Restrict SMB Access to a Share

HAMMERSPACE

Table of Contents

Applies to: Hammerspace 5.3 and later.

By default a share's access control list grants **Everyone** full control, much as a Windows share does, and SMB clients may reach the share from any client IP address to any DSX static or floating portal IP address. File and folder permissions still determine what a user can do with the contents.

Turning off the SMB **Browseable** setting hides the share, but does not stop a client that knows the path from reaching it.

To actually block SMB access, add an access control entry to the share ACL that denies authenticated users.

- Members of the built-in Administrators group can still reach the share over SMB.
- The share ACL limits access for every protocol, not just SMB. Unix users can be represented through the NFSv4 special principals `owner@`, `group@`, and `everyone@`, and through Windows named principals where RFC 2307 attributes are populated.
- The deny entry may appear to be less than full control, but it does block SMB access for non-administrators.

1. Edit the Share ACL from Microsoft Management Console

To use the Shared Folders snap-in, you must be a member of the built-in Administrators group, and the cluster must be running 5.0.20-588 or later, or 5.1.18-262 or later. If it is not, use the `icacls` method instead.

1. Open Microsoft Management Console and choose **File** › **Add or Remove Snap-ins**.

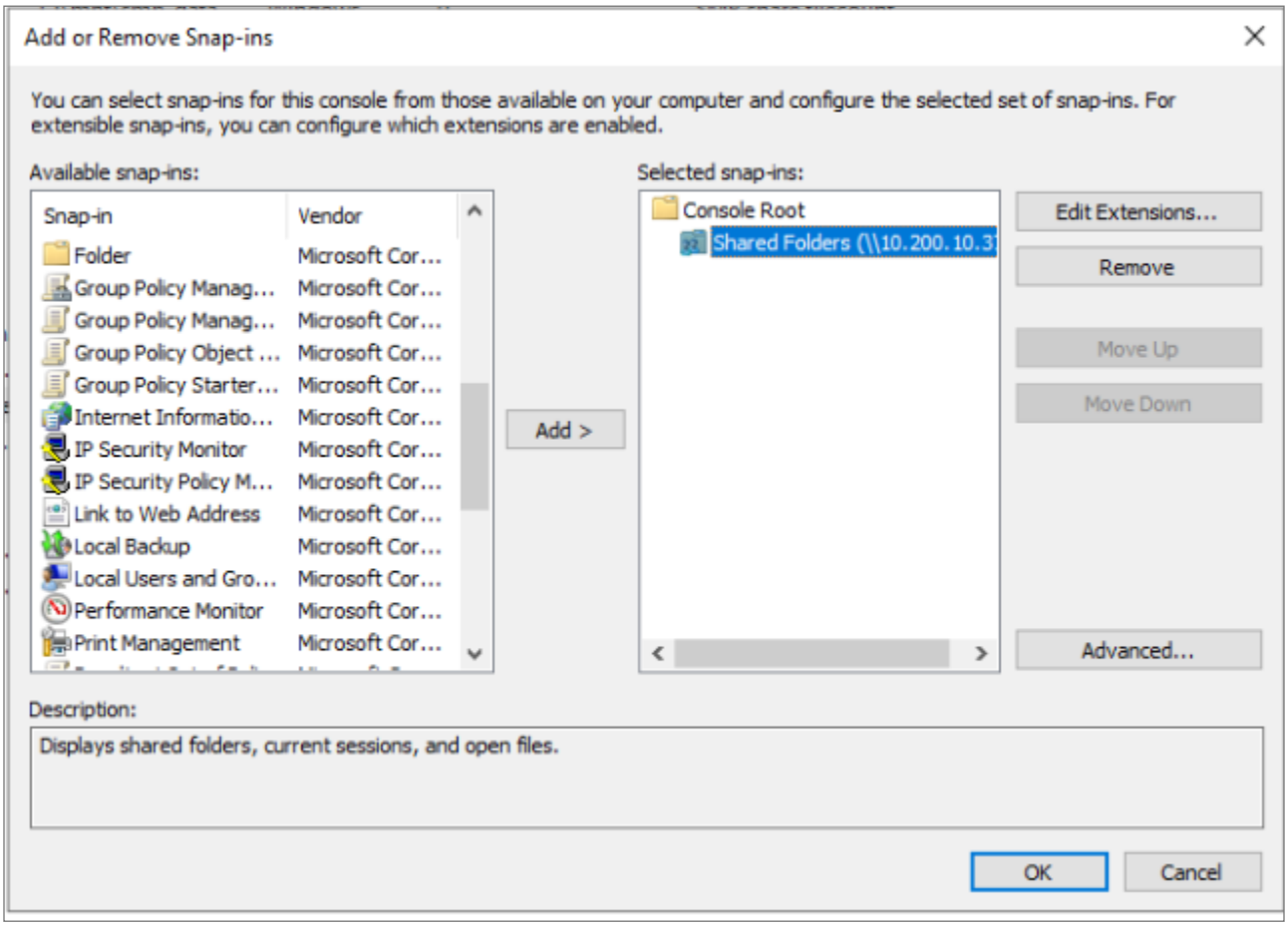

Figure 1. Adding a snap-in

2. Add **Shared Folders**, select **Another Computer**, enter a DSX floating IP address or hostname, and click **Finish**.

