Using UserAccountControl Flags to Manipulate Properties

January 23, 2022 by shelladmin

Active Directory UserAccountControl attribute contains flags to view or change the active directory user account values.

Active Directory UserAccountControl values represent which options have been enabled for a user account.

Ldp.exe tool or Adsiedit. msc snap-in tool shows the UserAccountControl values in Active Directory.

Search …

Recent Posts

How to View Docker Container Logs

How to Remove a Docker Container

How to Stop a Running Docker Container

Ldp.exe tool shows the values in hexadecimal. Adsiedit.msc snap-in tool shows the values in decimal.

In this article, we will discuss a list of **UserAccountControl flags** available. You can assign or change the possible UserAccountControl flags value.

Some of the flag values on the user or computer object can't change as they can be set or reset from the directory service.

Table of Contents [hide]

1 UserAccountControl Flags or Attribute Values
2 UserAccountControl Flags Descriptions
3 UserAccountControl 514 – Disable User Account
4 UserAccountControl 66048 – Enabled and Don't Expire User Password
5 UserAccountControl 66050 – Disabled and Don't Expire Password
6 UserAccountControl 544 – Enabled and Password not required
7 UserAccountControl 546 – Disabled and Password not required
8 UserAccountControl 66082 – Disabled,Password not required and Password Doesn't Expire
9 UserAccountControl 590336 – Enabled, User Cannot Change Password, Password Never Expires
10 UserAccountControl 4128 – WorkStation Trust Account, Password not required
11 UserAccountControl 2080 – InterDomain Trust Account, Password not required
12 Conclusion – UserAccountControl Flags

UserAccountControl Flags or Attribute Values

All UserAccountrol flag values are shown in the table.

Property flag	**Value in hexade**
SCRIPT	0x0001
ACCOUNTDISABLE	0x0002
HOMEDIR_REQUIRED	0x0008
LOCKOUT	0x0010
PASSWD_NOTREQD	0x0020
PASSWD_CANT_CHANGE	0x0040
ENCRYPTED_TEXT_PWD_ALLOWED	0x0080
TEMP_DUPLICATE_ACCOUNT	0x0100
NORMAL_ACCOUNT	0x0200
INTERDOMAIN_TRUST_ACCOUNT	0x0800
WORKSTATION_TRUST_ACCOUNT	0x1000
SERVER_TRUST_ACCOUNT	0x2000
DONT_EXPIRE_PASSWORD	0x10000
MNS_LOGON_ACCOUNT	0x20000
SMARTCARD_REQUIRED	0x40000
TRUSTED_FOR_DELEGATION	0x80000

NOT_DELEGATED	0x10000
USE_DES_KEY_ONLY	0x20000
DONT_REQ_PREAUTH	0x40000
PASSWORD_EXPIRED	0x80000
TRUSTED_TO_AUTH_FOR_DELEGATION	0x10000
PARTIAL_SECRETS_ACCOUNT	0x04000

UserAccountControl Attribute Table

UserAccountControl Flags Descriptions

Here is a Comprehensive list of UserAccountControl flags with their descriptions. Refer to the Official **Microsoft Knowledgebase article** for UserAccountControl.

- SCRIPT – The logon script will be run.
- ACCOUNTDISABLE – The user account is disabled.
- HOMEDIR_REQUIRED – The home folder is required.
- PASSWD_NOTREQD – No password is required.
- PASSWD_CANT_CHANGE – The user can't change the password. It's a permission on

the user's object. For information about how to programmatically set this permission, see Modifying User Cannot Change Password (LDAP Provider).

- ENCRYPTED_TEXT_PASSWORD_ALLOWED – The user can send an encrypted password.
- TEMP_DUPLICATE_ACCOUNT – It's an account for users whose primary account is in another domain. This account provides user access to this domain, but not to any domain that trusts this domain. It's sometimes referred to as a local user account.
- NORMAL_ACCOUNT – It's a default account type that represents a typical user.
- INTERDOMAIN_TRUST_ACCOUNT – It's a permit to trust an account for a system domain that trusts other domains.
- WORKSTATION_TRUST_ACCOUNT – It's a computer account for a computer that is running Microsoft Windows NT 4.0 Workstation, Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Professional, or Windows 2000 Server and is a member of this domain.
- SERVER_TRUST_ACCOUNT – It's a computer account for a domain controller that is a member of this domain.
- DONT_EXPIRE_PASSWD – Represents the password, which should never expire on the

account.

