Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Set-BitsTransfer'

PS C:\Users\wahid> Get-Help Set-BitsTransfer

NAME

Set-BitsTransfer

SYNOPSIS

Modifies the properties of an existing BITS transfer job.

SYNTAX

Set-BitsTransfer [-BitsJob] <BitsJob[]> [-ACLFlags <ACLFlagValue>]
[-Authentication {Basic | Digest | Ntlm | Negotiate | Passport}] [-CertHash
<Byte[]>] [-CertStoreLocation <CertStoreLocationValue>] [-CertStoreName
<String>] [-Confirm] [-Credential <PSCredential>] [-CustomHeaders <String[]>]
[-CustomHeadersWriteOnly] [-Description <String>] [-DisplayName <String>]
[-Dynamic] [-HttpMethod <String>] [-MaxDownloadTime <Int32>] [-NotifyCmdLine
<String[]>] [-NotifyFlags <NotifyFlagValue>] [-Priority {Foreground | High |
Normal | Low}] [-ProxyAuthentication {Basic | Digest | Ntlm | Negotiate |
Passport}] [-ProxyBypass <String[]>] [-ProxyCredential <PSCredential>]
[-ProxyList <Uri[]>] [-ProxyUsage {SystemDefault | NoProxy | AutoDetect |
Override}] [-RetryInterval <Int32>] [-RetryTimeout <Int32>] [-SecurityFlags
<SecurityFlagValue>] [-SetOwnerToCurrentUser] [-TransferPolicy {None |
Unrestricted | Capped | BelowCap | NearCap | OverCapCharged | OverCapThrottled

| UsageBased | Roaming | IgnoreCongestion | PolicyUnrestricted | Standard | NoSurcharge | NotRoaming | Always}] [-UseStoredCredential {None | Server | Proxy}] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-BitsTransfer cmdlet modifies the properties of an existing Background Intelligent Transfer Service (BITS) transfer job. You can specify the job that you want to modify in the BitsJob parameter. Or, you can specify the job by passing it through the pipeline.

PARAMETERS

-ACLFlags <ACLFlagValue>

Specifies the owner and access control list (ACL) information to maintain for the transfer job. Specify one or more of the following values:

- o: Copy owner information with file.

- g: Copy group information with file.

- d: Copy discretionary access control list (DACL) information with file.

- s: Copy system access control list (SACL) information with file.

-Authentication <String>

Specifies the authentication mechanism to be used at the server. The acceptable values for this parameter are:

- Basic : Basic is a scheme in which the user name and password are sent in clear text to the server or proxy.

- Digest : Digest is a challenge-response scheme that uses a

server-specified data string for the challenge.

- NTLM : NT LAN Manager (NTLM) is a challenge-response scheme that uses the credentials of the user for authentication in a Windows-based network environment.

- Negotiate (the default): Negotiate is a challenge-response scheme that negotiates with the server or proxy to determine which scheme to use for authentication. For example, this parameter value allows negotiation to determine whether the Kerberos protocol or NTLM is used.

- Passport : Passport is a centralized authentication service provided by Microsoft that offers a single logon for member sites.

-BitsJob <BitsJob[]>

Specifies an array of BITS transfer jobs on which this cmdlet sets properties. You can pipe a value to this parameter from other cmdlets that return BitsJob objects, such as Get-BitsTransfer

-CertHash <Byte[]>

Specifies a SHA1 hash that identifies the certificate.

-CertStoreLocation <CertStoreLocationValue>

Specifies the certificate store location to use for to look up the certificate. Valid values are:

- CURRENT_USER

- LOCAL_MACHINE

- CURRENT_SERVICE

- SERVICES

- USERS

- CURRENT_USER_GROUP_POLICY

- LOCAL_MACHINE_GROUP_POLICY

- LOCAL_MACHINE_ENTERPRISE

-CertStoreName <String>

Specifies the name of the certificate store. Valid values are:

- CA: Certification Authority certificates

- MY: Personal certificates

- ROOT: Root certificates

- SPC: Software Publisher Certificate

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-Credential <PSCredential>

Specifies the credentials to use to authenticate the user at the server.
The default is the current user. Type a user name, such as "User01",
"Domain01\User01", or "User@Contoso.com". Or, use the Get-Credential
cmdlet to create the value for this parameter. When you type a user name,
you are prompted for a password.

