



# **Storage zones controller 5.x**

## Contents

<b>About storage zones controller</b>	<b>3</b>
<b>Architecture overview</b>	<b>6</b>
<b>System requirements</b>	<b>14</b>
<b>Install</b>	<b>19</b>
<b>Configure Citrix ADC for storage zones controller</b>	<b>20</b>
<b>Configure Citrix ADC manually</b>	<b>28</b>
<b>Create a network share for private data storage</b>	<b>32</b>
<b>Install an SSL certificate</b>	<b>35</b>
<b>Prepare your server for ShareFile data</b>	<b>35</b>
<b>Install storage zones controller and create a storage zone</b>	<b>44</b>
<b>Verify your storage zones controller setup</b>	<b>57</b>
<b>Change the default zone for user accounts</b>	<b>58</b>
<b>Specify a proxy server for storage zones</b>	<b>59</b>
<b>Configure the domain controller to trust the storage zones controller for delegation</b>	<b>60</b>
<b>Configure storage zones controller for Web App previews, thumbnails, and view-only sharing</b>	<b>61</b>
<b>Configure multitenant storage zones</b>	<b>67</b>
<b>Upgrade</b>	<b>69</b>
<b>Manage storage zones controllers</b>	<b>71</b>
<b>Join a secondary storage zones controller to a storage zone</b>	<b>72</b>
<b>Change the address or passphrase of a primary storage zones controller</b>	<b>73</b>
<b>Demote and promote storage zones controllers</b>	<b>74</b>
<b>Disable, delete, or redeploy a storage zones controller</b>	<b>75</b>

<b>Transfer files to a new network share</b>	<b>76</b>
<b>Back up a primary storage zones controller configuration</b>	<b>77</b>
<b>Recover a primary storage zones controller configuration</b>	<b>80</b>
<b>Replace a primary storage zones controller</b>	<b>83</b>
<b>Prepare storage zones controller for file recovery</b>	<b>84</b>
<b>Recover files and folders from your ShareFile Data backup</b>	<b>91</b>
<b>Reconcile the ShareFile cloud with a storage zone</b>	<b>93</b>
<b>Windows Server 2012R2 Migration Guide for ShareFile storage zones</b>	<b>94</b>
<b>Configure antivirus scans of uploaded files</b>	<b>95</b>
<b>Migrate ShareFile data</b>	<b>100</b>
<b>Connector Favorites</b>	<b>102</b>
<b>Manage storage zones for ShareFile data</b>	<b>103</b>
<b>Create and manage storage zone connectors</b>	<b>106</b>
<b>Data Loss Prevention</b>	<b>113</b>
<b>Monitor</b>	<b>121</b>
<b>Reference: Storage zones controller configuration files</b>	<b>131</b>

## About storage zones controller

April 2, 2024

Storage zones controller extends the ShareFile Software as a Service (SaaS) cloud storage by providing your ShareFile account with private data storage.

For more information about storage zones controller, such as the components, data storage, and more, see [Storage zones controller 5.x](#).

See [What's new](#) for the latest enhancements in this and ShareFile.

To download the latest version of ShareFile Storagezone controller, see <https://dl.sharefile.com/storagezone-controller>. Sign in to your ShareFile account to access all application downloads.

### TIP:

ShareFile recommends that users enable [Threat detection alerts](#).

## Fixed issues

### Fixed issues in storage zones controller 5.11.25

This release addresses several issues that improve overall performance and stability.

### Fixed issues in storage zones controller 5.11.24

**Security fixes:** This release contains fixes for security and reliability.

### Fixed issues in storage zones controller 5.11.23

**Security fixes:** This release contains fixes for security and reliability.

### Fixed issues in storage zones controller 5.11.22

**Security fixes:** This release contains fixes for security and reliability.

### Fixed issues in storage zones controller 5.11.21

**Security fixes:** This release contains fixes for security and reliability.

#### **Fixed issues in storage zones controller 5.11.18**

**Security fixes:** This release contains fixes for security and reliability.

#### **Fixed issues in storage zones controller 5.11.17**

**Security fixes:** This release contains fixes for security and reliability.

#### **Fixed issues in storage zones controller 5.11**

This release addresses a number of issues that improve overall performance and stability.

#### **Fixed issues in storage zones controller 5.10**

This release addresses a number of issues that help to improve overall performance and stability.

#### **Fixed issues in storage zones controller 5.9**

This release contains fixes to improve reliability and performance.

#### **Fixed issues in storage zones controller 5.8**

This release contains a fix to improve error messaging for checked out files and a fix for newly published managed paths in SharePoint.

#### **Fixed issues in storage zones controller 5.7**

This release contains fixes to address a redirect issue in file uploads to storage zone and on-premises connectors.

#### **Fixed issues in storage zones controller 5.6**

**WOPI Fix:** Includes changes to resolve issues seen when trying to edit office files subsequent times.

**SharePoint Connector Fix:** This release includes changes to display valid error messages when creating folders that already exist on SharePoint Connector.

## **Fixed issues in storage zones controller 5.5**

This release contains fixes to improve reliability and performance.

## **Fixed issues in storage zones controller 5.4.2**

**SharePoint Connector Fix:** Moving files that are present on the SharePoint connector might fail for specific scenarios. This release ensures that moving files that are present on SharePoint Connector works as expected.

**Security fixes:** This release contains fixes for security and reliability.

## **Fixed issues in storage zones controller 5.4.1**

**Security fixes:** This release contains fixes for security and reliability.

**Additional support:** Support has been added for *cloud*/*cloudburrito* accounts for the Workspace environment.

## **Fixed issues in storage zones controller 5.3.1**

This release contains fixes to improve reliability and performance.

## **Fixed issues in storage zones controller 5.3.1**

**WOPI Fix:** WOPI access tokens were potentially spoofed by theft of the public cryptographic key. This version ensured that the key is not shared between storage zones controllers.

**Security fixes:** This release contains fixes for security, performance, and reliability.

## **Known issues**

### **Known issues in storage zones controller 5.10**

No new issues have been observed in this release.

### **Known issues in storage zones controller 5.9**

No new issues have been observed in this release.

### **Known issues in storage zones controller 5.8**

No new issues have been observed in this release.

### **Known issues in storage zones controller 5.7**

No new issues have been observed in this release.

## **Architecture overview**

December 9, 2019

This section provides an overview to deploying storage zones controller for proof-of-concept evaluations or high-availability production environments. High-availability deployment is shown both with and without a DMZ proxy such as Citrix ADC.

To evaluate a deployment with multiple storage zones controllers, follow the guidelines for a high availability deployment.

Each of the deployment scenarios require a ShareFile Enterprise account. By default, ShareFile stores data in the secure ShareFile-managed cloud. To use private data storage, either an on-premises network share or a supported third-party storage system, configure storage zones for ShareFile Data.

To securely deliver data to users from network file shares or SharePoint document libraries, configure storage zone connectors.

### **Storage zones controller proof of concept deployment**

#### **Caution:**

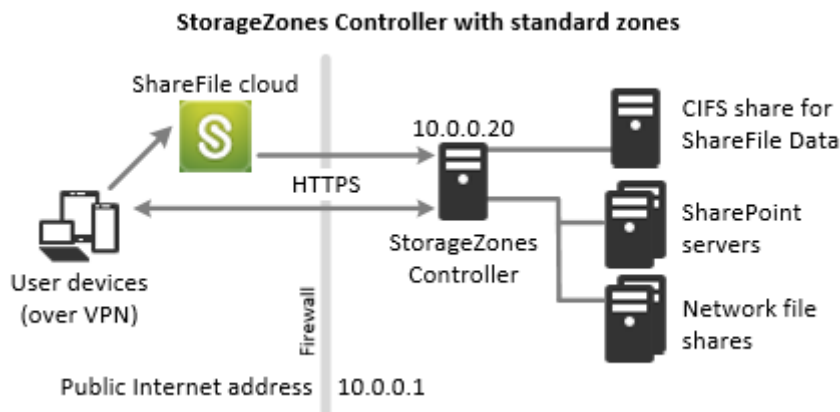
A proof-of-concept deployment is intended for evaluation purposes only and should not be used for critical data storage.

A proof-of-concept deployment uses a single storage zones controller. The example deployment discussed in this section has both storage zones for ShareFile Data and storage zone connectors enabled.

To evaluate a single storage zones controller, you can optionally store data in a folder (such as C:\ZoneFiles) on the hard drive of the storage zones controller instead of on a separate network share. All other system requirements apply to an evaluation deployment.