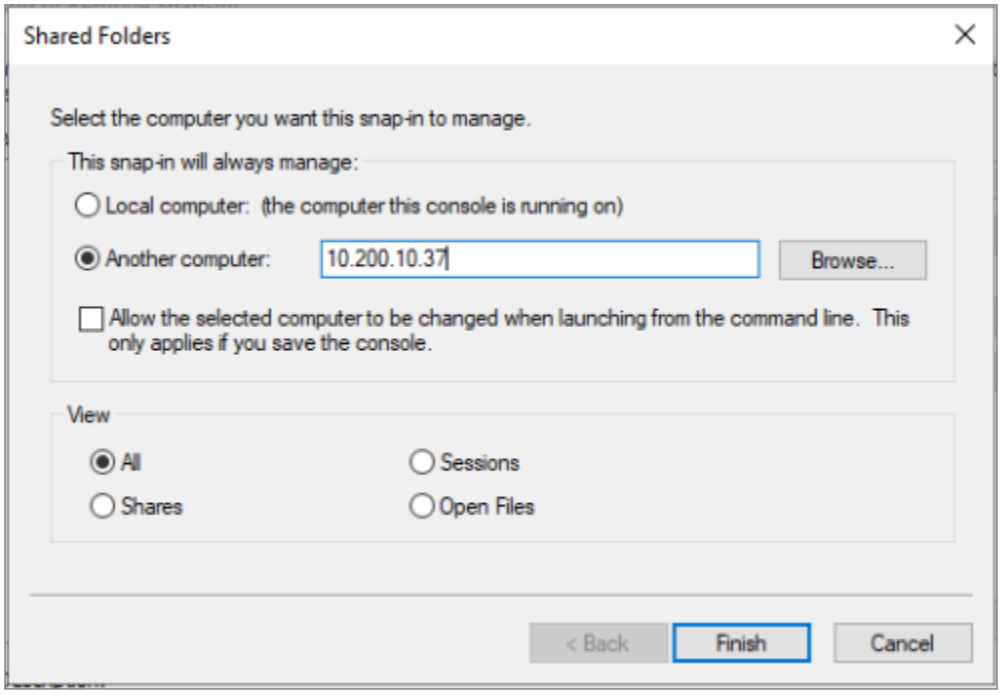

Figure 2. Pointing the snap-in at a DSX floating IP address

3. Double-click **Shares**.

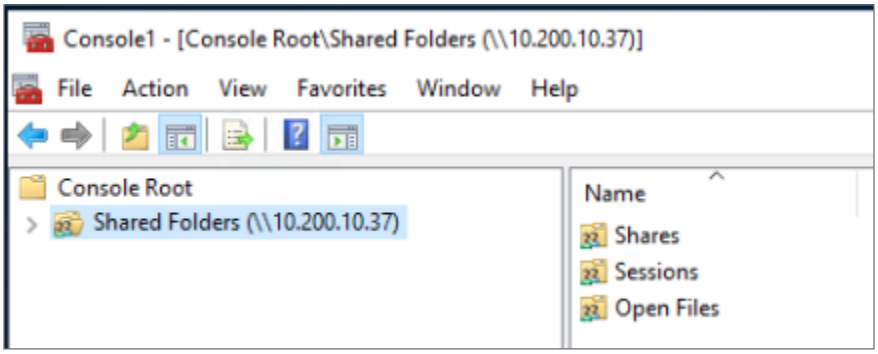

Figure 3. The Shares node

4. Right-click the share and open the **Share Permissions** tab.

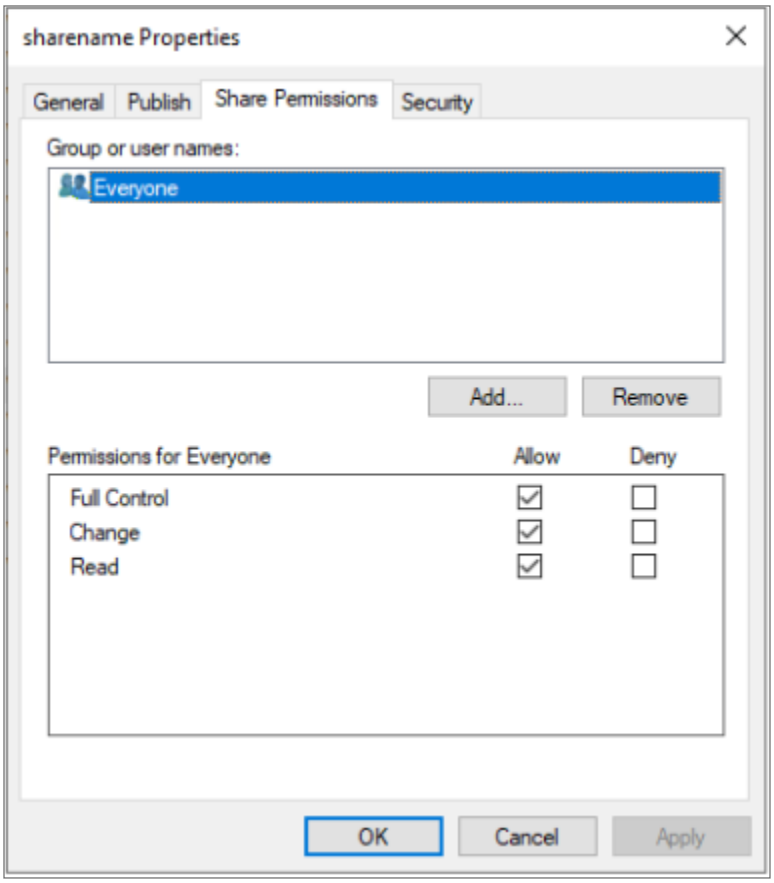

Figure 4. The Share Permissions tab

5. Click **Add**, set the location to **Entire Directory**, add **Authenticated Users**, click **Check Names**, and click **OK**.