-CustomHeaders <String[]>

Specifies one or more custom HTTP headers to include in the request to the
server. Specify an array of strings.

-CustomHeadersWriteOnly [<SwitchParameter>]

Indicates that the HTTP custom headers for this job are write-only.

Use this parameter when your custom headers include security information. Other programs on the same computer can't read the header. The BITS process can read the headers and send them over the HTTP connection.

You cannot change this value for a job after you set headers to write-only.

-Description <String>

Specifies a description for the BITS transfer job. The description is limited to 1,024 characters.

-DisplayName <String>

Specifies a display name for the BITS transfer job. The display name provides a user-friendly way to differentiate BITS transfer jobs.

-Dynamic [<SwitchParameter>]

Indicates that the transfer uses the dynamic setting.

-HttpMethod <String>

Specifies a method for the transfer other than the default method GET. If you specify GET, the parameter has no effect.

If you specify a method, the job takes foreground priority, which can't be changed.

-MaxDownloadTime <Int32>

Specifies the maximum time, in seconds, for transferring the files in a job. The default is 7,776,000 seconds or 90 days.

-NotifyCmdLine <String[]>

Specifies a program to run after the job finishes or encounters an error.
The program runs in the context of the user who runs this cmdlet.

Specify the program name and any parameters as an array of strings.

-NotifyFlags <NotifyFlagValue>
Specifies the type of event notification you want to receive, such as job transferred events. Valid values are:

- 1: Generates an event when all files in the job have been transferred.

- 2: Generates an event when an error occurs.

- 4: Disables notifications.

The default value is 1|2.

-Priority <String>
Specifies the priority of the BITS transfer job, which affects bandwidth usage. The acceptable values for this parameter are:

- Foreground (default): Transfers the job in the foreground. Foreground transfers compete for network bandwidth with other applications, which can impede the user's overall network experience. However, if the Start-BitsTransfer cmdlet is being used interactively, this is likely the best option. This is the highest priority level.

- High : Transfers the job in the background with a high priority. Background transfers use the idle network bandwidth of the client computer to transfer files.

- Normal : Transfers the job in the background with a normal priority. Background transfers use the idle network bandwidth of the client computer to transfer files.

- Low : Transfers the job in the background with a low priority. Background transfers use the idle network bandwidth of the client to transfer files. This is the lowest background priority level.

-ProxyAuthentication <String>

Specifies the authentication mechanism to use at the Web proxy. The acceptable values for this parameter are:

- Basic : Basic is a scheme in which the user name and password are sent in clear text to the server or proxy.

- Digest : Digest is a challenge-response scheme that uses a server-specified data string for the challenge.

- NTLM : NTLM is a challenge-response scheme that uses the credentials of the user for authentication in a Windows-based network environment.

- Negotiate (the default): Negotiate is a challenge-response scheme that negotiates with the server or proxy to determine which scheme to use for authentication. For instance, this parameter value allows negotiation to determine whether the Kerberos protocol or NTLM is used.

- Passport : Passport is a centralized authentication service provided by Microsoft that offers a single logon for member sites.

-ProxyBypass <String[]>

Specifies a list of host names to use for a direct connection. The hosts in the list are tried in order until a successful connection is achieved.
If you specify this parameter the cmdlet bypasses the proxy. If this

parameter is used, the ProxyUsage parameter must be set to Override ;
otherwise, an error occurs.

-ProxyCredential <PSCredential>
Specifies the credentials to use to authenticate the user at the proxy.
You can use the Get-Credential cmdlet to create a value for this parameter.

-ProxyList <Uri[]>
Specifies an array of proxies to use. The proxies in the list are tried in
order until a successful connection is achieved. If this parameter is
specified and ProxyUsage is set to a value other than Override , an error
occurs.

-ProxyUsage <String>
Specifies the proxy usage settings. The acceptable values for this
parameter are:

- SystemDefault (the default): Use the system default proxy settings.

- NoProxy : Do not use a proxy to transfer the files. Use this option when
you transfer files within a local area network (LAN).

- AutoDetect : Automatically detect proxy settings. BITS detects proxy
settings for each file in the job.