### Proof-of-concept deployment for standard storage zones

A storage zones controller configured for standard zones must accept in-bound connections from the ShareFile cloud. To do that the controller must have a publicly accessible internet address and SSL enabled for communications with the ShareFile cloud. The following figure indicates the traffic flow between user devices, the ShareFile cloud, and storage zones controller.



In this scenario, one firewall stands between the Internet and the secure network. Storage zones controller resides inside the firewall to control access. User connections to ShareFile must traverse the firewall and use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall and install a public SSL certificate on the IIS service of the storage zones controller.

### Storage zones controller high availability deployment

For a production deployment of ShareFile with high-availability, the recommended best practice is to install at least two storage zones controllers. When you install the first controller, you create a storage zone. When you install the other controllers, you join them to the same zone. Storage zones controllers that belong to the same zone must use the same file share for storage.

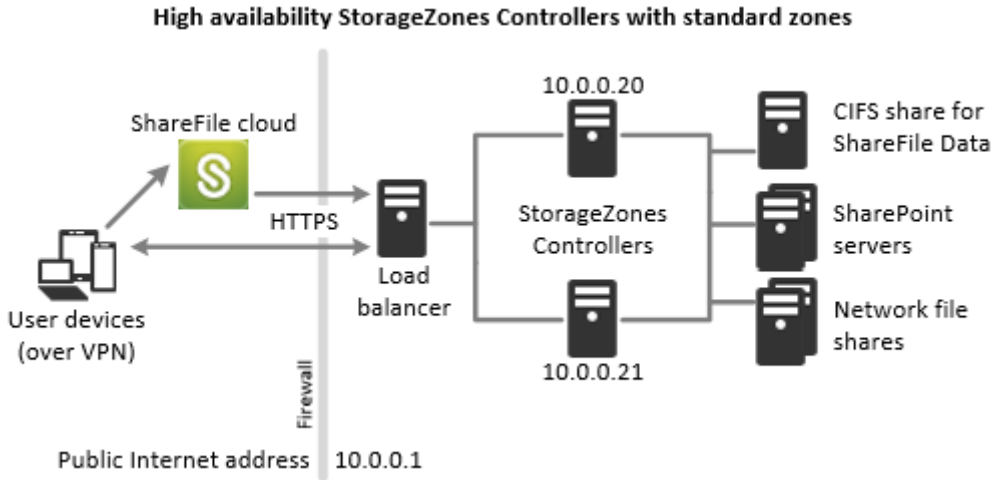
In a high availability deployment the secondary servers are independent, fully functioning storage zones controllers. The storage zones control subsystem randomly chooses a storage zones controller for operations. If the primary server goes offline, you can easily promote a secondary server to primary. You can also demote a server from primary to secondary.

### High availability deployment for standard zones

Storage zones controllers configured for standard storage zones must accept in-bound connections from the ShareFile cloud. To do that each controller must have a publicly accessible internet address and SSL enabled for communications with the ShareFile cloud. You can configure multiple external



public addresses, each associated with a different storage zones controller. The following figure shows a high availability deployment for standard storage zones.



Similar to the Proof-of-concept deployment scenario above, one firewall stands between the Internet and the secure network. The storage zones controllers reside inside the firewall to control access. User connections to ShareFile must traverse the firewall and use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall and install a public SSL certificate on the IIS service of all storage zones controllers.

**Shared storage configuration**

Storage zones controllers that belong to the same storage zone must use the same file share for storage. Storage zones controllers access the share using the IIS Account Pool user. By default, application pools operate under the Network Service user account, which has low-level user rights. A storage zones controller uses the Network Service account by default.

You can use a named user account instead of the Network Service account to access the share. To use a named user account, specify the user name and password in the storage zones console Configuration page. Run the IIS application pool and the Citrix ShareFile Services using the Network Service account.

**Network connections**

Network connections vary based on the type of zone —Citrix-managed or standard.

**Citrix-managed zones** The following table describes the network connections that occur when a user logs on to ShareFile and then downloads a document from a Citrix-managed zone. All connections use HTTPS.

Step	Source	Destination
1. User logon request	Client	<a href="#">company.sharefile.com:443</a>
1. (Optional) Redirect to SAML IdP logon	Client	SAML Identity Provider URL
1. File/folder enumeration and download request	Client	<a href="#">company.sharefile.com:443</a>
1. File download	Client	<a href="#">storage-location.sharefile.com:443</a>

**Standard storage zones** The following table describes the network connections that occur when a user logs on to ShareFile and then downloads a document from a standard storage zone. All connections use HTTPS.

Step	Source	Destination
1. User logon request	Client	<a href="#">company.sharefile.com</a>
1. (Optional) If using ADFS, redirect to SAML IdP logon	Client	SAML Identity Provider URL
1. File/folder enumeration and download request	Client	<a href="#">company.sharefile.com</a>
1. File download authorization	<a href="#">company.sharefile.com</a>	<a href="#">szc.company.com</a>
1. File download	Client	<a href="#">szc.company.com</a>

## Storage zones controller DMZ proxy deployment

A demilitarized zone (DMZ) provides an extra layer of security for the internal network. A DMZ proxy, such as Citrix ADC VPX, is an optional component used to:

- Ensure all requests to a storage zones controller originate from the ShareFile cloud, so that only approved traffic reaches the storage zones controllers.

storage zones controller has a validate operation that checks for valid URI signatures for all incoming messages. The DMZ component is responsible for validating signatures before forwarding messages.

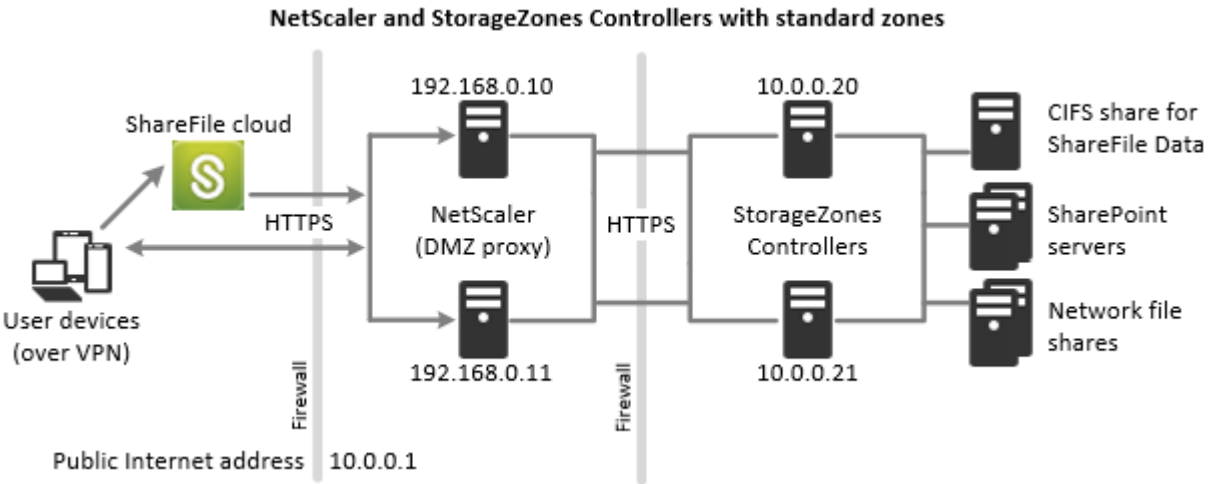
- Load balance requests to storage zones controllers using real-time status indicators.

Operations can be load-balanced to storage zones controllers if they all can access the same files.

- Offload SSL from storage zones controllers.
- Ensure requests for files on SharePoint or network drives are authenticated before passing through the DMZ.

**Citrix ADC and storage zones controller deployment**

**Deployment for standard storage zones** Storage zones controllers configured for standard zones must accept in-bound connections from the ShareFile cloud. To do that the Citrix ADC must have a publicly accessible internet address and SSL enabled for communications with the ShareFile cloud.

