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

This topic lists the Errata found in [MS-SAMR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V36.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	Added 2 new sections and updated several others to describe that the 16-byte encryption key that is used to encrypt the user password is the application key that is derived for the underlying SMB session. In Section 1.2.1, Normative References, added the following references: [MS-CIFS] Microsoft Corporation, "Common Internet File System (CIFS) Protocol". [MS-SMB2] Microsoft Corporation, "Server Message Block (SMB) Protocol Versions 2 and 3". In Section 1.4, Relationship to Other Protocols, updated the figures to include blocks for [MS-SMB2]. In Section 1.5, Prerequisites/Preconditions, added a reference to [MS-SMB2]. In Section 2.2.7.6, SAMPR_USER_ALL_INFORMATION, changed from: LmOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_LM_OWF_PASSWORD structure with the cleartext value being an LM hash, and the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). NtOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_NT_OWF_PASSWORD structure with the cleartext value being an NT hash, and the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: LmOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_LM_OWF_PASSWORD structure with the cleartext value being an LM hash, and the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. NtOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_NT_OWF_PASSWORD structure with the cleartext value being an NT hash, and the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. In Section 2.2.7.23, SAMPR_USER_INTERNAL1_INFORMATION, changed from:

Errata Published*	Description
	EncryptedNtOwfPassword: An NT hash encrypted with the 16-byte SMB [MS-SMB] session key for the connection established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). EncryptedLmOwfPassword: An LM hash encrypted with the 16-byte SMB [MS-SMB] session key for the connection established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: EncryptedNtOwfPassword: An NT hash encrypted with the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. EncryptedLmOwfPassword: An LM hash encrypted with the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. In Section 2.2.7.26, SAMPR_USER_INTERNAL5_INFORMATION, changed from: UserPassword: A cleartext password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD, with the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: UserPassword: A cleartext password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD, with the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. In Section 2.2.7.27, SAMPR_USER_INTERNAL5_INFORMATION_NEW, changed from: UserPassword: A password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD_NEW, with the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: UserPassword: A password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD_NEW, with the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. Added section 3.1.2.3 Acquiring an SMB Session Key 3.1.2.3 Acquiring an SMB Session Key The server MUST retrieve the SMB session key as specified in [MS-CIFS] section 3.3.4.6. In Section 3.1.5.6.4.4, UserInternal4Information, changed from: 3. If the USER_ALL_NTPASSWORDPRESENT or USER_ALL_LMPASSWORDPRESENT flag is present in the WhichFields field, the server MUST update the clearTextPassword attribute with the (decrypted) value of SAMPR_USER_INTERNAL4_INFORMATION.UserPassword, using the decryption key of the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (Kerberos or NTLM). Changed to:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>3. If the USER_ALL_NTPASSWORDPRESENT or USER_ALL_LMPASSWORDPRESENT flag is present in the WhichFields field, the server MUST update the clearTextPassword attribute with the (decrypted) value of SAMPR_USER_INTERNAL4_INFORMATION.UserPassword, using, as the decryption key, the 16-byte SMB session key obtained as specified in section 3.1.2.3.

In Section 3.2.2.2, MD5 Usage, changed from:

user-session-key is a 16-byte value obtained from the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]).

Changed to:
user-session-key is the 16-byte SMB session key obtained as specified in section 3.2.2.3.

Added section 3.2.2.3 Acquiring an SMB Session Key
3.2.2.3 Acquiring an SMB Session Key
The client MUST retrieve the SMB session key as specified in [MS-CIFS] section 3.4.4.6.</td></tr>
<tr><td>2016/05/02</td><td>In Section 3.1.5.13.7.1, SamValidateAuthentication, updated the order of the constraints.

Changed from:
<table><tr><th>Condition (fields based on ValidateAuthenticationInput)</th><th>ValidateAuthenticationOutput changes</th></tr><tr><td>If the current time is less than or equal to LockoutTime plus DomainLockoutDuration.</td><td>ValidationStatus MUST be set to SamValidateAccountLockedOut.</td></tr><tr><td>If the current time is greater than LockoutTime plus DomainLockoutDuration.</td><td>LockoutTime MUST be set to 0 (and continue processing)</td></tr><tr><td>PasswordLastSet is zero.</td><td>ValidationStatus MUST be set to SamValidatePasswordMustChange.</td></tr><tr><td>PasswordLastSet plus DomainMaximumPasswordAge is less than the current time.</td><td>ValidationStatus MUST be set to SamValidatePasswordExpired.</td></tr><tr><td>PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is greater than or equal to the current time.</td><td>1. ValidationStatus MUST be set to SamValidatePasswordIncorrect.
2. BadPasswordCount MUST be set to ValidateAuthenticationInput.BadPasswordCount plus 1.
3. BadPasswordTime MUST be set to the current time.
4. If DomainLockoutThreshold is greater than 0 and BadPasswordCount is greater than or equal to DomainLockoutThreshold, LockoutTime MUST be set to the current time.</td></tr><tr><td>PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is less than the current time.</td><td>1. ValidationStatus MUST be set to SamValidatePasswordIncorrect.
2. BadPasswordCount MUST be set to 1.
3. BadPasswordTime MUST be set to the current time.</td></tr></table></td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>PasswordMatched is nonzero.</td><td>1. ValidationStatus MUST be set to SamValidateSuccess.
2. If BadPasswordCount is nonzero, BadPasswordCount MUST be set to 0.</td></tr>
</table>