- MNS_LOGON_ACCOUNT – It's an MNS logon account.
- SMARTCARD_REQUIRED – When this flag is set, it forces the user to log on by using a smart card.
- TRUSTED_FOR_DELEGATION – When this flag is set, the service account (the user or computer account) under which a service runs is trusted for Kerberos delegation. Any such service can impersonate a client requesting the service. To enable a service for Kerberos delegation, you must set this flag on the userAccountControl property of the service account.
- NOT_DELEGATED – When this flag is set, the security context of the user isn't delegated to a service even if the service account is set as trusted for Kerberos delegation.
- USE_DES_KEY_ONLY – (Windows 2000/Windows Server 2003) Restrict this principal to use only Data Encryption Standard (DES) encryption types for keys.
- DONT_REQUIRE_PREAUTH – (Windows 2000/Windows Server 2003) This account doesn't require Kerberos pre-authentication for logging on.
- PASSWORD_EXPIRED – (Windows 2000/Windows Server 2003) The user's password has expired.

- TRUSTED_TO_AUTH_FOR_DELEGATION – (Windows 2000/Windows Server 2003) The account is enabled for delegation. It's a security-sensitive setting. Accounts that have this option enabled should be tightly controlled. This setting lets a service that runs under the account assume a client's identity and authenticate as that user to other remote servers on the network.
- PARTIAL_SECRETS_ACCOUNT – (Windows Server 2008/Windows Server 2008 R2) The account is a read-only domain controller (RODC). It's a security-sensitive setting. Removing this setting from an RODC compromises security on that server.

Let's try to understand with an example to set UserAccountControl values for a user account.

Let's practice!

> **Cool Tip:** How to **get active directory users** in PowerShell!

UserAccountControl 514 – Disable User Account

To disable a user account, we require a user's normal account flag value and the Disabled account flag value.

Refer to the above UserAccountControl table,

NORMAL_ACCOUNT property flag has hexadecimal value = 0x0200 and decimal = **512**

ACCOUNTDISABLE property flag has hexadecimal value = 0x0002 and decimal = **2**

Property flag	**Value in hexadecimal**	**Value in decimal**
NORMAL_ACCOUNT	0x0200	512
ACCOUNTDISABLE	0x0002	2
Disabled, Don’t Expire Password	**0x0202**	**514**

UserAccountControl 514 – Disabled User Account

UserAccountControl flags are cumulative. Sum up the hexadecimal value (0x0200 + 0x0002 = **0x0202**) and decimal value (512+2 = **514**)

ldp.exe tool shows the value in hexadecimal hence set **UserAccountControl 0x0202** value to disable user account.

adsiedit.msc snap-in tool shows the value in decimal, hence setting **UserAccountControl 514** value to disable a user account.

UserAccountControl 514 – Disabled User Account.

> **Cool Tip:** How to get aduser samaccountname in PowerShell!

UserAccountControl 66048 – Enabled and Don't Expire User Password

To set user password never expires on the enabled user account, we require user normal account flag and password don't expired flag.

Refer to the above UserAccountControl flag table.

NORMAL_ACCOUNT property flag has hexadecimal value = 0x0200 and decimal = **512**

DONT_EXPIRE_PASSWORD property flag has hexadecimal value = 0x10000 and decimal value = **65536**

Property flag	Value in hexadecimal	Value in decimal
NORMAL_ACCOUNT	0x0200	512
DONT_EXPIRE_PASSWORD	0x10000	65536
Enabled, Don't Expire Password	**0x10200**	**66048**

UserAccountControl 66048 – Enabled,don't expire password

Let's sum up flag values to get cumulative value.

Hexadecimal value = 0x200 + 0x10000 = **0x10200**

Decimal value = 512 + 65536 = **66048**

Assign Active Directory UserAccountControl attribute to 66048 to set user password never expired.

UserAccountControl 66048 – Enabled User Account with Password never expires.

Cool Tip: How to remove a user from the group in PowerShell!

UserAccountControl 66050 – Disabled and Don’t Expire Password

To set user password never expires on the disabled user account, we require user normal account flag, account disable flag and password don’t expired flag.

Property flag	Value in hexadecimal	Value in decimal
NORMAL_ACCOUNT	0x0200	512
ACCOUNTDISABLE	0x0002	2
DONT_EXPIRE_PASSWORD	0x10000	65536
Disabled, Don’t Expire Password	0x0222	66050

UserAccountControl 66050 – Disabled,don’t expire password

In the above table, we have summed up all the property flags to get cumulative value for a disabled user account whose password never expires.

Modify the **value of the UserAccountControl** attribute to **66050** in adsiedit.msc tool.

UserAccountControl 66050 – Disabled User Account with Password never expires.

> **Cool Tip:** Event Id 4634 – An Account was logged off!

UserAccountControl 544 – Enabled and Password not required

To set up an enabled user account with a password not required flag, we require a NORMAL_ACCOUNT flag and the PASSWD_NOTREQD flag.