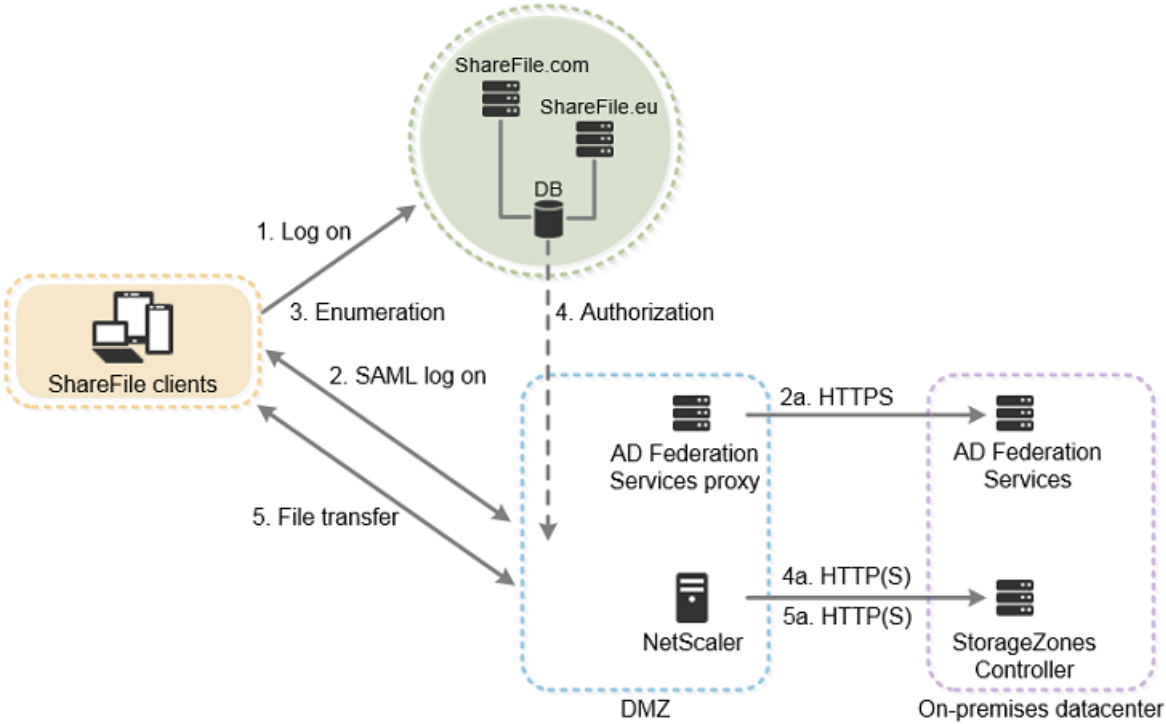


In this scenario, two firewalls stand between the Internet and the secure network. Storage zones controllers reside in the internal network. User connections to ShareFile must traverse the first firewall and use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall and install a public SSL certificate on the IIS service of the DMZ proxy servers (if they terminate the user connection).

**Network connections for standard zones**

The following diagram and table describe the network connections that occur when a user logs on to ShareFile and then downloads a document from a standard zone deployed behind Citrix ADC. In this case, the account uses Active Directory Federation Services (ADFS) for SAML logon.

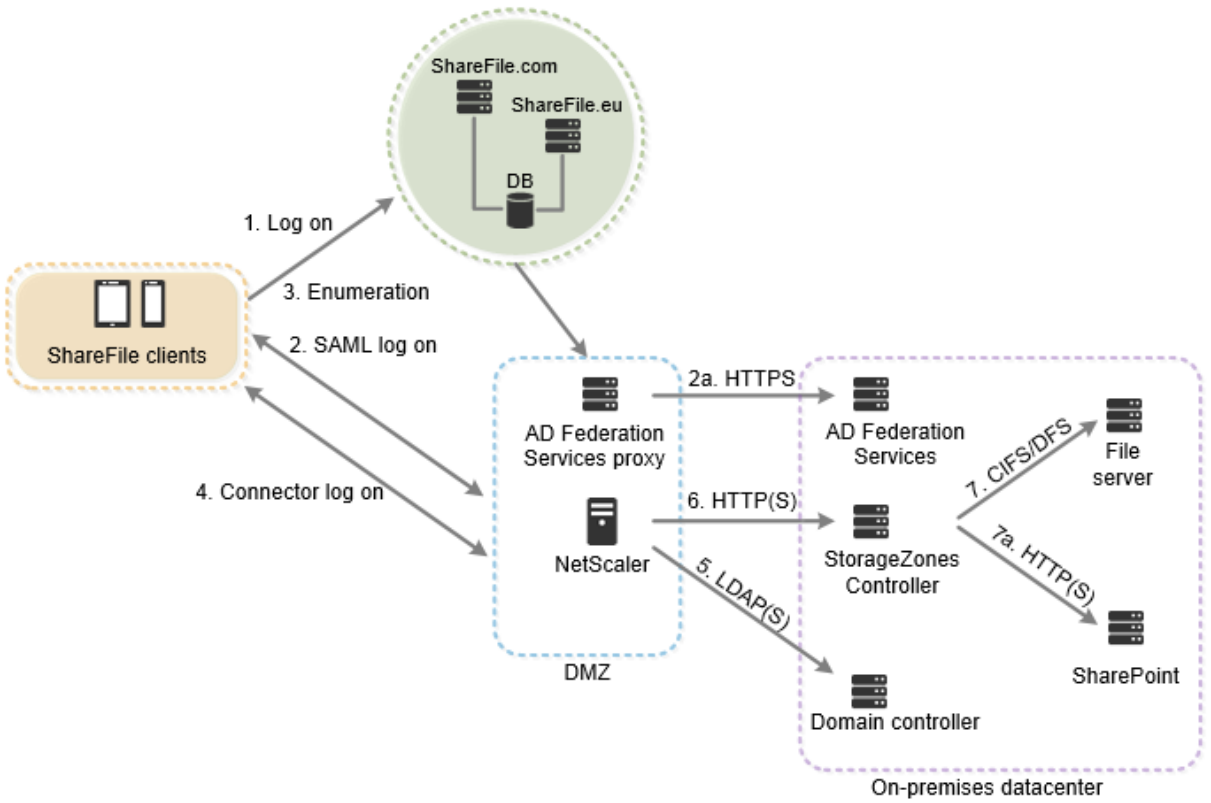
Authentication traffic is handled in the DMZ by an ADFS proxy server that communicates with an ADFS server on the trusted network. File activity is accessed via Citrix ADC in the DMZ, which terminates SSL, authenticates user requests and then accesses the storage zones controller in the trusted network on behalf of authenticated users. The Citrix ADC external address for ShareFile is accessed using the Internet FQDN szc.company.com.



Step	Source	Destination	Protocol
1. User logon request	Client	company.sharefile.com	HTTPS
1. (Optional) Redirect to SAML IdP logon	Client	SAML Identity Provider URL	HTTPS
2a. ADFS logon	ADFS proxy	ADFS server	HTTPS
1. File/folder enumeration and download request	Client	company.sharefile.com	HTTPS
1. File download authorization	ShareFile	szc.company.com (external address)	HTTP(S)

Step	Source	Destination	Protocol
4a. File download authorization	Citrix ADC IP (NSIP)	storage zones controller	HTTPS
1. File download	Client	<a href="#">szc.company.com</a> (external address)	HTTPS
5a. File download	Citrix ADC IP (NSIP)	storage zones controller	HTTP(S)