- Override : Specify the proxies or servers to use. If the ProxyList
parameter is also specified, the proxies in that list are used. If the
ProxyBypass parameter is also specified, the servers in that list are
used. In both cases, the first member of the list is used. If the first
member is unreachable, the subsequent members are tried until a member is
contacted successfully.

-RetryInterval <Int32>

Specifies the minimum length of time, in seconds, that BITS waits before it attempts to transfer the file after BITS encounters a transient error. The minimum allowed value is 60 seconds. If this value exceeds the RetryTimeout value from the BitsJob object, BITS will not retry the transfer. Instead, BITS sets the state of the BITS transfer job to the Error state.

The default is 600 seconds (10 minutes).

-RetryTimeout <Int32>

Specifies the length of time, in seconds, that BITS attempts to transfer the file after the first transient error occurs. Setting the retry period to 0 prevents retries. If the retry period value exceeds the JobInactivityTimeout Group Policy setting (90-day default), BITS cancels the job.

The default value is 1,209,600 seconds (14 days).

-SecurityFlags <SecurityFlagValue>

Specifies security flags for the HTTP request.

The flags you can set, from the least significant bit, are the following bits:

- 1: Enable CRL Check.

- 2: Ignore incorrect common names in the server certificate.

- 3: Ignore incorrect dates in the server certificate.

- 4: Ignore incorrect certification authorities in the server certificate.

- 5: Ignore incorrect usage of the server certificate.

- 12: Allow redirection from HTTPS to HTTP.

Use bits 9 through 11 to implement your redirection policy:

- 0,0,0: Redirects are automatically allowed.

- 0,0,1: Remote name is updated if a redirect occurs.
-0,1,0: BITS fails the job if a redirect occurs.

-SetOwnerToCurrentUser [<SwitchParameter>]
Indicates that the cmdlet sets the owner of the BITS transfer job to the current user.

-TransferPolicy <CostStates>
Specifies the network cost states in which the transfer is allowed to be scheduled. The current cost state of the network is a bitmask that indicates the kinds of charges that would be incurred if a transfer was scheduled at this time. This cost state represents a bitmask; if the bit corresponding to the current network cost state is set, the transfer can be scheduled. If the bit corresponding to the current network cost state is not set, the transfer is ignored for scheduling purposes. You can submit any of the named values listed here, or add them together to provide a custom value.

The acceptable values for this parameter are:

- Unrestricted (or unknown) : 0x00000001 : the cost state for this network is not known.

- Capped : 0x00000002 : the cost state for this network is a capped plan,

or a plan that has a data usage limit.

- BelowCap : 0x00000004 : the cost state for this network is below the data plan cap.

- NearCap : 0x00000008 : the cost state for this network is near the data plan cap.

- OverCapCharged : 0x00000010 : the cost state for this network is above the data plan cap, and such usage is charged.

- OverCapThrottled : 0x00000020 : the cost state for this network is above the data plan cap, and such usage is throttled.

- UsageBased : 0x00000040 : the cost state for this network is charged based on usage.

- Roaming : 0x00000080 : the cost state for this network incurs roaming charges.

The cost state also includes one option (IgnoreCongestion) and a set of standard policies (Uncosted, Standard, NoSurcharge, NotRoaming, and Always) which are combinations of the discrete bit values.

- IgnoreCongestion : 0x80000000 : the job can be scheduled even if the network provider reports that the network is congested.

- PolicyUnrestricted : 0x80000021 : the set of cost states that do not consume the quota of a capped plan, or incur extra charges.

- Standard : 0x80000067 : a set of cost states suitable for moderate-priority transfers.

- NoSurcharge : 0x8000006f : the set of cost states that incur no surcharge for use.

- NotRoaming : 0x8000007f : the set of cost states that exclude the roaming state.

- Always : 0x800000ff : the set of all cost states.

The default value is determined by a combination of job priority and group policy. If this value is not explicitly set, it can vary when job priority or current group policy are modified.

-UseStoredCredential <AuthenticationTargetValue>

Specifies that credentials stored in the Windows Credential Manager should be used for authentication when required for the specified target server type. If this parameter is not specified and a server requires authentication, then explicit credentials must be included by using the Credential or ProxyCredential parameters. This parameter is a flag parameter whose values can be added together to create the desired behavior.

