[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 V28.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/10/12</td><td>The character case of the lockOutObservationWindow attribute has been corrected from "lock<b>o</b>utObservationWindow" to "lock<b>O</b>utObservationWindow" in the following sections and locations:

Section 3.1.1.3 (Attribute Listing), in the attribute list.
Section 3.1.1.5 (Password Settings Attributes for Originating Update Constraints), in item 2.1.
Section 3.1.1.6 (Attribute Constraints for Originating Updates), in items 1 and 2.
Section 3.1.5.13.7 (SamrValidatePassword (Opnum 67)), in the third row of the table in item 2.
Section 3.1.5.14.8 (Domain Field to Attribute Name Mapping), in the sixth row of the table.</td></tr>
<tr><td>2015/09/04</td><td>In various sections, changes were made to support [MSKB-3072595], available on 2015/09/08:

In Section 3.1.1.6, Attribute Constraints for Originating Updates, changed from:
…
A client implementation MUST treat all failure codes as complete failures of the requested operation unless explicitly noted in this section. The possible status codes used for these explicit return codes are found in section 2.2.1.15.
…
19. userAccountControl MUST contain one and only one of the following bits, as defined in section 2.2.1.13; on error, return a failure code.
<table>
<tr><th>Bits</th></tr>
<tr><td>UF_NORMAL_ACCOUNT</td></tr>
<tr><td>UF_INTERDOMAIN_TRUST_ACCOUNT</td></tr>
<tr><td>UF_WORKSTATION_TRUST_ACCOUNT</td></tr>
<tr><td>UF_SERVER_TRUST_ACCOUNT</td></tr>
</table>

Changed to:
…
A client implementation MUST treat all failure codes as complete failures of the requested operation unless explicitly noted in this section. The possible status codes used for these explicit return codes are found in section 2.2.1.15.
…</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
19. userAccountControl MUST contain one and only one of the following bits, as defined in section 2.2.1.13; on error, return a failure code.
<table>
<tr><th>Bits</th></tr>
<tr><td>UF_NORMAL_ACCOUNT</td></tr>
<tr><td>UF_INTERDOMAIN_TRUST_ACCOUNT</td></tr>
<tr><td>UF_WORKSTATION_TRUST_ACCOUNT</td></tr>
<tr><td>UF_SERVER_TRUST_ACCOUNT</td></tr>
</table>

20. An existing userAccountControl attribute SHOULD NOT be modified such that the UF_WORKSTATION_TRUST_ACCOUNT bit is removed and the UF_NORMAL_ACCOUNT bit is added, or vice-versa; on error, return a failure code. This modification, however, MUST be allowed if the client is a member of the Domain Administrators group.<24a>

<24a> Section 3.1.1.6: This modification is always allowed in Windows 2000 and in the following products that do NOT have [MSKB-3072595] installed: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

In Section 3.1.5.4.4, SamrCreateUser2InDomain (Opnum 50), changed from:

13. If the client does not have the ACTRL_DS_CREATE_CHILD access right on the Container-Object objectand the AccountType parameter is USER_WORKSTATION_TRUST_ACCOUNT, then:

1. On a DC configuration:

1. If the RpcImpersonationAccessToken.Privileges[] field does not have the SE_MACHINE_ACCOUNT_NAME privilege (defined in [MS-LSAD] section 3.1.1.2.1), return a processing error.

2. Else:

- 1. Let CallerSid be RpcImpersonationAccessToken.Sids[RpcImpersonationAccessToken.UserIndex].

- - 1. The number of computer objects in the domain with msDS-creatorSID equal to CallerSid MUST be less than the value of ms-DS-MachineAccountQuota on the account domain object. On error, abort and return a failure code.frommsDS-creatorSID MUST be set to CallerSid.The owner and group of the default security descriptor MUST be the Domain Admins SID for the domain in which the account is created.

2. On a nonDC configuration:

▪ The server MUST abort processing and return STATUS_ACCESS_DENIED.

Changed to:

13. If the client does not have the ACTRL_DS_CREATE_CHILD access right on the Container-Object object, the client is not otherwise denied access due to an explicit DENY ACE <45a>, and the AccountType parameter is USER_WORKSTATION_TRUST_ACCOUNT, then:

1. On a DC configuration:

1. If the RpcImpersonationAccessToken.Privileges[] field does not have the SE_MACHINE_ACCOUNT_NAME privilege (defined in [MS-LSAD] section 3.1.1.2.1), return a processing error.

2. Else:

- 1. Let CallerSid be RpcImpersonationAccessToken.Sids[RpcImpersonationAccessToken.UserIndex].

- 2. Let CallerPrimaryGroup be RpcImpersonationAccessToken.PrimaryGroup.

- 3. If CallerPrimaryGroup is not equal to DOMAIN_GROUP_RID_COMPUTERS, then:
</td></tr>
</table>