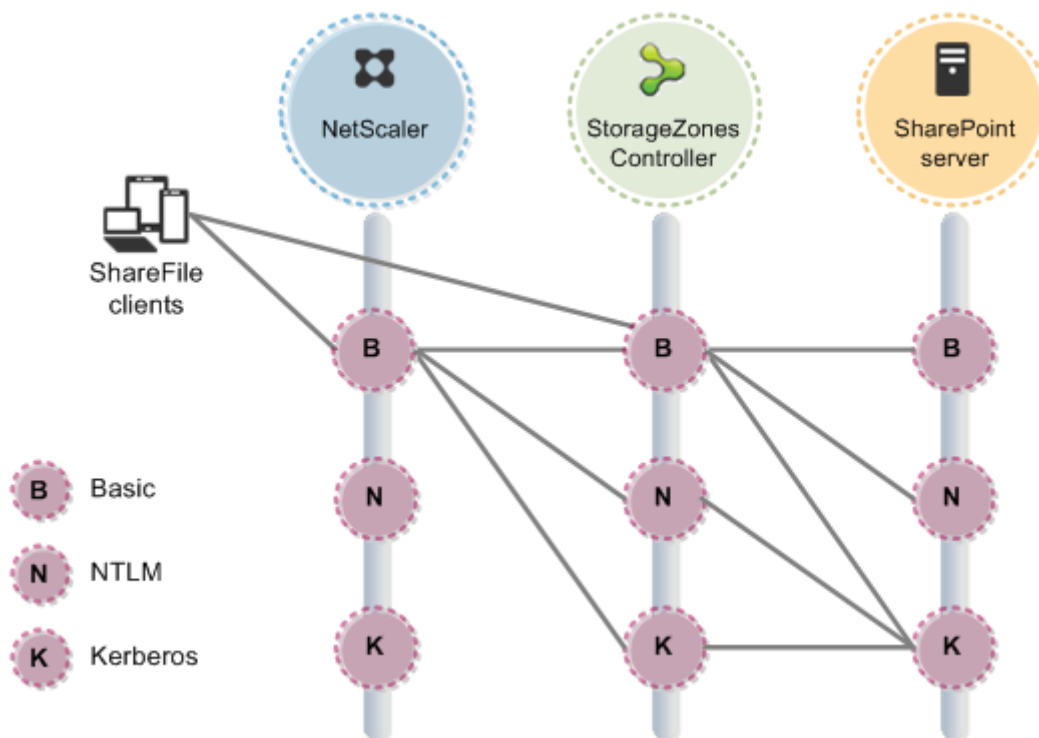
The following diagram and table extend the previous scenario to show the network connections for StorageZone Connectors. This scenario includes use of NetScaler in the DMZ to terminate SSL and perform user authentication for Connectors access.



Step	Source	Destination	Protocol
1. User logon request	Client	<a href="#">company.sharefile.com</a>	HTTPS

Step	Source	Destination	Protocol
1. (Optional) Redirect to SAML IdP logon	Client	SAML Identity Provider URL	HTTPS
2a. ADFS logon	ADFS proxy	ADFS server	HTTPS
1. Top-level connector enumeration	Client	<a href="#">company.sharefile.com</a>	HTTPS
1. User log on to storage zones controller server	Client	<a href="#">szc.company.com</a> (external address)	HTTPS
1. User authentication	Citrix ADC IP (NSIP)	AD Domain controller	LDAP(S)
1. File/folder enumeration and upload/- download requests	Citrix ADC IP (NSIP)	storage zones controller	HTTP(S)
1. Network share enumeration and upload/- download	Storage zones controller	File server	CIFS or DFS
7a. SharePoint enumeration and upload/download	Storage zones controller	SharePoint	HTTP(S)

The following diagram summarizes the supported combinations of authentication types based on whether the user authenticates.



## System requirements

September 22, 2023

### Important:

Microsoft is ending support for Windows Server 2012R2 on October 10, 2023. It is important to migrate your server to a newer version before the end of support date.

### Storage zones controller

- A dedicated physical or virtual machine with 2 CPUs and 4 GB RAM
- Windows Server 2012 R2 (Datacenter, Standard, or Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

#### For standard storage zones:

- Use a publicly resolvable Internet host name (not an IP address).
- Enable SSL for communications with ShareFile.

- The SSL certificate on the storage zones controller must be trusted by user devices and ShareFile web servers. If you use SSL directly with IIS, refer to <http://support.microsoft.com/kb/298805> for information about configuring SSL.
- Allow inbound TCP requests on port 443 through your firewall.
- Allow outbound TCP requests to the ShareFile control plane on port 443 through your firewall.
  - [Click here for a detailed list of IP ranges and domains.](#)

**For the server health check used only for storage zones for ShareFile Data:**

- Open port 80 on the localhost.

**For a high availability production environment:**

- A minimum of two servers with storage zones controller installed.
- If you are not using DMZ proxy servers, install an SSL certificate on the IIS service.

For information about supported certificates, see the certificate requirements for standard zones above.

**For a DMZ proxy deployment:**

- One or more DMZ proxy servers, such as Citrix ADC VPX instances.
- For a DMZ proxy server that terminates the client connection and uses HTTP, install an SSL certificate on the proxy server.

If communications between the DMZ proxy server and the storage zones controller are secure, you can use HTTP. However, HTTPS is recommended as a best practice. If you use HTTPS, you can use a private (Enterprise) certificate on the storage zones controller if it is trusted by the DMZ proxy. The external address exposed by the DMZ proxy must use a commercially trusted certificate. For information about supported certificates, see the certificate requirements for standard zones above.

**Other requirements**

**Note:**

ShareFile does not officially support and does not recommend utilizing DFS replication. It has been known to cause locking failures for larger files. If DFS replication must be used, use separate backup solutions during off-peak hours when the zone is not actively in use.

- The storage zones controller installer requires administrative privileges.
- For remote administration of storage zones controller, use a remoting protocol, such as RDP or Citrix ICA, to connect to the server and then open the storage zones controller console.



### Supported third-party storage systems

- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure

### Supported Data Loss Prevention solutions

- Storage zones controller integrates with any ICAP-compliant DLP solution, including:
  - Symantec Data Loss Prevention
  - McAfee DLP Prevent
  - Websense TRITON AP-DATA
  - RSA Data Loss Prevention

### Storage zones for ShareFile Data

Storage zones for ShareFile Data is an optional feature that you enable on a storage zones controller.

Requirements:

- ShareFile Enterprise account, with the storage zone feature enabled
- A ShareFile user account that includes permission to create and manage zones
- A CIFS share for private data storage

If you plan to store ShareFile files in a supported third-party storage system, the CIFS share is used for temporary files (encryption keys, queued files) and as a temporary storage cache.

- The Web Server (IIS) role and ASP.NET 4.x. For more information, see [Prepare your server for ShareFile data](#).

Note: Access to a ShareFile account from an FTP client is not compatible with storage zones for ShareFile Data.

### Storage zone connector for SharePoint

Storage zone connector for SharePoint is an optional feature that you enable on a storage zones controller.

Requirements:

- ShareFile Enterprise account, with the storage zone feature enabled, or Citrix Endpoint Management.
- Only **Microsoft SharePoint Server 2010 and newer** are supported.

- The storage zones controller server must be a domain member, in the same forest as the SharePoint server.
- The Web Server (IIS) role and ASP.NET 4.x. For more information, see [Prepare your server for ShareFile data](#).
- SharePoint policies:
  - The default maximum upload file size for a Web application in SharePoint 2013 is 250 MB and in SharePoint 2010 is 50 MB. To change the default: In SharePoint Central Administration, go to the Web Application General Settings page and change the Maximum Upload Size. The upload file size limit for SharePoint is 2 GB.
  - ShareFile clients always attempt to check in a major version (publish) of a file. However, SharePoint policies determine whether a file is checked in as a major or minor version.
  - The SharePoint View-Only permission does not enable a user to download files. To read a file from a ShareFile client, a SharePoint user must have Read permission.
- User devices: For the latest information about user device support for storage zone connectors, refer to the [ShareFile Knowledge Base](#).

### **Storage zone connector for SharePoint authentication**

After authenticating the user, the storage zones controller server makes connections to the SharePoint server on the authenticated user's behalf and responds to authentication challenges presented by the SharePoint server. Storage zone connector for SharePoint supports the following authentication methods on the SharePoint server.

- Basic

Requires that you add `<add key="CacheCredentials" value="1">` to `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.
- Negotiate (Kerberos)
- Windows Challenge/Response (NTLM)

ShareFile mobile clients use Basic authentication over HTTPS to authenticate to the storage zones controller or DMZ proxy. Single sign-on to SharePoint is governed by the authentication requirements set on the SharePoint server. To use Kerberos or NTLM authentication on the SharePoint server: [Configure the domain controller to trust the storage zones controller for delegation](#).

If your SharePoint server is configured for Kerberos authentication: Configure a service principal name (SPN) for the named user service accounts for the SharePoint server application pool. For more information, see "Configure trust for delegation for Web parts" in <http://support.microsoft.com/kb/832769>.

For deployments with Citrix ADC, it is possible to terminate basic authentication at the Citrix ADC and then perform other types of authentication to the storage zones controller.

## **Storage zone connector for Network File Shares**

Storage zone connector for Network File Shares is an optional feature that you enable on a storage zones controller.

Requirements:

- ShareFile Enterprise or Citrix Endpoint Management account.
- The storage zone connector server must be a domain member, in the same forest as the network file servers.
- The Web Server (IIS) role and ASP.NET 4.x. For more information, see [Prepare your server for ShareFile data](#).
- User devices: For the latest information about user device support for storage zone connectors, see the [ShareFile Knowledge Base](#).

