



Using a Polycom® KIRK® Wireless
Server 6000 Solution in a Microsoft®
Lync™ Server 2010 Setup

Application Note

Introduction

This application note describes how to setup a KIRK Wireless Server 6000 in a Lync Server 2010 setup. The description applies to Lync Server 2010 as well as to Microsoft® Office Communication Server 2007 R2. When a specific setup of the Microsoft® Office Communication Server 2007 R2 is required, it will be mentioned in this document.

Overview

The application note includes information about:

- Transport Protocol
- SIP User Authentication
- Secure Real time Transport Protocol(SRTP)
- Settings required for Lync Server 2010
- Server settings summary
- KIRK Wireless Server 6000 – Lync Server 2010 integration settings
- Adding users to KIRK Wireless Server 6000
- Setup of user credentials on KIRK Wireless Server 6000 for user installation

Firmware Compatibility

The KIRK Wireless Server 6000 interops with the Lync Server 2010 from firmware version PCS08B_. The KIRK Microsoft Lync Interoperability is backwards compatible with Microsoft® Office Communications Server 2007 R2.

The communication protocol between the KIRK Wireless Server 6000, the KIRK Media Resources and the KIRK IP Base Stations is not backward compatible starting with PCS08B_ of the KIRK Wireless Server 6000 and PCS08__ of the KIRK IP Base Station. This means that KIRK Media Resources with a firmware version older than PCS08B_ and KIRK IP Base Stations with firmware version older than PCS08__ will not be able to connect to a KIRK Wireless Server running firmware PCS08B_ or newer. To minimize downtime, update KIRK Media Resources and KIRK Wireless Server 6000 to firmware PCS08B_ and KIRK IP Base Stations to firmware PCS08__ before rebooting any of these.

Transport Protocol

To interop with the Microsoft Lync Server 2010, the KIRK Wireless Server 6000 supports TLS as transport protocol for SIP signalling. This requires a Certificate Authority on the KIRK Wireless Server 6000.

The KIRK Wireless Server 6000 is delivered with a Certificate Authority (CA) bundle with common Certificate Authorities. This means that the KIRK Wireless Server 6000 will accept certificates issued by e.g. Verisign out-of-the-box. In addition to the CA-bundle, the GUI allows installing a local CA certificate bundle; if the certificate is generated by a local authority (e.g. a service provider or the local IT department) a certificate bundle in PEM-format (also known as base-64 encoded X.509) can be imported.

Highlights of Supported Features

- SIP User Authentication via NTLM and Kerberos
- Incoming calls
- Outgoing calls
- Call waiting
- Message Waiting Indication
- Call logs:
 - Missed calls
 - Received calls
 - Outgoing calls
- Call hold
- Call forward
- Call transfer
- Call completed elsewhere
- Redial from stack
- Ad hoc conferencing. Enables users to participate in conference calls
- SBA (Survival Branch Appliance). Enables users to continue placing and receiving calls in a remote branch during WAN failure
- Basic Presence. In the Microsoft® Lync™ 2010 client or desk phone you will be able to see the presence status of each subscribed DECT handset as either “Away” (not in a call) or “In a call”.
***Note:** An initial log-in to a Lync client with each DECT user is required in order to activate presence functionality of the handset.*

Note: ICE will be supported in a future firmware release.

SIP User Authentication

In a Lync Server setup, SIP users are authenticated against an Active Directory Server. There are two authentication methods:

1. Service User : Kerberos (recommended)

A service user account is created on the Active Directory Server.

This service user is allowed to delegate to the SIP service.

The service user account and password are filled in on the KIRK Wireless Server 6000 and by authority delegation (this service user is used for the Lync Server 2010 authentication procedures).

2. User Authentication: NTLM (not recommended)

The credentials for each SIP user are filled in to the KIRK Wireless Server 6000 either by using the web GUI or using provisioning.

This user authentication method is best suited in scenarios where the user credentials are managed by the administrator and not by the user.

The KIRK Wireless Server 6000 does not support changing the Authentication Username or Password directly from the DECT handsets, only on the KIRK Wireless Server 6000.

Configuration

Settings Required for Lync Server 2010

When configuring a KIRK Wireless Server 6000 for Lync Server 2010, there are some specific settings and general SIP settings that need to be configured in a specific way.

