

# **Port Scanner ActiveX Control for Microsoft® Windows™**

**Copyright © Magneto Software  
All rights reserved**

## Contents

|   |           |
|---|-----------|
| <b>1 PORT SCANNER ACTIVEX CONTROL OVERVIEW.....</b> | <b>3</b>  |
| 1.1 INTRODUCTION.....                               | 3         |
| 1.2 USAGE.....                                      | 3         |
| 1.3 PROPERTY SUMMARY .....                          | 4         |
| 1.4 EVENT SUMMARY .....                             | 4         |
| 1.5 METHOD SUMMARY.....                             | 4         |
| 1.6 ERROR CODES .....                               | 5         |
| <b>2 PROPERTIES .....</b>                           | <b>6</b>  |
| 2.1 OPTCONNECTTIMEOUT .....                         | 6         |
| 2.2 OPTPORTMIN .....                                | 7         |
| 2.3 OPTPORTMAX .....                                | 8         |
| 2.4 OPTPROMPTUSER.....                              | 9         |
| 2.5 OPTSCANMAXTCPOPENSOCKETS .....                  | 10        |
| 2.6 OPTSCANMODE.....                                | 11        |
| 2.7 OPTPREFERIPVERSION .....                        | 12        |
| 2.8 OPTSCANTIMEOUT .....                            | 13        |
| 2.9 OPTSTATUSUPDATEINTERVAL .....                   | 14        |
| <b>3 EVENTS.....</b>                                | <b>15</b> |
| 3.1 PORTSCANCOMPLETED.....                          | 15        |
| 3.2 PORTSCANFOUNDPORT .....                         | 16        |
| 3.3 PORTSCANQUERYCOMPLETED .....                    | 17        |
| 3.4 PORTSCANSTATUSUPDATE.....                       | 18        |
| <b>4 METHODS .....</b>                              | <b>19</b> |
| 4.1 ABOUTBOX .....                                  | 19        |
| 4.2 GETPORTSTABLEENTRYINFO .....                    | 20        |
| 4.3 GETPORTSTABLESIZE.....                          | 21        |
| 4.4 GETSERVBYPORT .....                             | 22        |
| 4.5 PORTSCANREMOTEHOST.....                         | 23        |
| 4.6 PORTSCANRESET .....                             | 24        |
| 4.7 RESETPORTSCANSETTINGS.....                      | 25        |

# 1 Port Scanner ActiveX Control Overview

## 1.1 Introduction

Port Scanner ActiveX control (skportscan.ocx) is a lightweight and powerful port scanner control. It allows developers to integrate port-scanning capabilities into their 32-Bit or 64-Bit applications.

Port Scanner ActiveX control can be used for network exploration or security auditing. Skportscan can determine what services (ports) are open (offered) by remote hosts.

It is capable of scanning multiple hosts simultaneously.

Skportscan can scan TCP ports in 3 different scan modes:

- Scan range of ports.

- Scan authorized ports only port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023, Registered Ports are those from 1024 through 49151, and the Dynamic and/or Private Ports are those from 49152 through 65535. The Well Known Ports are assigned by the IANA (Internet Assigned Numbers Authority) and on most systems can only be used by system (root level) processes or by programs executed by privileged users).

- Scan hostile ports only (ports that are mostly used for backdoors or Trojan programs.

Hackers/crackers that break into systems often start processes running on one of the following ports and then use them to either regain entry or launch attacks against other sites.

Skportscan ActiveX Control has one of the most complete ports databases available today built in, and, provides comprehensive APIs for accessing it.

The control can be used from any Windows-based applications development environment, including Visual Studio.

It comes with documentation, sample code, and working demo programs.

Additional information about protocol numbers can be found at this location:

[RFC 1700 - ASSIGNED NUMBERS](#)

## 1.2 Usage

Skportscan ActiveX Control can perform multiple TCP ports scans simultaneously while providing information from the ports usage database.

### **1.3 Property Summary**

#### **optConnectTimeout**

Specify timeout value in milliseconds to wait for replies.

#### **optPortMin**

Specify starting port number value for the range scan mode.