Errata Published*	Description
	- - 1. The number of computer objects in the domain with msDS-creatorSID equal to CallerSid MUST be less than the value of ms-DS-MachineAccountQuota on the account domain object. On error, abort and return a failure code. - 4. If CallerPrimaryGroup is equal to DOMAIN_GROUP_RID_COMPUTERS, then:<45b> - - 1. If the domain SID portion of CallerSid is different from the current domain SID, return a failure code. - - 2. The server MUST compute the sum of all computer objects in the domain created by CallerSid and transitively created by other computer objects created by CallerSid. This sum MUST be less than the value of ms-DS-MachineAccountQuota on the account domain object. On error, abort and return a failure code. - 5. If the previous constraints are met, then: - - 1. msDS-creatorSID MUST be set to CallerSid. - - 2. The owner and group of the default security descriptor MUST be the Domain Admins SID for the domain in which the account is created. 2. On a nonDC configuration: The server MUST abort processing and return STATUS_ACCESS_DENIED. <45a> Section 3.1.5.4.4: The test for an explicit DENY ACE is NOT performed in Windows 2000. This test is also NOT performed in the following products that do not have [MSKB-3072595] installed: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. <45b> Section 3.1.5.4.4: This behavior is NOT performed in Windows 2000, and is also NOT performed in the following products that do not have [MSKB-3072595] installed: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. In these cases, the server behaves as if CallerPrimaryGroup is NOT equal to DOMAIN_GROUP_RID_COMPUTERS.
2015/08/17	In Section 3.1.5.3, Selective Enumerate Pattern, clarified the implicit constraints for use patterns utilized to obtain deterministic results. Changed from: The client use-pattern for these methods is a call to SamrGetDisplayEnumerationIndex2, followed by a call to SamrQueryDisplayInformation3, passing in the state returned by SamrGetDisplayEnumerationIndex2. This state is used as an index to indicate the account at which SamrQueryDisplayInformation3 will start its enumeration. These methods require a domain handle from the "open" pattern of methods (section 3.1.5.1). Changed to: The client use pattern for these methods is a call to SamrGetDisplayEnumerationIndex2, followed by a call to SamrQueryDisplayInformation3, passing in the state returned by SamrGetDisplayEnumerationIndex2. This state is used as an index to indicate the account at which SamrQueryDisplayInformation3 will start its enumeration. The client can also choose to skip the call to SamrGetDisplayEnumerationIndex2 and begin the enumeration by calling SamrQueryDisplayInformation3, specifying an index of zero. With either use pattern, the client can continue the enumeration process by calling SamrQueryDisplayInformation3 repeatedly, specifying on each call the Index value of the last account returned in the previous call. These methods require a domain handle from the "open" pattern of methods (section 3.1.5.1). The server MAY<44> cache implementation-specific details about the ongoing state of the enumeration on the domain handle; clients therefore MUST follow one of the use patterns described previously in order to produce deterministic results.

Errata Published*	Description
	<44>Non-DC configurations do not cache implementation-specific enumeration states on the domain handle; DC configurations do.
2015/08/03	In Section 3.1.5.9.1, SamrGetGroupsForUser (Opnum 39), clarified the SamrGetGroupsForUser criteria for when the server determines the union of all database objects. Changed from: 3. The server MUST determine the union of all database objects with class group and groupType GROUP_TYPE_SECURITY_ACCOUNT or GROUP_TYPE_SECURITY_UNIVERSAL whose member value contains the SID of the user referenced by UserHandle.Object. Changed to: 3. The server MUST determine the union of all database objects that meet the following criteria: ▪ They are of class group. ▪ Their groupType is GROUP_TYPE_SECURITY_ACCOUNT or GROUP_TYPE_SECURITY_UNIVERSAL. ▪ Their member value contains the SID of the user referenced by UserHandle.Object. ▪ They are in the same domain as the user referenced by UserHandle.Object. The union MUST also contain the group identified by the primaryGroupId attribute of the user that is referenced by UserHandle.Object.
2015/08/03	In Section 3.1.5.3.1, SamrQueryDisplayInformation3 (Opnum 51), clarified the return value of TotalAvailable when the DisplayInformationClass is not set to the DomainDisplayUser. Changed from: 5. For each candidate object to return, the server MUST fill an element in the Buffer output parameter according to the following table. … A call with DisplayInformationClass set to DomainDisplayOemUser or DomainDisplayOemGroup MUST behave identically to a call with DisplayInformationClass set to DomainDisplayUser or DomainDisplayGroup, respectively. The only exception to this rule is that the RPC_UNICODE_STRING structures in the non-Oem cases of DisplayInformationClass MUST be translated to RPC_STRING structures using the OEM code page. Changed to: 5. For each candidate object to return, the server MUST fill an element in the Buffer output parameter according to the following table. …

Errata Published*	**Description**
	A call with DisplayInformationClass set to DomainDisplayOemUser or DomainDisplayOemGroup MUST behave identically to a call with DisplayInformationClass set to DomainDisplayUser or DomainDisplayGroup, respectively, with the following exceptions: ▪ The RPC_UNICODE_STRING structures in the Oem cases of DisplayInformationClass MUST be translated to RPC_STRING structures using the OEM code page. ▪ The value returned in TotalAvailable MUST be set to zero.
2015/08/03	In Section 3.1.5.12.1, SamrSetSecurityObject (DC Configuration), revised the content to indicate that the server does not ignore the request when SecurityInformation is OWNER_SECURITY_INFORMATION. Changed from: … 3. If the database object referenced by ObjectHandle.Object is not a user object and the DACL_SECURITY_INFORMATION is not set in SecurityInformation, the server MUST silently ignore the request by aborting processing and returning 0. 4. Otherwise, the server MUST determine whether the DACL of SecurityDescriptor of the input message matches one of the following DACLs. The ordering of the ACEs is not relevant. Let Self denote the SID of the user object referenced by ObjectHandle.Object. 5. If there is no match from constraint 4, the server MUST silently ignore the request by aborting processing and returning 0. Changed to: … 3. If the DACL_SECURITY_INFORMATION bit is set in SecurityInformation, the server MUST determine whether the DACL of SecurityDescriptor of the input message matches one of the following DACLs. The ordering of the ACEs is not relevant. Let Self denote the SID of the user object referenced by ObjectHandle.Object. 4 If there is no match from the preceding constraint, the server MUST silently ignore the request by aborting processing and returning 0.

*Date format: YYYY/MM/DD