[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

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

October 6, 2021 - Download

Errata below are for Protocol Document Version V44.0 – 2021/10/06.

Errata Published*	Description
2021/11/09	Added the constraint that the sAMAccountName for computer accounts with USER_WORKSTATION_TRUST_ACCOUNT flag must end with a single dollar sign ($). Also ensured that the objectClass of a new account MUST match the sAMAccountType. Added new behavior note to specify this and the supporting operating systems. In Section 3.1.1.6 Attribute Constraints for Originating Update Changed From: 10. ".... On error, return a failure code." Changed To: 10. ".... On error, return a failure code." 11. sAMAccountName MUST end with a single '$' (dollar sign) character if the objects UserAccountControl contains UF_WORKSTATION_TRUST_ACCOUNT. On error, return a failure code. This modification, MUST be allowed if the client is a member of the Domain Administrators group.<26> <26>The sAMAccountName for computer accounts with the USER_WORKSTATION_TRUST_ACCOUNT flag that MUST end in a single dollar sign ($) and the objectClass of a new account that MUST match the sAMAccount type is supported by the operating systems specified in [MSFT-CVE-2021-42278], each with its related MSKB article download installed. .... Changed From: "22. objectClass MUST be of type computer or derived from computer if userAccountControl contains the following bit: UF_SERVER_TRUST_ACCOUNT.

Errata Published*	Description
	23. unicodePwd MUST be exactly 16 bytes in length or not present." Changed To: "23. objectClass MUST be of type computer or derived from computer if userAccountControl contains the following bit: UF_SERVER_TRUST_ACCOUNT. 24. objectClass MUST be of type computer or derived from computer if the userAccountControl attribute contains the following bit: UF_WORKSTATION_TRUST_ACCOUNT. On error, return a failure code. This modification MUST be allowed if the client is a member of the Domain Administrators group.<28> 25. unicodePwd MUST be exactly 16 bytes in length or not present." <28>objectClass that MUST be of type computer or derived from the same if the userAccountControl attribute contains the UF_WORKSTATION_TRUST_ACCOUNT bit, is supported in the operating systems specified in [MSFT-CVE-2021-42278], each with its related MSKB article download installed."
2021/10/26	In Section 3.1.1.8.5 clearTextPassword : Clarified the conditions under which the value of a clearTextPassword MUST be replaced with a randomly generated value, and the conditions where the server MUST abort the request. Changed from: "2. If the RID of the objectSid attribute is DOMAIN_USER_RID_KRBTGT and the requesting protocol is a change-password protocol, the server MUST abort the request and return an error status. 3. If the RID of the objectSid attribute is DOMAIN_USER_RID_KRBTGT and the requesting protocol is a set-password protocol, ..." Changed to: "2. If either the RID of the objectSid attribute is DOMAIN_USER_RID_KRBTGT or the msDS-KrbTgtLinkBl attribute is present and refers to a read-only domain controller (RODC) object, and the requesting protocol is a change-password protocol, the server MUST abort the request and return error status. 3. If either the RID of the objectSid attribute is DOMAIN_USER_RID_KRBTGT or the msDS-KrbTgtLinkBl attribute is present and refers to an RODC object, and the requesting protocol is a set-password protocol, ..."

*Date format: YYYY/MM/DD