Lync Server 2010 Specific Settings

- A Lync Server 2010 license needs to be installed on the KIRK Wireless Server 6000.
- SRTP needs to be enabled.
- Lync Server 2010 support needs to be enabled.
- The Lync Server 2010 domain needs to be configured.
- The Lync Server 2010 Front End Pool(s) and SBA(s) needs to be configured.
- The name and password of the DECT service user account needs to be configured if a service user is used for authentication.

KIRK Wireless Server 6000 Settings Summary

The following server settings are specifically relevant in a Lync Server 2010 setup:

Configuration key	Description	Lync Setting
sip.lync.enable	Enable Lync Server 2010 support Values: true, false. Default: false	True
sip.lync.domain	The domain of the Lync Server 2010	The domain of the Lync Server 2010
sip.lync.servicename	The name of the DECT service user account	The name of the DECT service user account
sip.lync.password	The password of the DECT service user account.	The password of the DECT service user account.
sip.media.sdp_ignore_version	Specifies whether to ignore the version information in incoming SDP received from remote endpoints. Values: true/false. Default: false.	True

sip.transport	Specifies the transport mechanism used for SIP requests. Values: UDP, TCP, TLS. Default: UDP.	TLS
sip.dnsmethod	Specifies the dns method used for SIP requests. Values: arecord, dnssrv. Default: arecord.	arecord
sip.gruu	Specifies the use of Globally Routable UA URI (GRUU) which is an URI which routes to a specific UA instance. If enabled a GRUU will be obtained from a server and communicated to a peer within a SIP dialog. Values: true/false Default: true.	True
sip.use_sips_uri	Normally SIP communication on a TLS connection is using the SIPS: URI scheme. Disabling this option causes the KIRK Wireless Server 6000 to use the SIP: URI scheme with a transport=tls parameter for TLS connections. Values: true/false Default: true.	False
sip.default_domain	The SIP domain of the Lync Server 2010.	
sip.proxy.domain sip.proxy.domain[2-4]	The FQDN of the Lync Front End Pool(s) and SBA(s).	
sip.media.srtp.enable	Enable SRTP between the KIRK Wireless Server 6000 and other endpoints. Not encrypted RTP is still allowed. Values: true, false. Default: false	True
sip.media.srtp.lifetime	Controls if SRTP lifetime key parameter is included in SDP security descriptors. Values: true, false. Default: false	True
sip.media.srtp.mki	Controls if SRTP MKI key parameter is included in SDP security descriptors. Values: true, false. Default: false	True
sip.media.srtp.required	Controls if SRTP is required for calls. If enabled calls will fail if the	True

	other end does not support SRTP. Values: true, false. Default: false.	
--	---	--

KIRK Wireless Server 6000 – Lync Server 2010 Integration Settings

Configuration of the Service User in AD

To create an AD user allowed to delegating to the sip service (Not required when using NTLM user authentication):

