

Windows

10 Anniversary Update

© 2016 Passcape Software
Passcape Software

1.		3
2.	Windows 10 Anniversary Update	3
3.		6

1

Windows 10, Microsoft

Windows 10 Anniversary Update

-
-
-
-
-
-
-

Microsoft

Hello . . . Cortana, Linux, Windows
 Windows 10
 Windows.
 Microsoft
 RC4. [Reset Windows](#)
[Password](#) Windows 10 AU.

2

Windows 10 Anniversary Update

Microsoft,

():

HKLM/SAM/SAM/Domains/Account/users/<RID>/V

<RID> -

HKLM/SAM/SAM/Domains/Account/users/names/<NAME>

, RID
) , 'Administrator' 500 (0x1F4) RID.
Guest — 501 (0x1F5).
V
, V : V - Variable, C -
Constant. 0 0xCC.
, 0x . . LM-
NT- 0x9C 0xA8 .

	0001	0203	0405	0607	0809	0A0B	0C0D	0E0F	0123456789ABCDEF
0x000	0000	0000	F400	0000	0300	0100	F400	0000ô.....ô...
0x010	1A00	0000	0000	0000	1001	0000	0000	0000
0x020	0000	0000	1001	0000	6C00	0000	0000	00001.....
0x030	7C01	0000	0000	0000	0000	0000	7C01	0000
0x040	0000	0000	0000	0000	7C01	0000	0000	0000
0x050	0000	0000	7C01	0000	0000	0000	0000	0000
0x060	7C01	0000	0000	0000	0000	0000	7C01	0000
0x070	0000	0000	0000	0000	7C01	0000	0000	0000
0x080	0000	0000	7C01	0000	0000	0000	0000	0000
0x090	7C01	0000	0800	0000	0100	0000	8401	0000
0x0A0	1800	0000	0000	0000	9C01	0000	3800	00008.....
0x0B0	0000	0000	D401	0000	1800	0000	0000	0000ô.....
0x0C0	EC01	0000	1800	0000	0000	0000	0100	1480	i.....
0x0D0	D400	0000	E400	0000	1400	0000	4400	0000	ô...ä.....D...
0x0E0	0200	3000	0200	0000	02C0	1400	4400	0501	..0.....À..D...
0x0F0	0101	0000	0000	0001	0000	0000	02C0	1400À..
0x100	FFFF	1F00	0101	0000	0000	0005	0700	0000	ÿÿ.....
0x110	0200	9000	0400	0000	0000	1400	5B03	0200[.....
0x120	0101	0000	0000	0001	0000	0000	0000	1800
0x130	FF07	0F00	0102	0000	0000	0005	2000	0000	ÿ.....
0x140	2002	0000	0000	3800	1B03	0200	010A	00008.....
0x150	0000	000F	0300	0000	0004	0000	DEA2	2867Ë(g
0x160	213E	D2AF	19AD	5D79	B0C1	0729	2756	FC20	!>ô-.]y°Á.)'Vü
0x170	D8AD	66F6	10F2	68FA	DF2A	F80F	0000	2400	ø-fô.òhúß*ø...ø.
0x180	4400	0200	0105	0000	0000	0005	1500	0000	D.....
0x190	DD30	4FC3	8766	1B73	CC43	79F4	F401	0000	-J Ñ-#i×0.øÈô...
0x1A0	0102	0000	0000	0005	2000	0000	2002	0000
0x1B0	0102	0000	0000	0005	2000	0000	2002	0000
0x1C0	4100	6400	6D00	6900	6E00	6900	7300	7400	A.d.m.i.n.i.s.t.
0x1D0	7200	6100	7400	6F00	7200	6424	4200	7500	r.a.t.o.r.d\$B.u.
0x1E0	6900	6C00	7400	2D00	6900	6E00	2000	6100	i.l.l.-i.n. a.
0x1F0	6300	6300	6F00	7500	6E00	7400	2000	6600	c.c.o.u.n.t. f.
0x200	6F00	7200	2000	6100	6400	6D00	6900	6E00	o.r. a.d.m.i.n.
0x210	6900	7300	7400	6500	7200	6900	6E00	6700	i.s.t.e.r.i.n.g.
0x220	2000	7400	6800	6500	2000	6300	6F00	6D00	.t.h.e. c.o.m.
0x230	7000	7500	7400	6500	7200	2F00	6400	6F00	p.u.t.e.r./d.o.
0x240	6D00	6100	6900	6E00	0102	0000	0700	0000	m.a.i.n.....
0x250	0100	0200	0000	0000	A10B	0D1F	D21D	B9CC;...ô.î
0x260	7A05	9F01	ADDC	1FE3	0100	0200	1000	0000	z...ü.ä.....
0x270	DB5E	9E14	8282	499B	72C6	AD87	4155	B0F6	Û~ . I rE- AU°ö
0x280	EE5C	E0B7	C998	6D28	4792	D1C0	9D14	240C	î\à-É m(G NÀ .ø.
0x290	C47C	53CB	50BC	348D	4F3D	3208	948A	99DD	Ä SËP4 O=2. Ý
0x2A0	0100	0200	0000	0000	56B0	2CF8	3122	B913V°,ø1"¹.
0x2B0	047D	D1CB	D164	86CA	0100	0200	0000	0000	.)ÑÑd È.....
0x2C0	DD30	4FC3	8766	1B73	CC43	79F4	FE01	9A0D	Ý00Ä f.sÏCyôp. .

Indexes

Variable offset

Variable size

Variable data

NTLM

HKLM/SAM/SAM/Domains/Account/Users/00001F4

- NTLM
0xA8.
0xCC NTLM 0x268, 0x19C.
- SYSKEY SAM (SAM session key).
HKLM/SAM/SAM/Domains/Account/V.
: MD5 RC4. Windows 10 Anniversary Update RC4 AES (Windows 10 Anniversary Update).
- AES.
SAM
RC4 AES (Windows 10 Anniversary Update).
- DES, RID
NTLM
Windows 10 Anniversary Update
RC4 3- 4- **AES.**
AES 16), (

3

Windows 10 Anniversary Update
SAM.

Windows Server 2016,

RC4.