#### **optPortMax**

Specify ending port number value for the range scan mode.

#### **optPromptUser**

Specify whether to prompt before performing a scanning on remote host.

#### **optScanMaxTcpOpenSockets**

Limits number of simultaneously open TCP sockets.

#### **optScanMode**

Specify scan mode (“Authorized ports”, or “Hostile ports”, or “Range of ports”).

#### **PreferIpVersion**

Specify Internet Protocol version to use if name is resolved to both IPv4 and IPv6 addresses.

#### **optScanTimeout**

Specify timeout value in milliseconds to limit a port scanning process.

#### **optStatusUpdateInterval**

Specify timeout value in milliseconds between status update notifications.

### **1.4 Event Summary**

#### **PortScanCompleted**

Indicate that skportscan ActiveX Control has stopped processing port scan requests.

#### **PortScanFoundPort**

Indicate that skportscan ActiveX Control found open (offered) port on the remote host.

#### **PortScanQueryCompleted**

Indicate that skportscan ActiveX Control has stopped processing a single scan request.

#### **PortScanStatusUpdate**

Status update notification.

### **1.5 Method Summary**

#### **AboutBox**

Display a dialog box with skportscan ActiveX Control license and version information.

#### **GetPortsTableEntryInfo**

Get a ports table entry

#### **GetPortsTableSize**

Get a ports table size

#### **GetServByPort**

Retrieve service information corresponding to a port and protocol

#### **PortScanRemoteHost**

Start scanning.

#### **PortScanReset**

Stop scanning.

## [ResetPortScanSettings](#)

Reset all skportscan settings back to default values.

### **1.6 Error codes**

The following provides a complete listing of error codes returned by skportscan ActiveX Control.

|                          |   |
|--------------------------|---|
| ERROR_SUCCESS (0)        | No errors.  |
| ERROR_CANCELLED (1223)   | User canceled the operation.  |
| ERROR_TIMEOUT (1460)     | This operation returned because the timeout period expired.   |
| WSAEFAULT (10014)        | The <i>name</i> or the <i>namelen</i> parameter is not a valid part of the user address space, the <i>namelen</i> parameter is too small, or the <i>name</i> parameter contains incorrect address format for the associated address family. |
| WSAEINVAL (10022)        | An invalid argument was supplied.   |
| WSAEPFNOSUPPORT (10046)  | The protocol family has not been configured into the system or no implementation for it exists.   |
| WSAEADDRNOTAVAIL (10049) | The remote address is not a valid address (such as ADDR_ANY).   |
| WSAENETDOWN (10050)      | The network subsystem has failed.   |
| WSAENETUNREACH (10051)   | The network cannot be reached from this host at this time.  |
| WSAENOBUFS (10055)       | No buffer space is available. The socket cannot be connected.   |
| WSAENOTCONN (10057)      | The socket is not connected.  |
| WSAETIMEDOUT (10060)     | Attempt to connect timed out without establishing a connection.   |
| WSAECONNREFUSED (10061)  | The attempt to connect was forcefully rejected.   |

## 2 Properties

### 2.1 *optConnectTimeout*

#### **Summary**

Specify timeout value in milliseconds to wait for replies.

#### **Description**

This property specifies the timeout value in milliseconds that is used to wait for a reply when a request packet is sent. By default this value is set to 3000 milliseconds (3 seconds).

This property is of type long.

#### **VB Example**

```
Dim lConTimeout As Long
```

```
lConTimeout = 3000
```

```
SKPORTSCAN.optConnectTimeout = lConTimeout
```

## **2.2 optPortMin**

### **Summary**

Specify starting port number value for the “Range of Ports” scan mode.

### **Description**

This property specifies the starting port value the “Range of Ports” scan mode

The default value is 1.

The maximum possible value is 65535 (0xffff).

This property is of type long.

### **VB Example**

```
Dim lPortMin As Long
```

```
lPortMin = 1
```

```
SKPORTSCAN.optPortMin = lPortMin
```

## **2.3 optPortMax**

### **Summary**

Specify ending port number value for the “Range of Ports” scan mode.