1. Open **Active Directory Users and Computers** window.
2. Create a new user named e.g. **DECTService**.

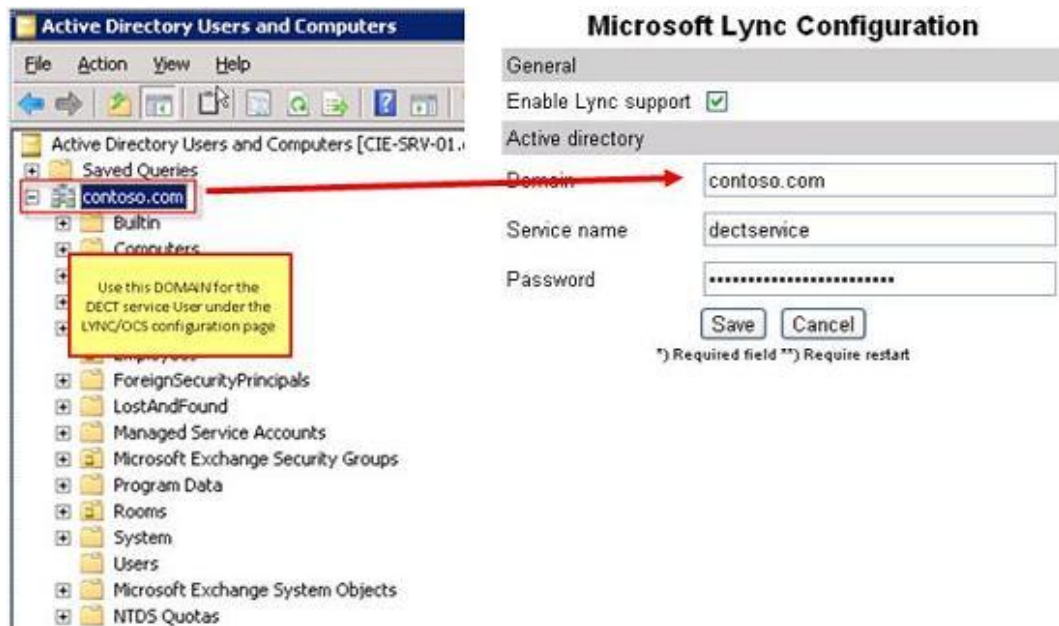


Figure 1 – Create an AD user

3. Disable **User must change password at next logon** checkbox.
4. Enable **User cannot change password** checkbox.
5. Enable **Password never expires** checkbox.

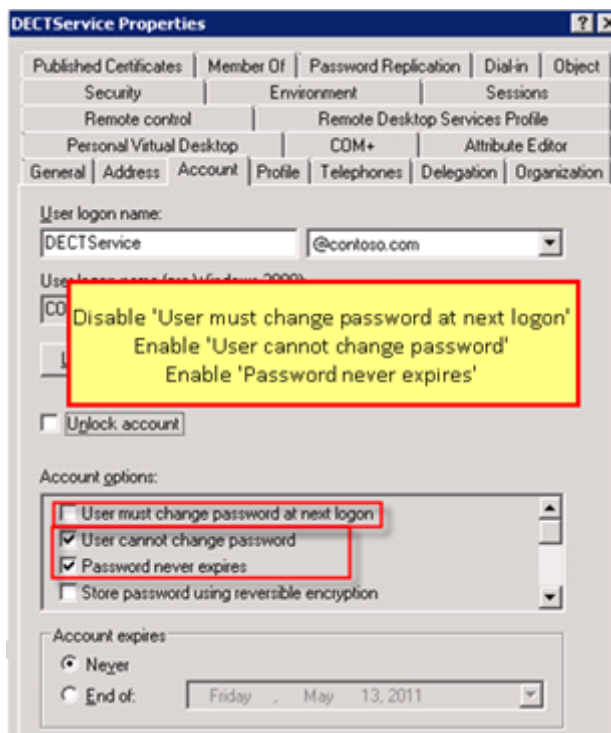


Figure 2 – Account settings

6. Set a password and save the user.
7. Enable **Advanced features** checkbox in the **View** menu.
8. Open the created user.
9. On the **Attribute Editor** page, set the **servicePrincipalName** attribute to **dect/<domain name>**.

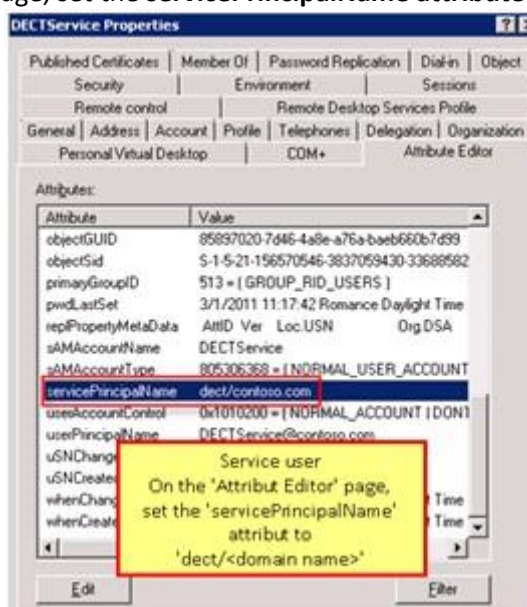


Figure 3 – Attribute settings

10. Close and re-open the user.
11. On the **Delegation** page:
 1. Select **Trust this user for delegation to specified services only** checkbox.

2. Select **Use any authentication protocol** checkbox.
3. Click the **Add** button to create an allowed delegation.



Figure 4 – Delegation settings

12. Select **Users or Computers**:

- (When using OCS 2007 R2) Enter **RTCService** as search object.
- (When using Lync Server 2010) Enter Front End Server name (without the domain name) as search object. Repeat for each front end server in the pool.