## **Connector for Network File Shares authentication**

After authenticating the user, the storage zones controller server makes connections to the network file server on the authenticated user's behalf and responds to authentication challenges presented by the file server. Storage zone connector for Network File Shares supports the following authentication methods on the file server.

- Negotiate (Kerberos)
- Windows Challenge/Response (NTLM)

To use Kerberos or NTLM authentication on the storage zones controller: [Configure the domain controller to trust the storage zones controller for delegation](#).

For deployments with Citrix ADC: To provide users with a single sign-on experience when Citrix ADC is configured for basic authentication, configure the connector for both Negotiate (Kerberos) and NTLM authentication.

## **PowerShell scripts and commands**

The storage zones controller installation includes several PowerShell scripts and commands, located in `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\`.

- Run the scripts in the 32-bit (x86) version of PowerShell.

- For best results, upgrade to PowerShell 4.0 or later, included with [Windows Management Framework](#).

PowerShell 2.0 causes significant problems due to compatibility issues with .NET Framework 4.

## Install

August 29, 2019

Complete the following tasks, in the order presented, to install and set up storage zones controller, storage zones for ShareFile Data, and storage zones connectors.

1. [Configure Citrix ADC for storage zones controller](#)

You can use Citrix ADC as a DMZ proxy for storage zones controller.

2. [Create a network share for private data storage](#)

Storage zones for ShareFile Data requires a network share for your private data, even if you store ShareFile files in a supported third-party storage system.

3. [Install an SSL certificate](#)

A storage zones controller that hosts standard zones requires an SSL certificate.

4. [Prepare your server for ShareFile data](#)

IIS and ASP.NET setup is required for storage zones for ShareFile data and for storage zone connectors.

5. [Install storage zones controller and create a storage zone](#)

6. [Verify your storage zones controller setup](#)

7. [Change the default zone for user accounts](#)

By default, existing and newly provisioned user accounts use the ShareFile-managed cloud storage as the default zone.

8. [Specify a proxy server for storage zones](#)

The storage zones controllers console enables you to specify a proxy server for storage zones controllers. You can also specify a proxy server using other methods.

9. [Configure the domain controller to trust the storage zones controller for delegation](#)

Configure the domain controller to support NTLM or Kerberos authentication on network shares or SharePoint sites.

#### 10. [Join a secondary storage zones controller to a storage zone](#)

To configure a storage zone for high availability, connect at least two storage zones controllers to it.

For a demonstration of configuring storage zones controller with Microsoft Azure Storage, [click here](#).

For a demonstration of configuring ShareFile Enterprise to use a Microsoft Azure storage zone, [click here](#).

### Additional setup instructions

- [Configure multitenant storage zones](#)
- [Configure storage zones controller for Web App Previews, Thumbnails, and View-Only Sharing](#)

## Configure Citrix ADC for storage zones controller

September 1, 2021

NetScaler, version 10.1 build 120.1316.e and later, includes a wizard that prompts you for basic information about your storage zones controller environment. Then it generates a configuration that:

- Load balances traffic across storage zones controllers
- Provides user authentication for storage zone connectors
- Validates URI signatures for ShareFile uploads and downloads
- Terminates SSL connections at the Citrix ADC appliance

The diagram shows these Citrix ADC components created by the configuration:

- **Citrix ADC content switching virtual server** — Sends user requests for data from ShareFile and from storage zone connectors to the appropriate Citrix ADC load balancing virtual server.
- **Citrix ADC load balancing virtual server** — Load balances the traffic for your storage zones controllers and also handles the following:
  - For requests for data from your private data storage, a load balancing virtual server performs hash validation, to ensure valid URI signatures are present on incoming requests.
  - For requests for data from storage zone connectors, a load balancing virtual server can perform user authentication. It stops a user request at the Citrix ADC, authenticates the user, and then performs single sign-on of the user to storage zones controller.

**Note:**

Authentication to storage zone connectors through Citrix ADC is optional. Due to a known issue, if authentication is enabled in Citrix ADC, storage zone connectors in WebApp do not work in Chrome, Chromium, Safari, and Edge browsers. It is compatible with other browsers and desktop/mobile clients.

As of storage zones controller 4.0, administrators can limit inbound connections to the storage zones controllers to TLS v1.2. If protocols earlier than TLS v1.2 are disabled for inbound traffic to the storage zone controller, all client software components that interact with the storage zone must also support TLS v1.2. [Click here for additional information and configuration instructions.](#)

**Note:**

To set up NetScaler versions before 10.1 build 120.1316.e, see [Configure Citrix ADC manually](#).

The setup of Citrix ADC for ShareFile wizard does not handle the configuration required to use Citrix Endpoint Management as a SAML identity provider for ShareFile. For more information, [click here](#).

## Prerequisites

- A working Citrix ADC configuration
- Security certificate: If one is not already available in Citrix ADC, the wizard enables you to install one on the content switching virtual server.
- Information about your Active Directory configuration (**The Citrix ADC for ShareFile Wizard must be completed with the Citrix NetScaler Enterprise Edition License**):
  - IP address and port of your Active Directory server
  - Active Directory domain name
  - LDAP Base DN where users are stored
  - Account name and password for an administrator account that has permissions to communicate with Active Directory

## Configure Citrix ADC for storage zones controllers

The following steps describe how to use the Citrix ADC for ShareFile wizard.

1. Log on to the Citrix ADC appliance and, on the Configuration tab, navigate to Traffic Management.

2. Under Citrix ShareFile, click Set up Citrix ADC for ShareFile.

You can also access the wizard as follows: Under Mobility, click **Configure Endpoint Management, ShareFile, and Citrix Gateway**.

3. Supply the information requested in the wizard.

---

Option	Description
Name	A display name for the content switching virtual server.
IP Address	The external (public or DMZ) IP address to be used for the content switching virtual server. If you use a DMZ IP address, you must define a Network Address Translation (NAT) mapping from your external firewall address to this DMZ IP address.
ShareFile Data	This option is enabled, indicating that you will use the Citrix ADC connection for storage zones for ShareFile Data.
storage zone connectors for Network File Share/SharePoint	If you use connectors and you want to perform user authentication at the Citrix ADC, select the check box.
Certificate	Choose a certificate or install one for the content switching virtual server. If you choose to install a certificate, you are prompted to upload the certificate and private key. For standard zones, certificates must be publicly trusted and not self-signed.
storage zones controller IP Address	The internal IP addresses for one or more storage zones controller servers. These IP addresses define the storage zones controller servers as entities inside Citrix ADC. If you already added the servers to Citrix ADC, click Add From Existing and select the servers. To use Citrix ADC for load balancing, enter an internal IP address for each storage zones controller server. To use Citrix ADC only for SSL and authentication, enter just one IP address.
Port and Protocol	The port and protocol used for communication from the Citrix ADC to storage zones controllers.

Option	Description
The authentication, authorization, and auditing (Citrix ADC AAA) virtual server IP Address	An unused internal IP address for the Citrix ADC AAA virtual server. Citrix ADC creates this virtual server for its own use. The server does not require outside access.
LDAP Server IP Address and Port	The IP address and port of your Active Directory server. If you already added an LDAP server to Citrix ADC, click the Choose LDAP tab and choose the server.
Time out	The maximum number of seconds that the Citrix ADC waits for a response from the LDAP server. Defaults to 3 seconds. The minimum value is 1 second.
Single Sign-on Domain	The Active Directory domain name.
Base DN (location of users)	The LDAP Base Distinguished Name (DN) where users are stored. Specify the DN using the general form: CN=Users,dc=domain, dc=Net
Administrator Bind DN and Password	An administrator account that has permissions to communicate with Active Directory.
Logon Name	An LDAP attribute, used by Citrix ADC to determine whether users log on with their user name or email address. Defaults to sAMAccountName, which enables users to log on with their user names. To require users to enter their email address to log on, change this field to userPrincipalName.

## Configure Citrix ADC for web access to connectors

To support web access to storage zone connectors, you must perform additional Citrix ADC configuration after you complete the Citrix ADC for ShareFile wizard.

- Create and configure a third Citrix ADC load-balancing virtual server, used to ensure that ShareFile clients send credentials only when logged on to a trusted ShareFile domain.

As described in the following steps, you will configure the additional virtual server to allow anonymous access from clients for the HTTP OPTIONS verb. The OPTIONS request passes through to storage zones controller without being authenticated and without HTTPS callouts



to validate the signature. The CORS preflight check validates domain trust before sending credentials.

