARD_REQUIRED bit is set and is NOT present in the previous value, the dbcsPwd and unicodePwd attributes MUST be updated with 16 bytes of random bytes, and the supplementalCredentials attribute MUST be removed.

References

[MS-ADTS]: Active Directory Technical Specification

- 2.2.15 userAccountControl Bits
- 3.1.1.4.5.17 msDS-User-Account-Control-Computed

[MS-SAMR]

- 2.2.1.12 USER_ACCOUNT Codes
- 2.2.7.1 Common User Fields
- 2.2.1.13 UF_FLAG Codes
- 3.1.5.14.2 userAccountControl Mapping Table

[MS-ERREF]: Windows Error Codes

- STATUS_PASSWORD_EXPIRED
- STATUS_ACCOUNT_LOCKED_OUT
- STATUS_ACCOUNT_DISABLED

3. Password Validation Attributes

[MS-SAMR]: Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)

[MS-ADTS]: Active Directory Technical Specification
- 3.1.1.3.1.5 Password Modify Operations
- 3.1.1.3.1.5.1 unicodePwd
- 3.1.1.3.1.5.2 userPassword

The sections noted in the below table contain operation descriptions of the operation, with attention to dbcsPwd and UnicodePwd.

dbcsPwd (DBCS-Pwd) LM Hash
unicodePwd (Unicode-Pwd) (NT Hash)

[MS-SAMR] 5.2 Index of Security Parameters

Security Parameter	Section	Title (not in document table)
Service principal name for server	2.1	Transport
Encryption algorithm for hashes	2.2.11.1	Encrypting an NT or LM Hash Value with a Specified Key
End-user password (to set)	3.1.5.6.4	SamrSetInformationUser2 (Opnum 58)
End-user password (to change)	3.1.5.10.1	SamrChangePasswordUser (Opnum 38) (**Note 4**)
End-user password (to change)	3.1.5.10.2	SamrOemChangePasswordUser2 (Opnum 54)
End-user password (to change)	3.1.5.10.3	SamrUnicodeChangePasswordUser2 (Opnum 55)
Recovery password (to set)	3.1.5.13.7	SamrSetDSRMPassword (Opnum 66)
End-user application password (set, change, and authenticate)	3.1.5.13.8	SamrValidatePassword (Opnum 67) (**Note 4**)
Encryption key for storing an encrypted LM hash	3.1.1.8.6	dbcsPwd
Encryption key for storing an encrypted NT hash	3.1.1.8.7	unicodePwd

Note 4: Password validation is described in:

[MS-SAMR]
- 3.1.5.10.1 SamrChangePasswordUser (Opnum 38)

3.1.5.13.8 SamrValidatePassword (Opnum 67)

References

[MS-SAMR] Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)
- 3.1.1.7.1 General Password Policy
- 3.1.1.8.5 clearTextPassword
- 3.1.1.8.7 unicodePwd
- 3.1.1.8.10 userAccountControl
- 3.1.1.9.1 Password History Update
- 3.1.5.10.1 SamrChangePasswordUser (Opnum 38)
- 3.1.5.10.2 SamrOemChangePasswordUser2 (Opnum 54)
- 3.1.5.10.3 SamrUnicodeChangePasswordUser2 (Opnum 55)
- 3.1.5.13.7 SamrSetDSRMPassword (Opnum 66)
- 3.1.5.13.8 SamrValidatePassword (Opnum 67)
- 3.1.5.14.3 PasswordCanChange Generation

unicodePwd (Unicode-Pwd) References

[MS-ADA3]
- 2.331 Attribute unicodePwd

[MS-ADLS]
- 2.357 Attribute unicodePwd

[MS-ADTS] Active Directory Technical Specification
- 3.1.1.3.1.5.1 unicodePwd
- 3.1.1.3.1.5.2 userPassword

[MS-NRPC]
- 3.1.1 Abstract Data Model (SharedSecret:)

[MS-SAMR] Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)
- See ' 2. Password Validation Attributes' References'

[MS-SAMS]
- 3.2.4.2 PasswordUpdate Request

dbcsPwd (DBCS-Pwd) References

[MS-ADA1]
2.141 Attribute dBCSPwd
[MS-SAMR] Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)
See ' 2. Password Validation Attributes' References'