The acceptable values for this parameter are:

- None : Use only credentials provided by the Credential or ProxyCredential parameters. This is the default behavior if the parameter is not specified.

- Proxy : Credentials stored in the Windows Credential Manager are used for authentication for any proxy server that requires authentication. If no credentials in the Windows Credential Manager match the proxy server needing authentication, then you must specify credentials by using the ProxyCredential parameter.

- Server : This value is not supported and generates an error if specified.

-WhatIf [<SwitchParameter>]

Shows what would happen if the cmdlet runs. The cmdlet is not run.

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,
ErrorAction, ErrorVariable, WarningAction, WarningVariable,
OutBuffer, PipelineVariable, and OutVariable. For more information, see
about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

---- Example 1: Modify the priority of a BITS transfer job ----

PS C:\> $Bits = Get-BitsTransfer -JobId 10778CFA-C1D7-4A82-8A9D-80B19224879C
PS C:\> Set-BitsTransfer -BitsJob $Bits -Priority High

This command modifies the priority of an existing BITS transfer job.

The first command retrieves the BITS transfer job specified by the JobId
parameter and then stores it in the $Bits variable.

The second command uses the BitsJob parameter to pass the BitsJob object
stored in the $Bits variable to the Set-BitsTransfer cmdlet. The Priority
parameter is used to set the priority of the BITS transfer job to High.
--- Example 2: Set the owner of a set of BITS transfer jobs ---

PS C:\> Get-BitsTransfer -AllUsers -Name *Microsoft* | Set-BitsTransfer
-SetOwnerToCurrentUser

This command makes the current user the owner of a set of existing BITS
transfer jobs.

The output of the Get-BitsTransfer cmdlet is a set of BitsJob objects whose

display name contains Microsoft. This output is passed to the Set-BitsTransfer cmdlet through the pipeline. The SetOwnerToCurrentUser parameter specifies that the owner of each BITS transfer job is the current user.

- Example 3: Modify the proxy settings of a BITS transfer job -

```
PS C:\> $Bits = Get-BitsTransfer -JobId 10778CFA-C1D7-4A82-8A9D-80B19224879C
PS C:\> $Cred = Get-Credential
PS C:\> Set-BitsTransfer -BitsJob $Bits -ProxyUsage AutoDetect
-ProxyAuthentication $Cred
```

This command modifies the proxy settings of an existing BITS transfer job.

The first command retrieves the BITS transfer job identified by the JobId parameter and then stores it in the variable named $Bits.

The second command retrieves credentials from the user and then stores them in the $Cred variable.

The third command uses the BitsJob parameter to pass the BitsJob object stored in the $Bits variable to the Set-BitsTransfer cmdlet. It uses the ProxyAuthentication parameter to pass the PSCredential object stored in the $Cred variable. The ProxyUsage parameter allows the BITS transfer job to automatically discover the Web proxy server by using the Web Proxy Autodiscovery Protocol (WPAD) protocol. The supplied set of credentials is used to authenticate the user at the proxy server.

Example 4: Modify the proxy settings of a BITS transfer job using a proxy list and proxy bypass

```
PS C:\> Get-BitsTransfer | Set-BitsTransfer -ProxyUsage Override -ProxyList
"http://proxy1", "http://proxy2:81" -ProxyBypass "http://directconnect"
```

This command modifies the proxy settings of an existing BITS transfer job.

The output of the Get-BitsTransfer cmdlet is the set of BitsJob objects that are owned by the current user. This output is piped to the Set-BitsTransfer cmdlet. The Override value that is specified in the ProxyUsage parameter indicates that an explicit list of proxy server and bypassed host names are provided.

The ProxyList parameter specifies two proxy servers. The first server in the list (`http://proxy1`) is used. If that connection fails, the command tries the connection by using the second server in the list (`http://proxy2:81`). If both connections fail, the job fails.

When a list of host names is specified in the ProxyBypass parameter, the connection that is made is a direct connection that does not use a proxy server. In this example, no proxy server is used to add a file to the BITS transfer queue on the directconnect server.

REMARKS

To see the examples, type: "get-help Set-BitsTransfer -examples".
For more information, type: "get-help Set-BitsTransfer -detailed".
For technical information, type: "get-help Set-BitsTransfer -full".
For online help, type: "get-help Set-BitsTransfer -online"