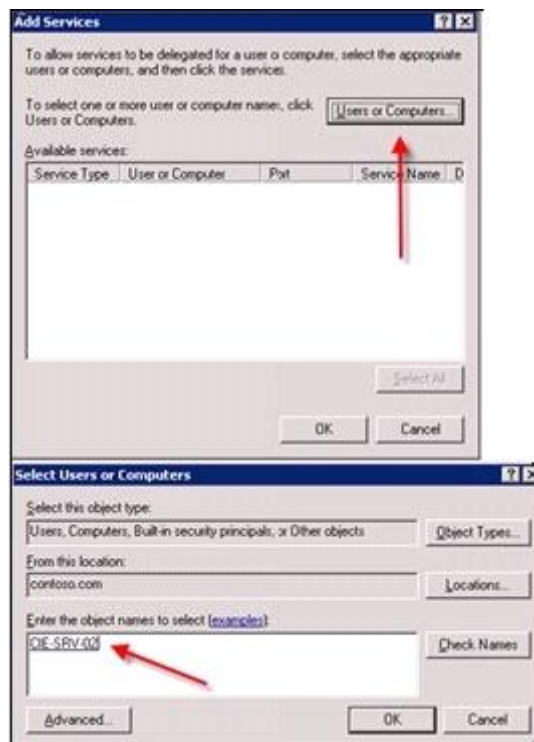


Figure 5- Users or Computers settings

13. Add the **SIP** service.

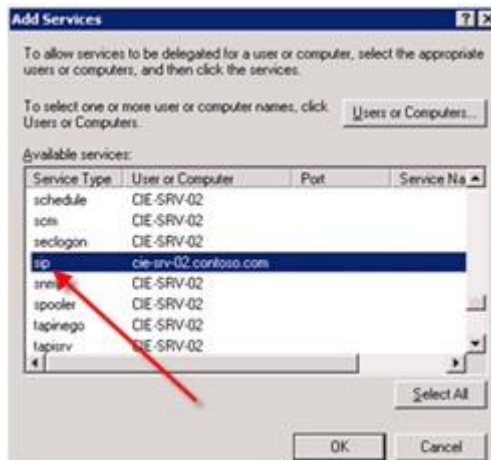


Figure 6- Service selection

To export the CA certificate:

1. Open **Certificate Authority**.
2. Open the **Properties** item of the CA of the domain.
3. On the **General** page, select **View Certificate**.
4. On the **Details** page, select **Copy to File...**
5. Set the format to **Base-64 encoded X.509 (.CER)**.
6. Save the certificate.

Note: This step is not required if the certificate of the Lync Server 2010 is signed by a public CA. This guide describes how to export the CA certificate from a Microsoft Certificated Authority. If a different CA authority technology is deployed, please refer to the vendor documentation.

KIRK Wireless Server 6000 Configuration

Note: A KIRK Microsoft Lync Interop License (part no. 14075270) must be installed on the KIRK Wireless Server 6000. The Lync Interop License includes the KIRK Software Security Package License (HTTPS, TLS, SRTP) as well. This license is needed for the RTP encryption towards the Lync Server 2010.

To configure Lync Server 2010 support on KIRK Wireless Server 6000

1. In the Lync Configuration menu (see [Figure 1 – Create an AD user](#)):
 - 1.1 Select the **Enable Lync support** check-box
 - 1.2 Set the domain name (not required when using NTLM user authentication)
 - 1.3 Enter the credentials of the AD user created above (not required when using NTLM user authentication)
2. In the SIP Configuration menu:
 - 2.1 Set the **Transport** to **TLS**
 - 2.2 Set the **DNS method** to **A records**

- 2.3 Set the **Default domain** to the SIP domain name of the Lync Server 2010.
e.g. John.doe@example.com should be “example.com” entered in default domain.

Note: SIP domain name refers to the Lync Server 2010 SIP domain name, not the AD domain if they are different.