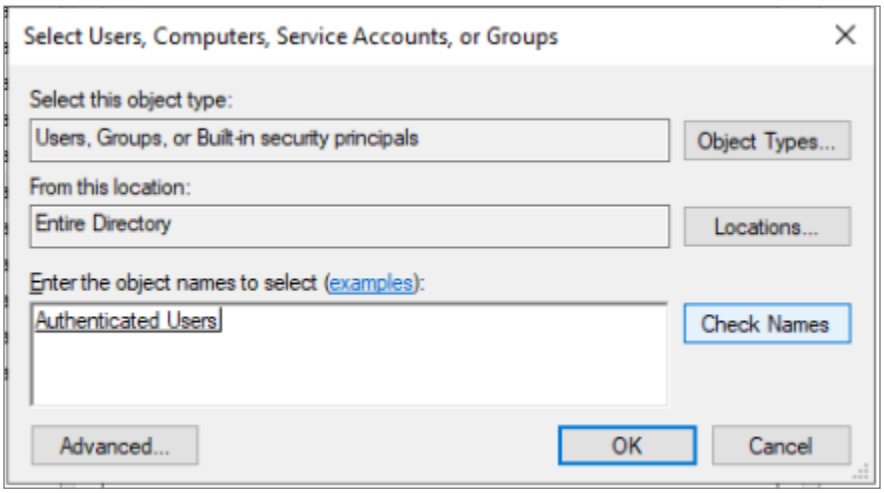

Figure 5. Adding Authenticated Users

6. Select **Deny** for **Full Control** against **Authenticated Users**.

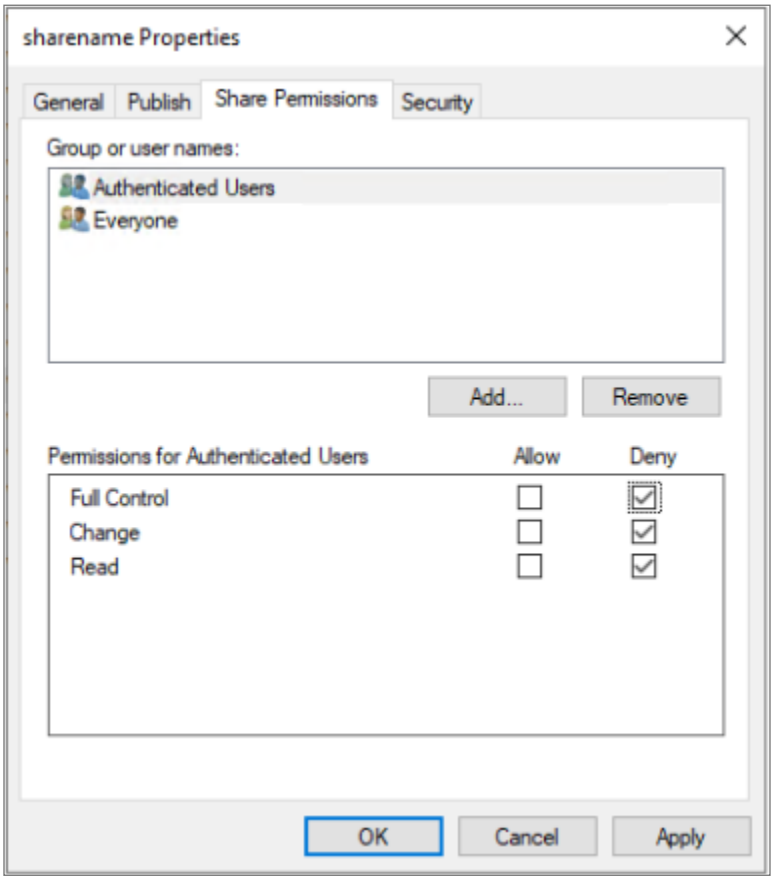

Figure 6. Denying full control to Authenticated Users

7. Give **Everyone** the permissions the share needs — full control, in this example.