An understanding of CORS is not needed to perform the configuration. However, for more information about CORS, see <http://enable-cors.org/>.

- To support web access to storage zone connectors, add a path (/ProxyService) to the content switching policy used for traffic to /cifs and /sp.

Perform the following steps in Citrix ADC after you complete the Citrix ADC for ShareFile wizard.

1. Create a third load-balancing virtual server:

- a) Navigate to **Traffic Management > Load Balancing > Virtual Servers**.
- b) Click Add.
- c) Specify the following values:

Option	Value
Name	A policy name, such as SF_ZONE_OPTIONS
Protocol	SSL
IP Address Type	Non Addressable

- d) Click through to create the virtual server.
- e) To bind the same services to it as the load-balancing virtual servers created by the wizard:  
In the Load Balancing Virtual Server screen, across from Service, click > and then click Save.
- f) Add a certificate to the virtual server.

2. Create a policy for the virtual server you just added:

- a) Navigate to **Traffic Management > Content Switching > Policies**.
- b) In the details pane, click Add and then specify the Name, Target LB Virtual Server, and Expression values. Click **Expression Editor** and then build this expression. Select **HTTP**. Select **REQ**. Select **METHOD**. Select EQ(String) and type OPTIONS. The expression should read as follows: `HTTP.REQ.METHOD.EQ("OPTIONS")`
- c) Click **Done**.
- d) Click **Create**.

3. Bind the policy you just created to the new load-balancing virtual server:

- a) Navigate to **Traffic Management > Content Switching > Virtual Servers**.

- b) In the list, click the virtual server and click **Edit**.
  - c) Navigate to the section of Content Switching Policy Binding and click 2 Content Switching Policies.
  - d) Click **Add Binding**.
  - e) Select the new Content Policy and select the Target Load Balancing Virtual Server.
  - f) Click **Bind**.
  - g) Click **Edit Binding** and update the **Priority**. Change the priority of the new policy so it has the lowest number of the three policies.  
The policy with the lowest value has the highest priority and so is handled first.
4. Update the policy used for traffic to storage zone connectors (\_SF\_CIF\_SP\_CSPOL):
- a) Navigate to **Traffic Management > Content Switching > Policies**.
  - b) Select the \_SF\_CIF\_SP\_CSPOL policy.
  - c) Add the following to the policy expression:

```
1 || HTTP.REQ.URL.CONTAINS("/ProxyService/")
2 <!--NeedCopy-->
```

The full policy expression should be as follows:

```
1 HTTP.REQ.URL.CONTAINS("/cifs/") || HTTP.REQ.URL.CONTAINS("/sp/
  ") ||
2 HTTP.REQ.URL.CONTAINS("/ProxyService/")
3 <!--NeedCopy-->
```

5. Update the policy used for traffic to storage zones for ShareFile Data (\_SF\_SZ\_CSPOL):
- a) Navigate to **Traffic Management > Content Switching > Policies**.
  - b) Select the \_SF\_SZ\_CSPOL policy.
  - c) Add the following to the policy expression:

```
1 && HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT
2 <!--NeedCopy-->
```

The full policy expression should be as follows:

```
1 HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("
  /sp/ ").NOT
2 && HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT
3 <!--NeedCopy-->
```

## Configure Citrix ADC for view-only sharing

To support the view-only sharing, users must be able to access your Microsoft Office Web Apps Server (OWA). If your OWA server is externally accessible on its own address, no additional Citrix ADC config-

uration should be required for your storage zones controller.

If you want to combine the storage zones controller and Office Web App Server onto a single external address using Citrix ADC content switching policies, you must perform additional Citrix ADC configuration after you complete the Citrix ADC for ShareFile wizard. Citrix ADC configuration is required to ensure that traffic is routed to your externally accessible OWA Server properly.

Once the following Citrix ADC rules are configured, Administrators can reuse the existing External address of their storage zones controller zone, eliminating the need to create an additional external address for OWA.

To create and configure an additional Citrix ADC load-balancing virtual server:

1. Create an additional load-balancing service.
  - Navigate to **Traffic Management > Load Balancing > Services**.
  - Click **Add**.
  - Enter the required information to create a service that corresponds to your OWA server(s). Click **OK**.
2. Create an additional load-balancing virtual server:
  - Navigate to **Traffic Management > Load Balancing > Virtual Servers**.
  - Click **Add**.
  - Specify the following values:

Option	Value
Name	A policy name, such as SF_OWA_vServer
Protocol	SSL
IP Address Type	Non Addressable

- Click through to create the virtual server.
  - To bind the virtual server to the OWA service you created in the previous step, click **Load Balancing Virtual Service Binding > Select Service**. Click the check box beside the service you created in the previous step.
  - Click **Select**.
  - Click **Bind**.
3. Create a new policy used to route traffic to your OWA server.
    - Navigate to **Traffic Management > Content Switching > Policies**.
    - Select **Add**.

- Name the policy.
- Add the following expression:
  - HTTP.REQ.URL.CONTAINS("/hosting/discovery")  
|| HTTP.REQ.URL.CONTAINS("/x/")  
|| HTTP.REQ.URL.CONTAINS("/wv/")  
|| HTTP.REQ.URL.CONTAINS("/p/")The full policy expression should be as follows:  
HTTP.REQ.URL.CONTAINS("/hosting/discovery")  
|| HTTP.REQ.URL.CONTAINS("/x/")  
|| HTTP.REQ.URL.CONTAINS("/wv/")  
|| HTTP.REQ.URL.CONTAINS("/p/")

4. Update the priority of the new policy within the load-balancing virtual
- Navigate to **Traffic Management > Content Switching > Virtual Servers**.
  - Click the load-balancing virtual server, then select Content Switching Policies.
  - Change the priority of the policies so that the (Example) “\_SF\_OWA” policy is third in priority.

Priority	Policy Name
90	SF_ZK_OPTIONS
95	_SF_CIF_SP_SPOL
99	_SF_OWA
100	_SF_SZ_CSPOL

- Click **Close**. Click **Done**

### Create a monitor for the storage zones controller service

By default, Citrix ADC pings the storage zones controller server to determine if it is online. However, even if the controller is online, it might not be able to send heartbeat messages to the ShareFile website. In that case, Citrix ADC will send traffic to storage zones controller although it is not communicating with ShareFile.

To verify storage zones controller outbound connectivity to ShareFile, you can create a monitor that checks heartbeat.aspx and bind it to the Citrix ADC service for each storage zones controller.

```
1 add lb monitor SZC_Heartbeat HTTP-ECV -send "GET /heartbeat.aspx" -  
   recv "***ONLINE*** " -secure YES  
2 bind service StorageZone_Svc -monitorName SZC_Heartbeat  
3 <!--NeedCopy-->
```

StorageZone\_Svc is the Citrix ADC service that corresponds to a storage zones controller. That service name is automatically created by the Citrix ADC for ShareFile wizard. The service name includes the IP address of the controller, such as SF\_SVC\_ip-address.

-secure YES is required if the service is listening on port 443.

## Verify the Citrix ADC configuration

After you complete the wizard, go to **Traffic Management > Load Balancing > Virtual Servers** to view the status of the load balancing virtual servers created by the wizard.

## View the throughput of ShareFile requests through Citrix ADC

Throughput statistics can be found on the **Dashboard** menu.

## Configure Citrix ADC manually

November 4, 2022

As of version 10.1 build 120.1316, NetScaler includes a wizard that configures the settings needed for the storage zone controller data and connectors.

The steps in this section describe the **Citrix ADC** settings needed for the storage zone controller. All links are for the NetScaler 10.1 documentation. Similar topics are available for later versions of Citrix ADC.