- 2.4 Enable **GRUU**
- 2.5 Disable **Use SIPS URI**
- 2.6 **Set the Proxies to the prioritized list of FQDN(s) the Front End Pool(s) and the SBA(s).**
- 2.7 Enable **Ignore SDP version**
- 2.8 Enable **Enable RTP encryption**
- 2.9 Enable **Require RTP encryption**
- 2.10 Enable **Include lifetime in SDES offers**
- 2.11 Enable **Include MKI in SDES offers**

Note: When SRTP is enabled between the KIRK Wireless Server 6000 and the Lync Server 2010, the number of voice channels will be reduced from 32 to 16 voice channels (with codec card from 24 to 16 channels). For maximum security, it is possible to enable SRTP between the KIRK Wireless Server 6000 and the KIRK IP Base Stations as well. Please note that the voice channels of the base stations will be reduced from 12 to 6 voice channels.

3. In the Certificates Configuration menu, import the CA certificate exported above.

Note: This step is not required if the certificate of the Lync Server 2010 is signed by a public CA.

Adding Users to KIRK Wireless Server 6000

The information that needs to be filled in when a user is added depends on the chosen authentication method:

1. Service User (Kerberos)

If a service user is used for authentication the required information is:

- Username/Extension field: SIP username (without domain)
- Authentication Username: AD login name

The **Display name** and **Standby text** are optional, but recommended.

2. User Authentication (NTLM)

For the user authentication the AD username and the password are required:

- Username/Extension field: SIP username (without domain)
- Authentication Username: AD login name
- Authentication Password: AD login password

Using a Polycom® KIRK® Wireless Server 6000 Solution in a Microsoft® Lync™ Server 2010 Setup

The authentication username must be the same username specified in the Active Directory without the domain. The password must be the same password specified in the Active Directory.

The **Display name** and **Standby text** are optional, but recommended.

Setup of User Credentials on the KIRK Wireless Server 6000 for the Lync Server 2010 Installation

To setup the User Credentials

On the **User** page:

1. Fill in the **Username/Extension** field with the **msRTCSIP-PrimaryUserAddress** attribute value (see the below figures).

User 5040

DECT	
IPEI	00077 0545273
Access code	
Standby text	5040
SIP	
Username / Extension *	5040
Domain	
Displayname	5040
Authentication user	5040
Authentication password	••••
Disabled	<input type="checkbox"/>
Features	
Call forward unconditional	