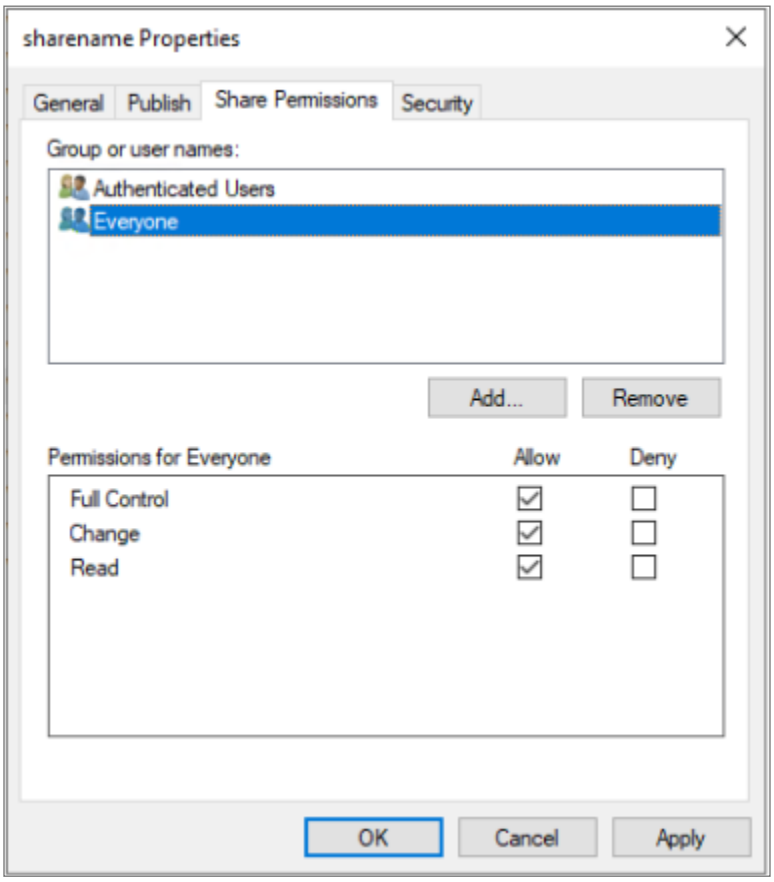

Figure 7. Setting the permissions for Everyone

8. Click **Apply** and confirm with **Yes**.

Figure 8. Confirming the change

The current Microsoft plug-in does not display the deny entry correctly. Verify it separately, as described below.