## To check for valid URI signatures on all incoming messages

1. Create an HTTP callout named sf\_callout:
  - a) In the Configure HTTP Callout dialog box, click **Virtual Server or IP Address** and specify the address.
  - b) Under Request to send to the server, click **Attribute-based** and then click **Configure Request Attributes**.
  - c) Select **Get Method**.
  - d) In Host Expression enter the virtual server IP address or the host IP address for any of the storage zones controllers.
  - e) In the URL Stem Expression, enter:

```
1  "/validate.ashx?RequestURI=" + HTTP.REQ.URL.BEFORE\_STR("&h")  
    .HTTP\_URL\_SAFE.B64ENCODE + "&h=" + HTTP.REQ.URL.QUERY.  
    VALUE("h")  
2  <!--NeedCopy-->
```

- f) Click **OK** and then return to the Configure HTTP Callout dialog box.
  - g) Under Server Response, choose a Return Type of Bool.
  - h) In the Expression to extract data from the response, enter:  
`HTTP.RES.STATUS.EQ(200).NOT`
  - i) Click **Create**.
2. Follow the preceding steps to configure an HTTP callout named sf\_callout\_y. Use the same settings except for the expression:

- In the URL Stem Expression, enter:

```
1  "/validate.ashx?RequestURI=" + HTTP.REQ.URL.HTTP\_URL\_SAFE.  
    B64ENCODE + "&h=" +  
2  <!--NeedCopy-->
```

3. Configure a responder policy:

- a) In the Configure Responder Policy dialog box: For Action, choose Drop.
- b) Enter the expression:

```
1  http.REQ.URL.CONTAINS("&h=") && http.req.url.contains("/  
    crossdomain.xml").not && http.req.url.contains("/validate.  
    ashx?requi").not && SYS.HTTP\_CALLOUT(sf\_callout) || http  
    .REQ.URL.CONTAINS("&h=").NOT && http.req.url.contains("/  
    crossdomain.xml").not && http.req.url.contains("/validate.  
    ashx?requi").not && SYS.HTTP\_CALLOUT(sf\_callout\_y)  
2  <!--NeedCopy-->
```

For more information, see [Responder](#).

4. [Bind the responder policy to the load balancer virtual server](#) and configure [SSL session-based persistence](#).

## To load balance

1. [Configure token-based load balancing](#).

Use the rule expression: “`http.REQ.URL.QUERY.VALUE("uploadid")`”

Token-based load balancing is required for storage zones controllers in a high availability deployment. Round-robin load balancing results in intermittent download or upload failures because a client request for an upload or download can get directed to a storage zone controller other than the one that received the authorization request from ShareFile.com.

2. Configure Citrix ADC to terminate SSL connections.

For information, see [Configuring SSL Offloading](#).

## To configure content switching and authentication for Connectors

1. To enable content switching, see [Enabling Content Switching](#).
2. Create a content switching policy for user requests for ShareFile data from your on-premises storage zones:

- a) In the Configure Content Switching Policy dialog box, enter a name for the content switching policy. These steps use the name Data\_Requests.
- b) Enter the expression:

```
1 HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerHostName")  
  && HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.  
  CONTAINS("/sp/").NOT  
2 <!--NeedCopy-->
```

- c) Click **OK**.

For more information, see [Content Switching](#).

3. Create a content switching policy for user requests for data accessed from storage zone connectors.

- a) In the Configure Content Switching Policy dialog box, specify a name for the content switching policy. These steps use the name Connector\_Requests.
- b) Enter the expression:

```
1 HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerFQDN") && (  
  HTTP.REQ.URL.CONTAINS("/cifs/") || HTTP.REQ.URL.CONTAINS("/  
  sp/"))  
2 <!--NeedCopy-->
```

Be sure to replace "StorageZonesControllerFQDN" with the FQDN of your controller.

- c) Click **OK**.

4. [Create a content switching virtual server](#).

5. Set the content switching policy targets:

- In the Configure Virtual Server (Content Switching) dialog box, for the Data\_Requests policy, specify the load balancer virtual server for storage zones for ShareFile data.

This load balancer virtual server is the one to bound the responder policy in Step 4 to check for valid URI signatures on all incoming messages and to load balance.

- For the Connector\_Requests policy, specify the load balancer virtual server for storage zone connectors.

6. Configure the authentication virtual server for the storage zone controller:

Although authentication to Citrix ADC is optional, it is a recommended best practice.

- a) In the navigation pane, expand Load Balancing, select the name of the load balancer virtual server for storage zones connectors, and then click Open.
- b) In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab and then expand Authentication Settings.
- c) Select the check box for 401 Based Authentication and then choose the Authentication virtual server.
- d) Click the **Method and Persistence** tab.
- e) For Persistence, choose **COOKIEINSERT**.
- f) For Time-out (min), enter **240**.

A time-out value of 240 minutes is recommended. Use a minimum value greater than 10 minutes.

For more information, see [Configuring the Authentication Virtual Server](#).

7. Use the Configure Authentication Server dialog box to create and configure an authentication server.

In SSO Name Attribute, enter **userPrincipalName**.

For more information about other settings, see [Authentication Policies](#).

8. Configure an authentication policy for the authentication server:

- a) In the Configure Authentication Policy dialog box: Enter a Name for the policy and then select the authentication Server configured in the previous step.
- b) Enter the expression:

`ns_true`

For more information, see [Configure an authentication policy](#).

9. Configure a session profile for single sign-on:

- a) In the Configure Session Profile dialog box, enter a name for the profile.
- b) Select the check box for single sign-on to Web Applications.
- c) For Credential Index, select **PRIMARY**.
- d) In the single sign-on domain, enter the domain name for your storage zones controller.



- e) Select the **Override Global** check boxes for each of the preceding three items.

For more information, see [Session Profiles](#).

10. Configure a session policy for single sign-on:

- a) In the Configure Session Policy dialog box, enter a name for the policy.
- b) For Request Profile, select the name of the session profile configured in the previous step.
- c) Enter the expression:

`ns_true`

For more information, see [Session Policies](#).

11. Create an authentication virtual server:

- a) In the Configure Virtual Server (Authentication) dialog box, enter a name and the IP Address for the server.
- b) Click the Authentication tab and for Protocol, select **SSL**.
- c) Select the check box for Authenticate Users.
- d) Under Authentication Policies, click **Primary** and then choose the authentication policy you configured in Step 7.
- e) Click the Policies tab, click **Session**, and then choose the session policy you configured in Step 9.

For more information, see [Configuring the Authentication Virtual Server](#).

## Create a network share for private data storage

July 30, 2020

Storage zones for ShareFile Data requires a network share for your private data. When multiple storage zones controllers are configured for high availability and load balancing within a zone, all controllers access the same shared location for private data.

Even if you store ShareFile files in a supported third-party storage system, storage zones controller requires a network share for encryption keys, queued files, other temporary items, and a storage cache for file uploads to or downloads from that storage system. For more information about the storage cache, see [Customize storage cache operations](#).

Storage zone controllers access a network share using the IIS Account Pool user. By default, application pools operate under the Network Service user account, which has low-level user rights. Storage

zones controller uses the Network Service account by default. You can use a named user account instead of the Network Service account to access the share. Use the Network Service account to run the IIS application pool and Citrix ShareFile Services.

1. If you want to use a named user account instead of the Network Service account to access the share, create a named user account in Active Directory. We will refer to that named user account as the ShareFile Service account.

Note: When you configure storage zones controller, you will specify the Network Share User Name and Network Share Password, which are the credentials for the account you will use to access the share, either the ShareFile Service account or the Network Service account.

To improve security, the admin will need to deny permissions to all other users to the particular folder containing the ShareFile storage repository and give access only to the storage location user that is being configured.

2. Connect to the server that will host the network share and create a folder for your ShareFile private data.
3. Right-click the folder and choose Share with specific people....
4. Add the account you will use to access the share (Network Service account or ShareFile Service account) and change the Permission Level to Read/Write.
5. Click Share and then click Done.
6. Right-click the folder and choose Properties.
7. On the Security tab, verify that the account you will use to access the share (Network Service account or ShareFile Service account) has Full Access permissions.

## **Increase the number of files per zone**

By default, a storage zones controller is configured to use a CIFS share to store files in a hierarchy of folders instead of a single folder.

You can configure storage zones controller to divide the persistent storage layout. This increases the maximum number of files per zone for some types of storage arrays from less than a half million to ten million or more. If you need additional capacity, you can change the default.

## **To enable storage zones controller to store files in multiple folders**

### **Caution:**

Editing the Registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use

of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

**Note:**

If the Storage Zone Controller has been upgraded, Please check if the value of the registry key `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone\PathSelection` is set to 1. If it is set to 0, update it to 1.

Restart IIS on the storage zones controllers when you are finished editing the registry.

### To increase the maximum number of folders

By default, divided storage layout has 256 top-level folders, each of which contains 256 folders. That configuration is represented in the primary storage zones controller registry key `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone: PathSelectionParams=2,2`.

The first value constrains the number of top-level folders to “16 to the power of 2” or 256. The second value also constrains the number of child folders of the top-level folders to 256.

