WindX and Security

PxPlus 2017 (v14) & PxPlus 2018 (v15)

DireXions 2018

WindX and Security

- Industry-wide problem
  - A few bad apples …
  - Approaches based on Canadian law CASL

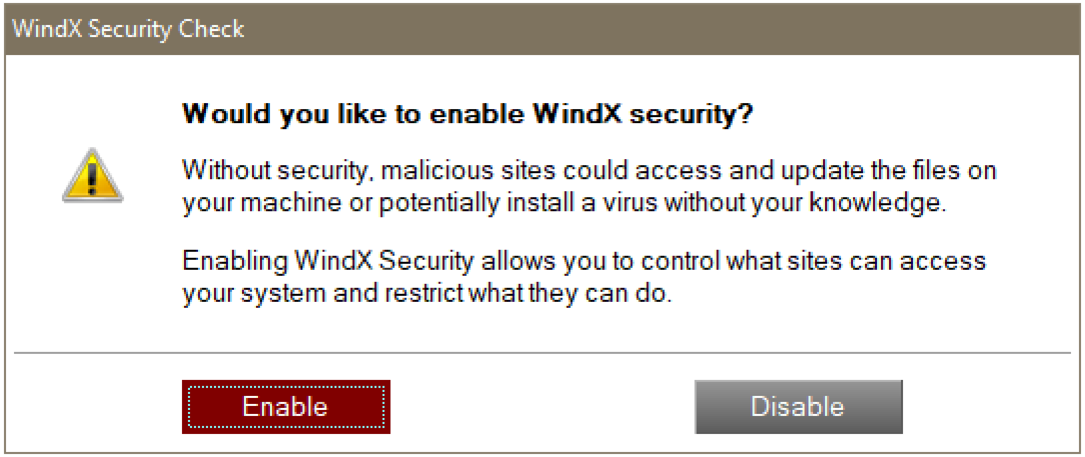
- Two areas of concern
  - Controlling access to the workstation
    - Restricting what the server can do to workstation
      - What it can read/write
      - What it can run
    - Assure end user acknowledges access rights
  - Assuring **secure** connection to **proper** host
    - Networks can be compromised
    - Public networks can 'spoof' servers

2017

Controlling Workstation Access

WindX System menu allows user to change their mind

- On initial launch of WindX system confirms if user wants access controls enabled.

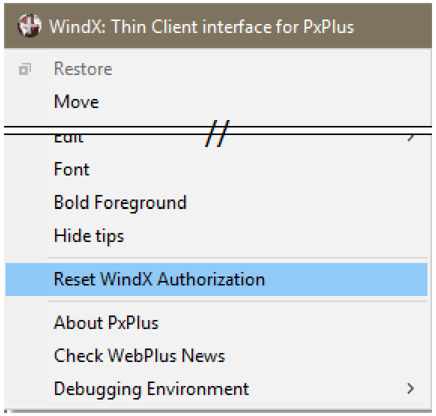


WindX Security Check

Would you like to enable WindX security?

Without security, malicious sites could access and update the files on your machine or potentially install a virus without your knowledge.

Enabling WindX Security allows you to control what sites can access your system and restrict what they can do.



WindX: Thin Client interface for PxPlus

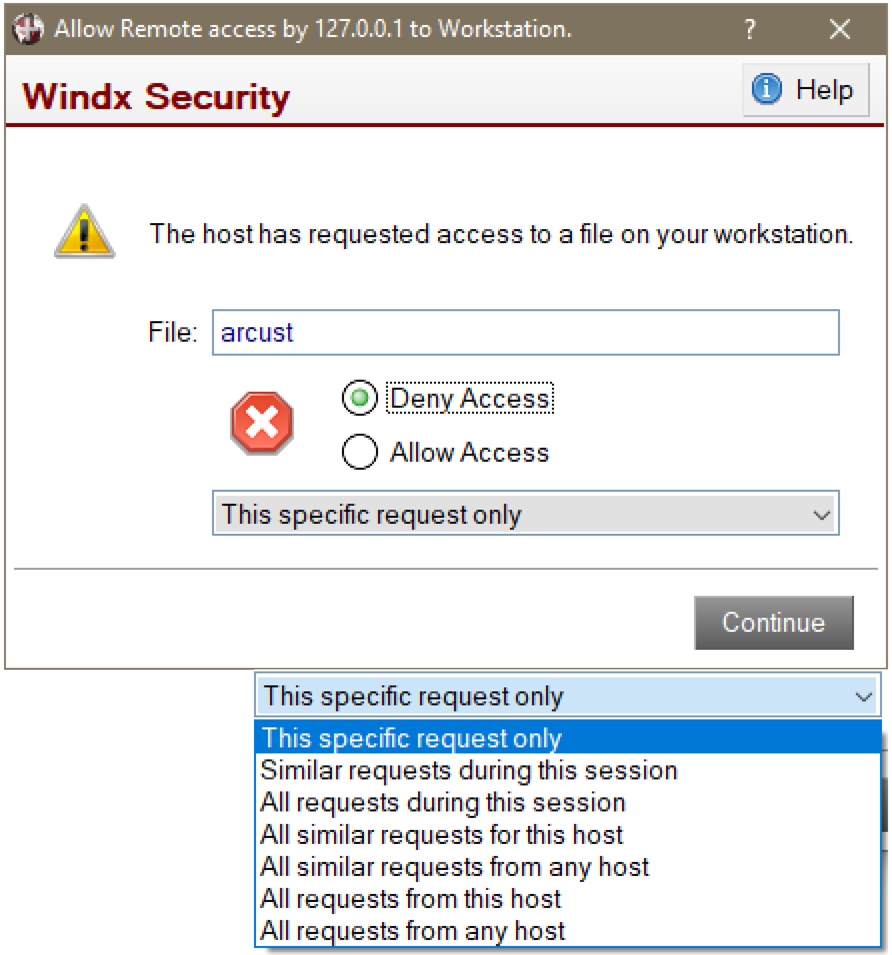
  - If they Disable security, no further question asked regardless of what server they connect to and regardless of what the server tries to do to their workstation