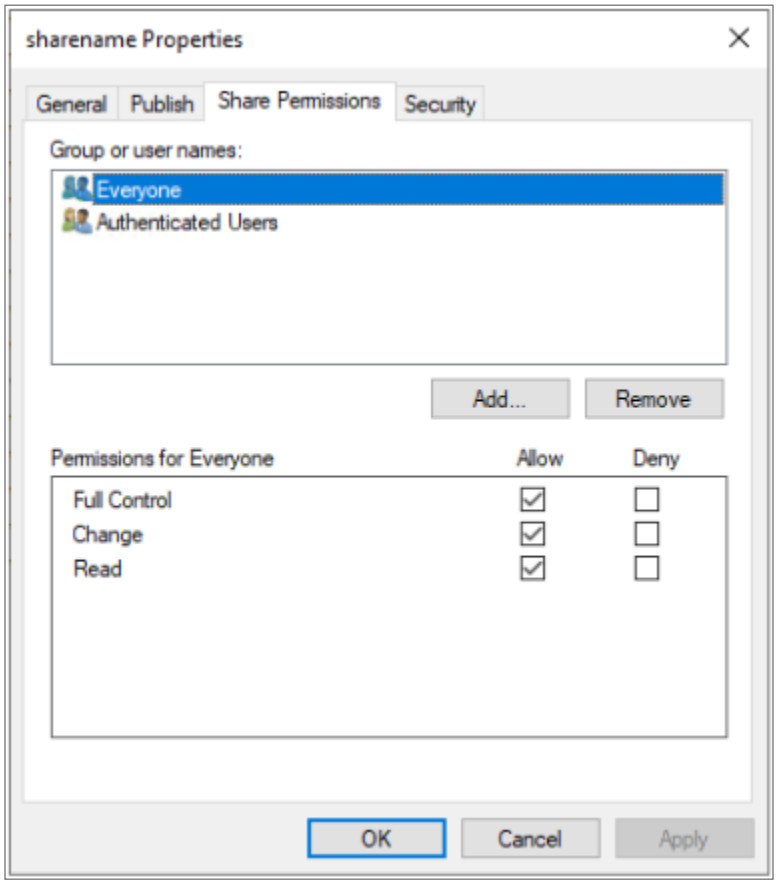

Figure 9. The permissions as the snap-in displays them

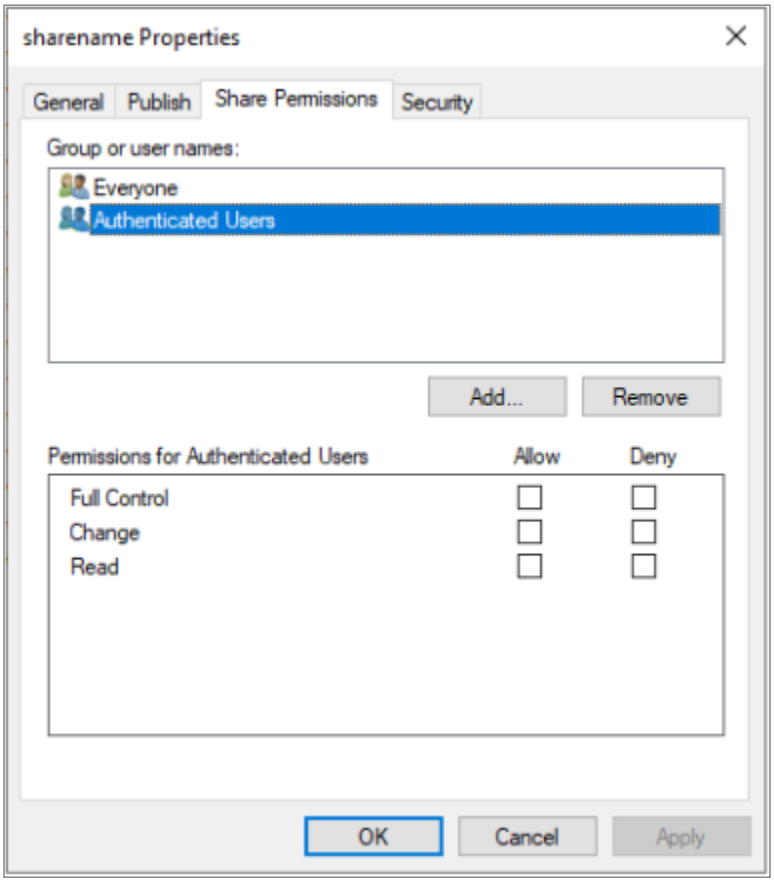

Figure 10. The share after the change

Display the real ACL from a Windows host using the UNC path to the share's `.share_attributes` file:

```
PS C:\Windows\system32> icacls \\10.200.10.37\sharename\.share_attributes
\\10.200.10.37\sharename\.share_attributes NT AUTHORITY\Authenticated Users:(DENY)(Rc,WDAC,S,RD,WD,AD,X,RA,WA)
                                           Everyone:(F)

Successfully processed 1 files; Failed processing 0 files
```