Property flag	Value in hexadecimal	Value in decimal
NORMAL_ACCOUNT	0x0200	512

PASSWD_NOTREQD	0x0020	32
Enabled, Password not required	0x0220	544

UserAccountControl 544 – Enabled, Password not required

In the above table, we have summed up all the property flags to get cumulative value for an enabled user account for password not required.

Modify the **value of the UserAccountControl** attribute to **544** in adsiedit.msc tool.

UserAccountControl 544 – Enabled User Account with don’t expired password.

> **Cool Tip:** How to **fix error code 0xc0000234 or event id 4776** in PowerShell!

UserAccountControl 546 – Disabled and Password not required

To set up a disabled user account with a password not required, we need the NORMAL_ACCOUNT flag, PASSWD_NOTREQD flag, and ACCOUNTDISABLE flag.

Property flag	Value in hexadecimal	Value in decimal
NORMAL_ACCOUNT	0x0200	512
ACCOUNTDISABLE	0x0002	2
PASSWD_NOTREQD	0x0020	32
Disabled, Don’t Expire Password	0x0222	546

UserAccountControl 66050 – Disabled,Password not required

In the above table, we have summed up all the property flags to get cumulative value for a disabled user account for password not required.

Modify the **value of the UserAccountControl** attribute to **546** in adsiedit.msc tool.

UserAccountControl 546 – Disabled User Account with password not required.

UserAccountControl 66082 – Disabled,Password not required and Password Doesn’t Expire

To set up a disabled user account with a password not required, we need the NORMAL_ACCOUNT flag, PASSWD_NOTREQD flag, ACCOUNTDISABLE flag, and DONT_EXPIRE_PASSWORD flag.

Property flag	Value in hexadecimal	Valu in deci
NORMAL_ACCOUNT	0x0200	512
ACCOUNTDISABLE	0x0002	2
DONT_EXPIRE_PASSWORD	0x10000	6553
PASSWD_NOTREQD	0x0020	32
Disabled, Don’t Expire Password	0x10222	6608

UserAccountControl 66082 – Disabled, Password not required, the password doesn’t expire

In the above table, we have summed up all the property flags to get cumulative value for a disabled user account for password not required.

Modify the **value of the UserAccountControl** attribute to **66082** in adsiedit.msc tool.

UserAccountControl 66082 – Disabled User Account, password not required and password doesn't expire.

UserAccountControl 590336 – Enabled, User Cannot Change Password, Password Never Expires

Assign 590336 value to UserAccountControl attribute to enable a user account, user cannot change password and password never expires.

UserAccountControl 4128 – WorkStation Trust Account, Password not required

To set up a workstation trust account with a password not required, we need the WORKSTATION_TRUST_ACCOUNT flag and PASSWD_NOTREQD flag.

Property flag	**Value in hexadecima**
WORKSTATION_TRUST_ACCOUNT	0x1000
PASSWD_NOTREQD	0x0020
Workstation trust account with a password not required	0x1020

UserAccountControl 4128- WorkStation Trust Account with password not required

In the above table, we have summed up all the property flags to get cumulative value for a disabled user account for password not required.

Modify the **value of the UserAccountControl** attribute to **4128** in adsiedit.msc tool.

UserAccountControl 4128 – Workstation Trust Account with Password not required.

UserAccountControl 2080 – InterDomain Trust Account, Password not required

To set up a workstation trust account with a password not required, we need the

WORKSTATION_TRUST_ACCOUNT flag and PASSWD_NOTREQD flag.

Property flag	Value in hexadecimal
INTERDOMAIN_TRUST_ACCOUNT	0x0800
PASSWD_NOTREQD	0x0020
InterDomain trust account with a password not required	0x0820

UserAccountControl 2080- InterDomain Trust Account with password not required

In the above table, we have summed up all the property flags to get cumulative value for a disabled user account for password not required.

Modify the **value of the UserAccountControl** attribute to **2080** in adsiedit.msc tool.

UserAccountControl 2080 – InterDomain Trust Account with Password not required.

Conclusion – UserAccountControl Flags

I hope the above article on Active Directory UserAccountControl values is helpful to you.

UserAccountControl property flags are cumulative.

You can sum of UserAccountControl flags hexadecimal or decimal values to assign it to the UserAccountControl attribute value in ldp.exe and Adsiedit.exe snap-in tool respectively.

You can find more topics about PowerShell Active Directory commands and PowerShell basics on the **ShellGeek** home page.

PowerShell
active directory useraccountcontrol values
‹ PowerShell NoExit – Keep PowerShell Console Open
› Error Code 0xc0000234 – Event Id 4776 – Fix