### **Description**

This property specifies the ending port value the “Range of Ports” scan mode

The default value is 5000.

The maximum possible value is 65535 (0xffff).

This property is of type long.

### **VB Example**

```
Dim IPortMax As Long
```

```
IPortMax = 5000
```

```
SKPORTSCAN.optPortMax = IPortMax
```



## **2.4 optPromptUser**

### **Summary**

Specify whether to prompt before performing a scanning on remote host.

### **Description**

This property specifies if user needs to be prompted every time before performing a port scan on remote host.

The default value is 1 (True).

This property is of type integer.

### **VB Example**

```
Dim nPrompt As Integer  
nPrompt = 1  
SKPORTSCAN.optPromptUser = nPrompt
```

## **2.5 optScanMaxTcpOpenSockets**

### **Summary**

Limits number of simultaneously open TCP sockets.

### **Description**

This property specifies the maximum number of simultaneously open TCP sockets.

The default value is 64.

This property is of type short.

### **VB Example**

```
Dim nMaxTcpSockets As Integer
```

```
nMaxTcpSockets = 64
```

```
SKPORTSCAN.optScanMaxTcpOpenSockets = nMaxTcpSockets
```

## **2.6 optScanMode**

### **Summary**

Specify scan mode (“Authorized ports”, or “Hostile ports”, or “Range of ports”).

### **Description**

This property specifies the scan mode.

skportscan ActiveX Control can operate in 3 different scan modes:

- Scan range of ports.
- Scan authorized ports only port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023, Registered Ports are those from 1024 through 49151, and the Dynamic and/or Private Ports are those from 49152 through 65535. The Well Known Ports are assigned by the IANA (Internet Assigned Numbers Authority) and on most systems can only be used by system (root level) processes or by programs executed by privileged users).
- Scan hostile ports only (ports, that are mostly used for backdoors or trojan programs. Hackers/crackers that break into systems often start processes running on one of the following ports and then use them to either regain entry or launch attacks against other sites.

Scan Modes Values:

0 – Range of Ports

1 – Authorized Ports

2 – Hostile Ports

This property is of type short.

The default value is 2 (Scan hostile ports)

### **VB Example**

```
Dim nScanMode As Integer
```

```
nScanMode = 1           ‘Scan authorized ports
```

```
SKPORTSCAN.optScanMode = nScanMode
```

## **2.7 optPreferIpVersion**

### **Summary**

Specify Internet Protocol version to use if name is resolved to both IPv4 and IPv6 addresses

### **Description**

This property specifies the IP version to use when name is resolved to both IPv4 and IPv6 addresses..

Values:

0 – prefer IPv4

1 – prefer IPv6

The default value is 0 (prefer IPv4)

### **VB Example**

```
Dim nPreferIpVersion As Integer
```

```
nPreferIpVersion = 0 ' Prefer IPv4
```

```
SKPORTSCAN.optPreferIpVersion = nPreferIpVersion
```

## **2.8 optScanTimeout**

### **Summary**

Specify timeout value in milliseconds to limit a port scanning process.

### **Description**

This property specifies the timeout value in milliseconds that is used to limit a port scanning process.

By default this value is set to 300000 milliseconds (300 sec, or 5 min).

This property is of type long.

### **VB Example**

```
Dim lScanTimeout As Long
```

```
lScanTimeout = 300000
```

```
SKPORTSCAN.optScanTimeout = lScanTimeout
```

## **2.9 *optStatusUpdateInterval***

### **Summary**

Specify timeout value in milliseconds between status update notifications.

### **Description**

This property specifies the timeout value in milliseconds between status update notifications.

By default this value is set to 3000 milliseconds (3 seconds).

To disable update notifications completely, the value needs to be set to 0.

This property is of type long.

### **VB Example**

```
Dim lStatusUpdateInterval As Long
```

```
lStatusUpdateInterval = 3000
```

```
SKPORTSCAN.optStatusUpdateInterval = lStatusUpdateInterval
```

## **3 Events**

### **3.1 PortScanCompleted**

#### **Summary**

Indicate that skportscan ActiveX Control has stopped processing port scan requests.