Figure 11. The true ACL shown by icacls

Authenticated SMB users who are not administrators now see a permission denied error.

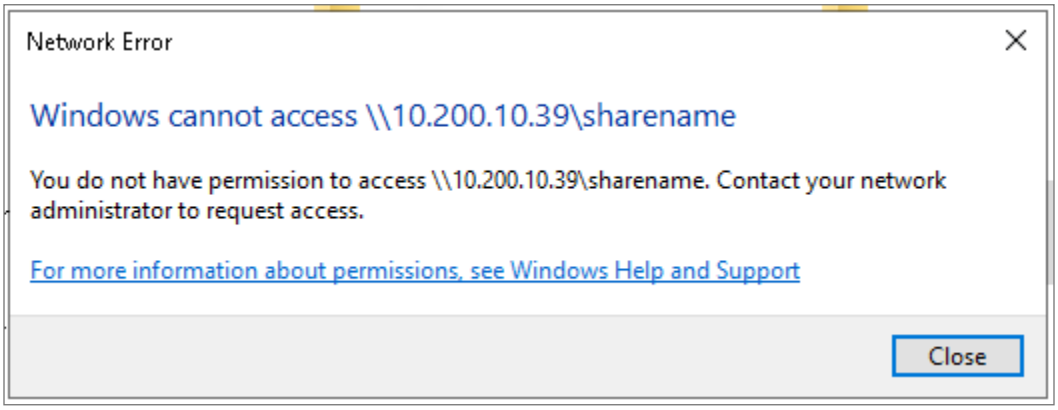

Figure 12. The error a restricted client sees

2. Edit the Share ACL with icacls

To use `icacls`, you must be a member of the built-in Administrators group, directly or through a group.

Show the current share ACL:

Command:

```
icacls \\<dsx-ip-address>\<share>\.share_attributes
```

Deny authenticated users, using the well-known security identifier `S-1-5-11`:

Command:

```
icacls \\<dsx-ip-address>\<share>\.share_attributes /deny *S-1-5-11:F
```

Show the result:

```
\\<dsx-ip-address>\<share>\.share_attributes
NT AUTHORITY\Authenticated Users: (DENY) (Rc, WDAC, S, RD, WD, AD, X, RA, WA)
Everyone: (F)
Successfully processed 1 files; Failed processing 0 files
```

Authenticated SMB users who are not administrators now see a permission denied error.

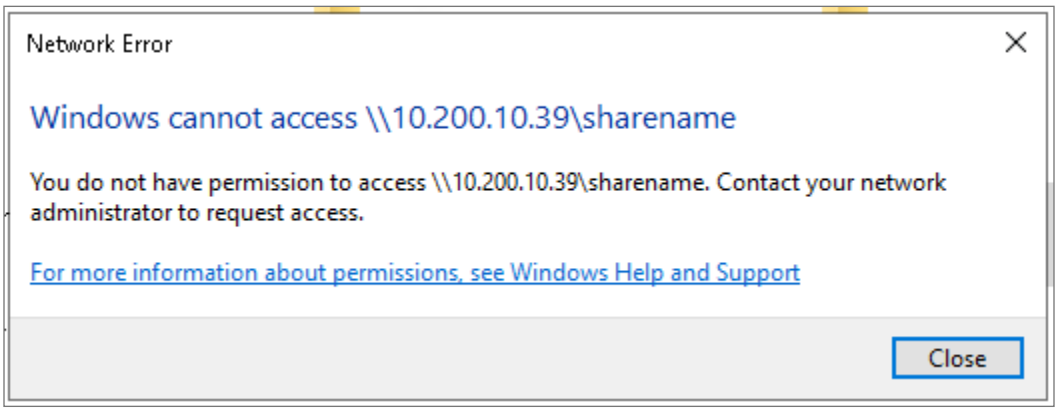

Figure 13. The error a restricted client sees