*) Required field

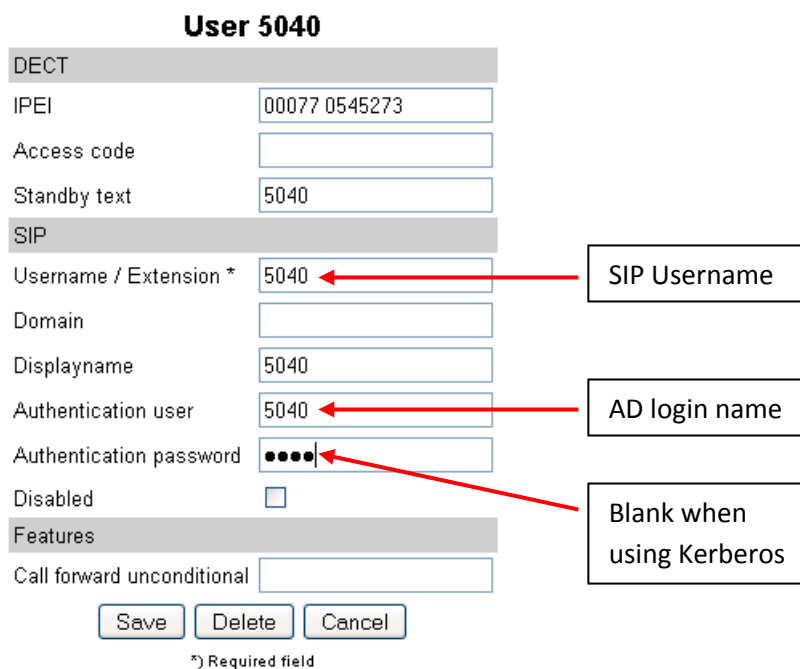


Figure 7 – User page

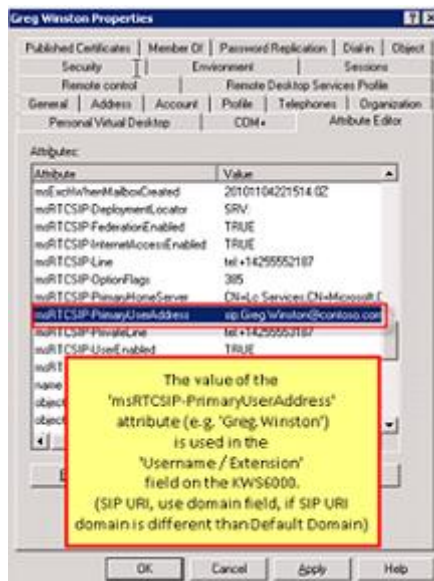


Figure 8 – 'msRTCSIP- PrimaryUserAddress' attribute

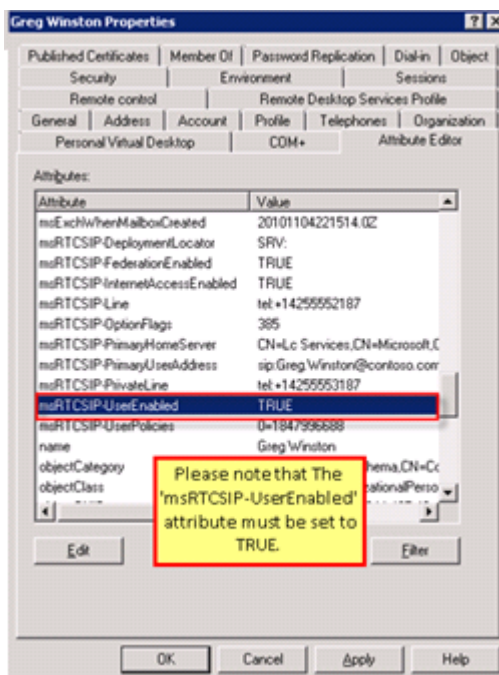


Figure 9 – 'msRTCSIP-UserEnabled' attribute (TRUE value)

2. Fill in the **Display name** field with the required attribute value (optional).

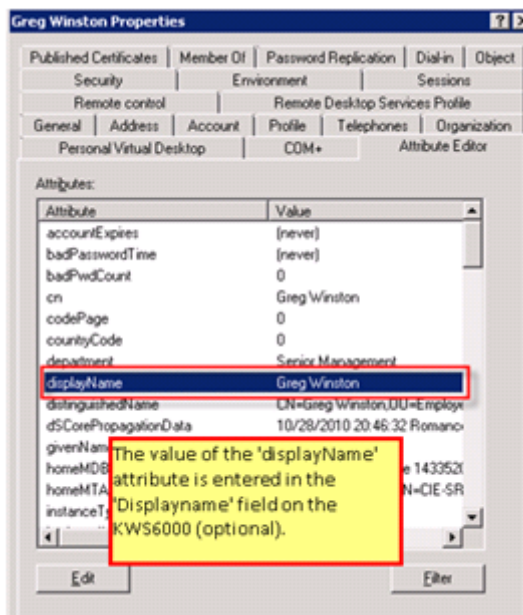


Figure 10 – ‘displayName’ attribute

- On the **User** page, fill in the **Authentication user** field with the required attribute value.

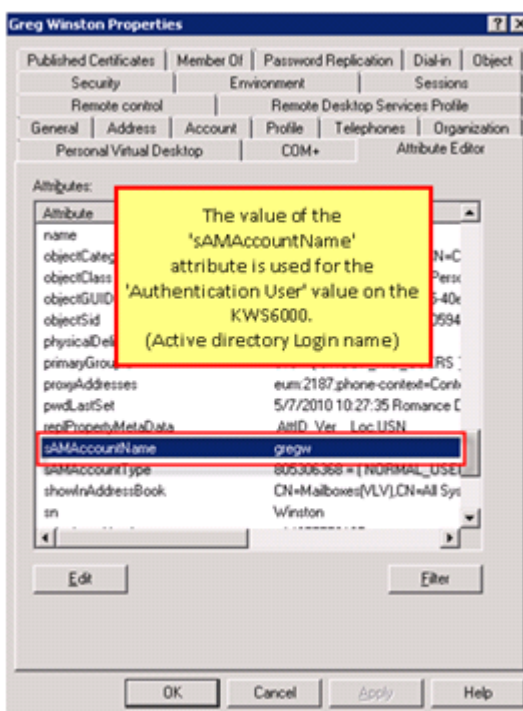


Figure 11 – ‘sAMAccountName’ attribute