WindX System menu allows user to change their mind

2017

Controlling Workstation Access

WindX confirms access with user



Allow Remote access by 127.0.0.1 to Workstation.

Windx Security

The host has requested access to a file on your workstation.

File: arcust

● Deny Access

○ Allow Access

This specific request only

This specific request only

- This specific request only
- Similar requests during this session
- All requests during this session
- All similar requests for this host
- All similar requests from any host
- All requests from this host
- All requests from any host

- User CAN **deny** or **allow**
  - Local file reading
  - Local file updates
  - Running local Windows programs
  - Executing PxPlus logic locally

- Drop box provides user to set option for
  - Specific request
  - Current session
  - Similar requests
  - Based on host

2017

Assuring Connection to Host

Options only available with Simple CS

For more information see SSL Certificates PDF

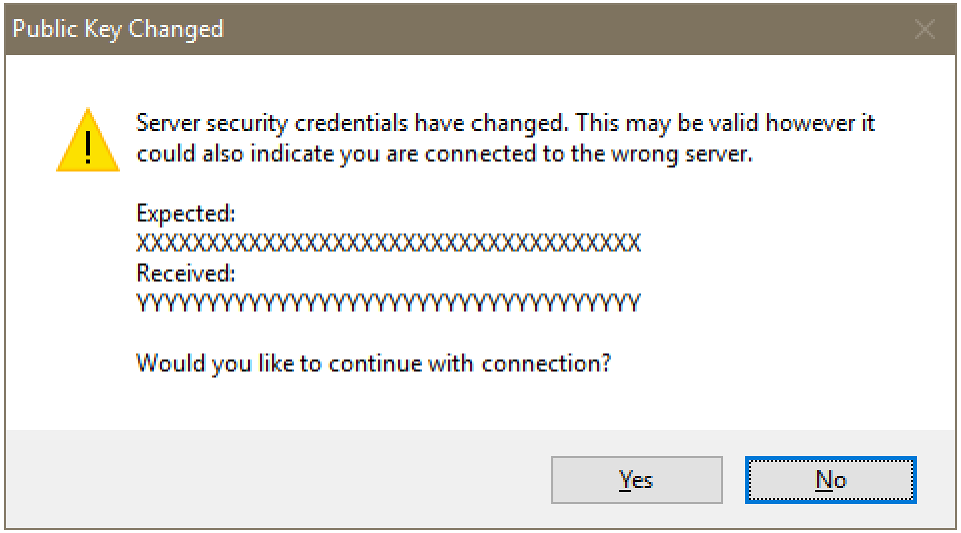
- Two major concerns
  - Is this connection secure enough?
    - SSL has multiple encryption algorithms and protocol versions
    - You should disable old protocols and ciphers on the server by including
      - NoSSLV2, NoSSLV3
      - CIPHERS=HIGH:MEDIUM:!ADH
  - Does server have proper certificate?
    - Option following 'secure'
      - CERTIFICATE=VALIDATE | TRUST
    - Checks host name, expiry date
      - Optionally certificate came from **TRUSTED** source

2017

Assuring Connection to Host

Option only available with Simple CS

- Host has a unique "Public" encryption key
  - Used to encrypt SSL communication
  - Simple CS with WindX can check this
    - Can be specified on the command line
      - Follows the SECURE option in argument 1
    - Default is to save on 1st connect and reports differences should they occur



Public Key Changed

Server security credentials have changed. This may be valid however it could also indicate you are connected to the wrong server.

Expected:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Received:
YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY

Would you like to continue with connection?

2017

Assuring Connection to Host

Option only available with Simple CS

- PUBKEY options

```
...\pxplus.exe *plus/cs/client –arg server;port;pubkey=XXXX...
```

- Only allows connection if public key matches

```
...\pxplus.exe *plus/cs/client –arg server;port;pubkey=check
```

- Ask user on first connection to manually validate public key

- Can be included in a .WINDX file

Additional Resources

The help link(s) below refer to the current on-line help pages. The functionality may have been further updated since the PxPlus 2018 (version 15) release.

- WindX Security
- WindX Overview
- Simple Client Server (CS) Interface