#### **Syntax**

PortScanCompleted(void);

#### **Description**

Indicate that skportscan.ocx has stopped processing requests.

#### **Parameters**

*None.*

## **3.2 PortScanFoundPort**

### **Summary**

Indicate that skportscan ActiveX Control found open (offered) port on the remote host.

### **Syntax**

PortScanFoundPort(BSTR bstrRemoteHostName, short nProtocol, long lPortNumber, BSTR  
bstrPortKeyWord, short nUsage, BSTR bstrAuthorizedUsageDescription,  
BSTR bstrHostileUsageDescription);

### **Description**

Indicate that skportscan ActiveX Control found open (offered) port on the remote host.

### **Parameters**

bstrRemoteHostName is the name of the remote host that is queried,

nProtocol is open port's protocol (Possible values: 1 – TCP).

lPortNumber is port for a service, in host byte order.

bstrPortKeyWord is service keyword (See [RFC 1700 - ASSIGNED NUMBERS](#) for more details)

nUsage indicates usage of the open port (Possible values: 0 – Authorized, or Legitimate usage, no information about trojans is available; 1 – Dual usage, there are common trojans that might use this port number; 2 – Hostile usage, there is no information in skportscan ports database regarding legitimate use of this port.

bstrAuthorizedUsageDescription is authorized usage description (from skportscan ports usage database)

bstrHostileUsageDescription is hostile usage description (from skportscan ports usage database).

In case of multiple programs known to use the same port number, multiple values will be separated by semicolon.



### **3.3 PortScanQueryCompleted**

#### **Summary**

Indicate that skportscan ActiveX Control has stopped processing a single scan request.

#### **Syntax**

```
PortScanQueryCompleted(BSTR bstrRemoteHostName, short nProtocols, long lStatus, long  
    lTcpPortMin, long lTcpPortMax, long lTcpPortCount, long lUdpPortMin, long  
    lUdpPortMax, long lUdpPortCount, long lElapsedTime);
```

#### **Description**

Indicate that skportscan ActiveX Control has stopped processing a single scan request.

#### **Parameters**

*bstrRemoteHostName* is the name of the remote host that was queried,

*nProtocols* is protocols used.

*lStatus* is the return status of each individual reply. See section [1.6 Error Codes](#) for the complete list of supported error codes,

*lTcpPortMin* is starting scanned TCP port.

*lTcpPortMax* is ending scanned TCP port.

*lTcpPortCount* is total number of scanned TCP ports.

*lUdpPortMin* is starting scanned UDP port.

*lUdpPortMax* is ending scanned UDP port.

*lUdpPortCount* is total number of scanned UDP ports.

*lElapsedTime* is elapsed time in milliseconds

### **3.4 PortScanStatusUpdate**

#### **Summary**

Status update notification.

#### **Syntax**

```
PortScanStatusUpdate(BSTR strRemoteHostName, short nProtocols, long dwElapsedTime, long  
                    lCountTcpPortsScanned, long lCountTcpPortsTotal, long  
                    lCountUdpPortsScanned, long lCountUdpPortsTotal);
```

#### **Description**

Status update notification while performing port scans. The interval between notifications is defined by property [optStatusUpdateInterval](#). To disable notification completely, set optStatusUpdateInterval to 0.

#### **Parameters**

bstrRemoteHostName is the name of the remote host that is queried,

nProtocols is protocols used

lElapsedTime is elapsed time in milliseconds

lCountTcpPortsScanned is total scanned TCP ports.

lCountTcpPortsTotal is total TCP ports to scanned in this scan query.

lCountUdpPortsScanned is total scanned UDP ports.

lCountUdpPortsTotal is total UDP ports to scanned in this scan query.

## **4 Methods**

### **4.1 AboutBox**

#### **Summary**

Display a dialog box with skportscan ActiveX Control license and version information.

#### **Syntax**

```
void AboutBox();
```

#### **Description**

This method could be used to display version license information or to register skportscan.ocx control.

#### **Parameters**

None.