Changed to:
<table>
<tr><th>Constraint</th><th>Condition (fields based on ValidateAuthenticationInput)</th><th>ValidateAuthenticationOutput changes</th></tr>
<tr><td>1</td><td>If the current time is less than or equal to LockoutTime plus DomainLockoutDuration.</td><td>ValidationStatus MUST be set to SamValidateAccountLockedOut.</td></tr>
<tr><td>2</td><td>If the current time is greater than LockoutTime plus DomainLockoutDuration.</td><td>LockoutTime MUST be set to 0 (and continue processing).</td></tr>
<tr><td>3</td><td>PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is greater than or equal to the current time.</td><td>1. ValidationStatus MUST be set to SamValidatePasswordIncorrect.
2. BadPasswordCount MUST be set to ValidateAuthenticationInput.BadPasswordCount plus 1.
3. BadPasswordTime MUST be set to the current time.
4. If DomainLockoutThreshold is greater than 0 and BadPasswordCount is greater than or equal to DomainLockoutThreshold, LockoutTime MUST be set to the current time.</td></tr>
<tr><td>4</td><td>PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is less than the current time.</td><td>1. ValidationStatus MUST be set to SamValidatePasswordIncorrect.
2. BadPasswordCount MUST be set to 1.
3. BadPasswordTime MUST be set to the current time.</td></tr>
<tr><td>5</td><td>PasswordLastSet is zero.[1]</td><td>ValidationStatus MUST be set to SamValidatePasswordMustChange.</td></tr>
<tr><td>6</td><td>PasswordLastSet plus DomainMaximumPasswordAge is less than the current time.[1]</td><td>ValidationStatus MUST be set to SamValidatePasswordExpired.</td></tr>
<tr><td>7</td><td>PasswordMatched is nonzero.</td><td>1. ValidationStatus MUST be set to SamValidateSuccess.
2. If BadPasswordCount is nonzero, BadPasswordCount MUST be set to 0.</td></tr>
</table>
[1] The order in which these conditions are tested SHOULD<64> follow the order shown in the preceding table.
<64> Section 3.1.5.13.7.1: Windows Server 2003 operating system, Windows Server 2003 R2, and Windows Server 2008 operating system with Service Pack 2 (SP2) test the PasswordLastSet conditions (constraints 5 and 6) immediately after testing the LockoutTime conditions (constraints 1 and 2).
</td></tr>
<tr><td>2016/04/22</td><td>In several sections, added new information for security bulletin [MSKB-3149090].</td></tr>
</table>

Errata Published*	Description
	In Section 1.2.1, Normative References, added a new reference: [MSKB-3149090] Microsoft Corporation, "MS16-047: Description of the security update for SAM and LSAD remote protocols", April 2016, https://support.microsoft.com/en-us/kb/3149090. In Section 2.1, Transport, changed from: … The protocol uses the underlying RPC protocol to retrieve the identity of the client that made the method call, as specified in [MS-RPCE] section 3.3.3.4.3. The server SHOULD use this identity to perform method-specific access checks, as specified in the message processing section of each method.<11> RPC clients for this protocol MUST use RPC over TCP/IP for the SamrValidatePassword method and MUST use RPC over SMB for the SamrSetDSRMPassword method. … Changed to: … The protocol uses the underlying RPC protocol to retrieve the identity of the client that made the method call, as specified in [MS-RPCE] section 3.3.3.4.3. The server SHOULD use this identity to perform method-specific access checks, as specified in the message processing section of each method.<11> The server SHOULD<12> reject calls that do not use an authentication level of either RPC_C_AUTHN_LEVEL_NONE or RPC_C_AUTHN_LEVEL_PKT_PRIVACY (see [MS-RPCE] section 2.2.1.1.8). RPC clients for this protocol MUST use RPC over TCP/IP for the SamrValidatePassword method and MUST use RPC over SMB for the SamrSetDSRMPassword method. … <12> Section 2.1: Servers running Windows 2000, Windows XP, and Windows Server 2003 accept calls at any authentication level. Without [MSKB-3149090] installed, servers running Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 v1507 operating system, or Windows 10 v1511 operating system also accept calls at any authentication level.

* Date format: YYYY/MM/DD