## 4.2 GetPortsTableEntryInfo

### Summary

Get a ports table entry

### Syntax

```
long GetPortsTableEntryInfo(short nProtocol, short nTableType, long lEntryIndex, long*  
    plMinPortNumber, long* plMaxPortNumber, BSTR* pbstrPortKeyWord,  
    short* pnUsage, BSTR* pbstrAuthorizedUsageDescription, BSTR*  
    pbstrHostileUsageDescription);
```

### Description

The GetPortsTableEntryInfo method retrieves an entry from the ports database.

It returns a long, which is set to 0 (ERROR\_SUCCESS) if the method is successfully executed, otherwise it will be set to the error code from section [1.6 Error Codes](#).

### Parameters

nProtocol is the protocol to use (Possible values: 1 – TCP; 2 – UDP).

nTableType is the table type (Possible values: 0 – Authorized ports table; 1 - Hostile Ports table).

lEntryIndex is an ordinal entry index in the table (starting from 0). Table size can be retrieved by calling method [GetPortsTableSize\(\)](#).

If method returns successfully, the following parameters will be filled:

plMinPortNumber will contain a minimum port number value

plMaxPortNumber will contain a maximum port number value.

If plMaxPortNumber is not equal to plMinPortNumber, it means that retrieved information is for the range, rather than for the single port. Vast majority of the entries in the skportscan database define a single port, not a range of ports.

pbstrPortKeyWord will contain a port key word, if available.

pnUsage will contain a port usage (Authorized, Dual or Hostile). See section [3.2 PortScanFoundPort](#) for more details.

pbstrAuthorizedUsageDescription will contain an authorized usage description, if available.

pbstrHostileUsageDescription will contain a hostile usage description, if available.

### **4.3 GetPortsTableSize**

#### **Summary**

Get a ports table size

#### **Syntax**

```
long GetPortsTableSize(short nProtocol, short nTableType);
```

#### **Description**

The GetPortsTableSize method retrieves an table size from the ports database.

If successful, it returns a non-zero value.

#### **Parameters**

nProtocol is protocol to use (Possible values: 1 – TCP; 2 – UDP).

nTableType is the table type (Possible values: 0 – Authorized ports table; 1 - Hostile Ports table).

## 4.4 GetServByPort

### Summary

Retrieve service information corresponding to a port and protocol

### Syntax

```
long GetServByPort(long lPortNumber, short nProtocol, BSTR* pbstrPortKeyWord, short*  
pnUsage, BSTR* pbstrAuthorizedUsageDescription, BSTR*  
pbstrHostileUsageDescription);
```

### Description

Retrieve service information corresponding to a port and protocol

It returns a long, which is set to 0 (ERROR\_SUCCESS) if the method is successfully executed, otherwise it will be set to the error code 1168 (ERROR\_NOT\_FOUND).

### Parameters

lPortNumber is the protocol number.

nProtocol is the protocol to use (Possible values: 1 – TCP; 2 – UDP).

If method returns successfully, the following parameters will be filled:

pbstrPortKeyWord will contain a port key word, if available.

pnUsage will contain a port usage (Authorized, Dual or Hostile). See section [3.2 PortScanFoundPort](#) for more details.

pbstrAuthorizedUsageDescription will contain an authorized usage description, if available.

pbstrHostileUsageDescription will contain a hostile usage description, if available.

## ***4.5 PortScanRemoteHost***

### **Summary**

Start scanning.

### **Syntax**

```
long PortScanRemoteHost(BSTR bstrRemoteHostName);
```

### **Description**

Start scanning.

### **Parameters**

bstrRemoteHostName is the name of the remote host that will be scanned,

## **4.6 PortScanReset**

### **Summary**

Stop scanning.

### **Syntax**

void PortScanIsReset (void)

### **Description**

The PortScanReset method terminates any pending scan requests.

### **Parameters**

None.



## **4.7 ResetPortScanSettings**

### **Summary**

Reset all skportscan settings back to default values.

### **Syntax**

```
void ResetPortScanSettings(void)
```

### **Description**

Reset all skportscan settings back to default values.

### **Parameters**

None.