Using that same formula (16 to the power of N) you can determine the appropriate values for your site. For example, `PathSelectionParams=3,4,4` constrains the number of top-level folders to 4096 (16 to the power of 3). The second value constrains the number of child folders of the top-level folders to 65536 (16 to the power of 4). The third value constrains the number of child folders of the second-level folders to 65536, and so on.

Restart IIS on the primary and secondary storage zones controllers if you are finished editing the registry.

### To remove empty folders

When storage zones controller stores files in multiple folders, file deletion can result in empty folders. By default, storage zones controller removes empty folders. The file delete service will delete empty folders, starting at the bottom of the tree and continuing up until it reaches a non-empty folder.

However, some upgrade paths might not update your settings. After an upgrade, verify that the following key appears in `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`:

```
<add key="DeleteEmptyFoldersAfterFileDeletion" value="1"/>
```

If you need to add the key, restart the File Delete Service when you are finished.

## Install an SSL certificate

July 9, 2019

If you do not use a wildcard certificate, you must create a Certificate Signing Request (CSR) for the storage zones controller server and submit your request to a Certificate Authority (CA). For help, see the documentation for your CA.

Follow these steps to install a certificate.

1. On the storage zones controller server, open MMC and then choose **File > Add/Remove Snap-in**.
2. Select **Certificates** and then click **Add**.
3. Select **Computer Account**, click **Next**, click **Finish**, and then click **OK**.
4. In the MMC console, expand **Certificates > Personal**.
5. Right-click **Certificates**, choose **All Tasks > Import**, and then click **Next**.
6. Click **Browse** and then from the file name extension menu, choose **Personal Information Exchange**.
7. Browse to the certificate location and then click **Open**.
8. Click **Next**, enter the **Password** associated with your private key, click **Next** twice, and then click **Finish**.
9. When the message **Import was Successful** appears, click **OK**.

For a public certificate, make sure that the domain it is issued to resolves to the local IP address of storage zones controller. To do that, update the hosts file on the storage zones controller to map the domain associated with the certificate to the storage zones controller IP address. If the two addresses do not resolve, users will not be able to upload files from storage zones controller.

## Prepare your server for ShareFile data

September 29, 2023

The Web Server (IIS) role and ASP.NET setup described in this section is required for storage zones for ShareFile data and for storage zone connectors. These instructions are based on Windows Server 2012 but are valid for later versions as well.

## Update Microsoft .NET Version

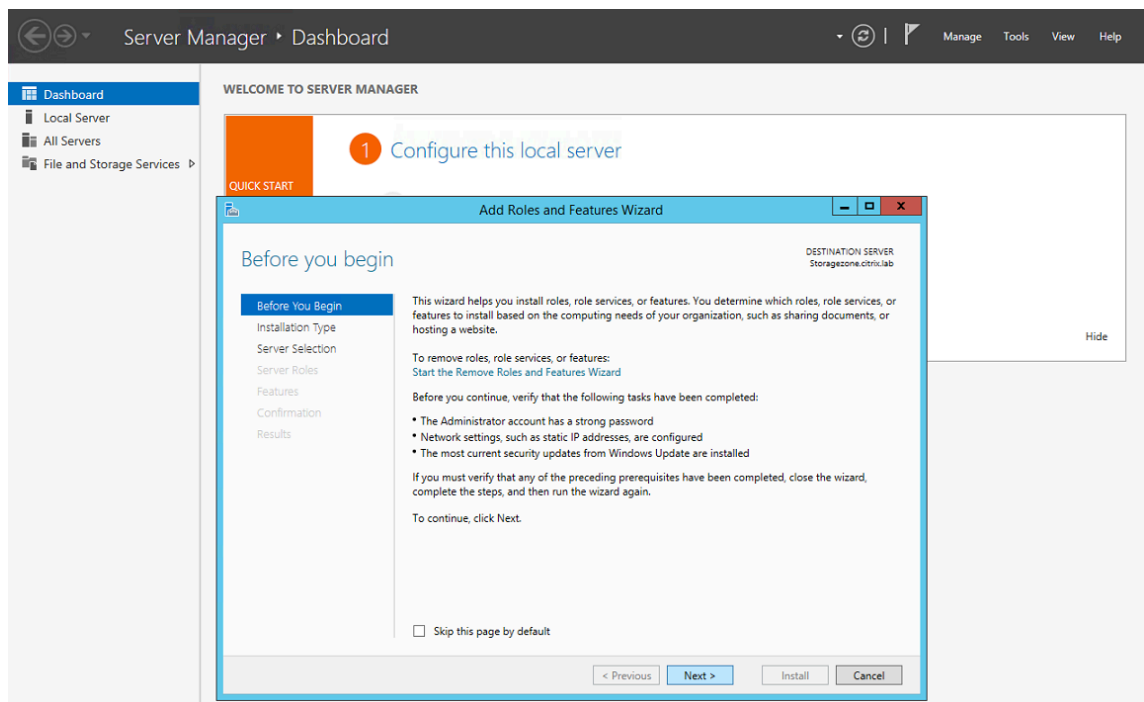
Before proceeding with storage zones controller installation, ensure that you are using the appropriate version of Microsoft .NET Framework.

- **Storage zones controller 5.x requires .NET 4.8 or later.** [Click here to download .NET 4.8](#)

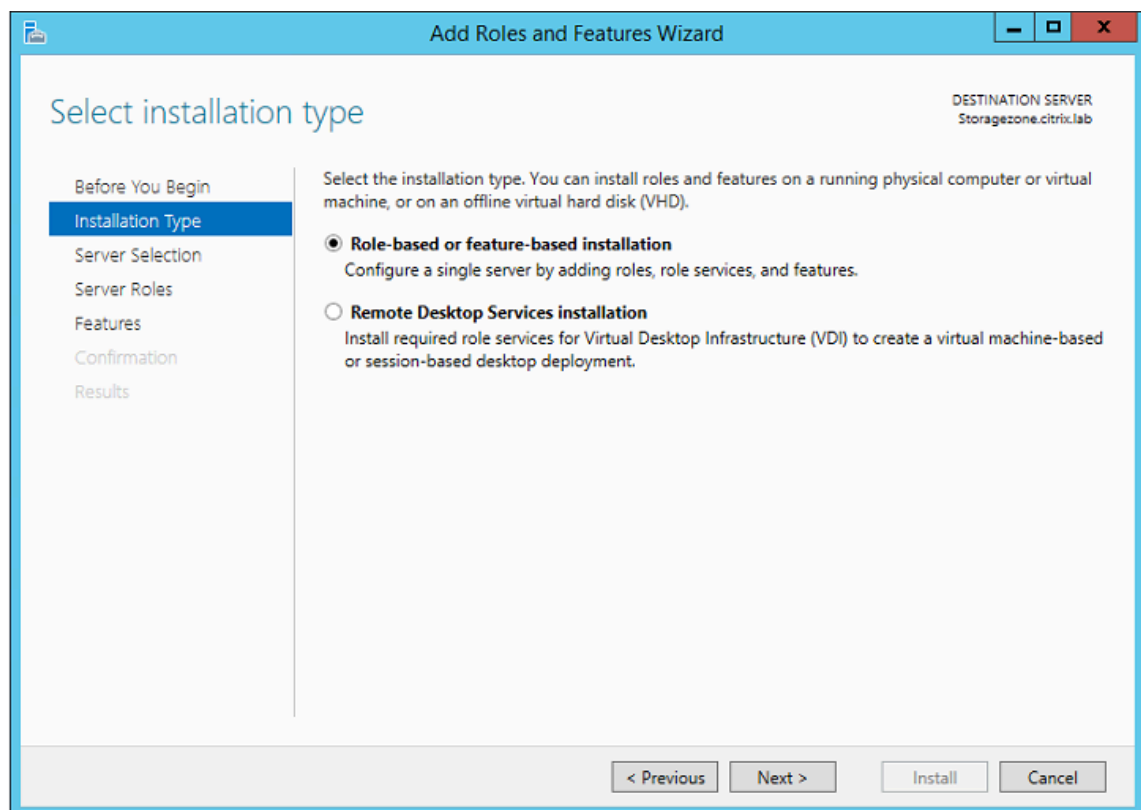
ShareFile recommends utilizing the latest version of Microsoft .NET when using ShareFile applications.

## To enable the Web Server (IIS) role and the ASP.NET role service

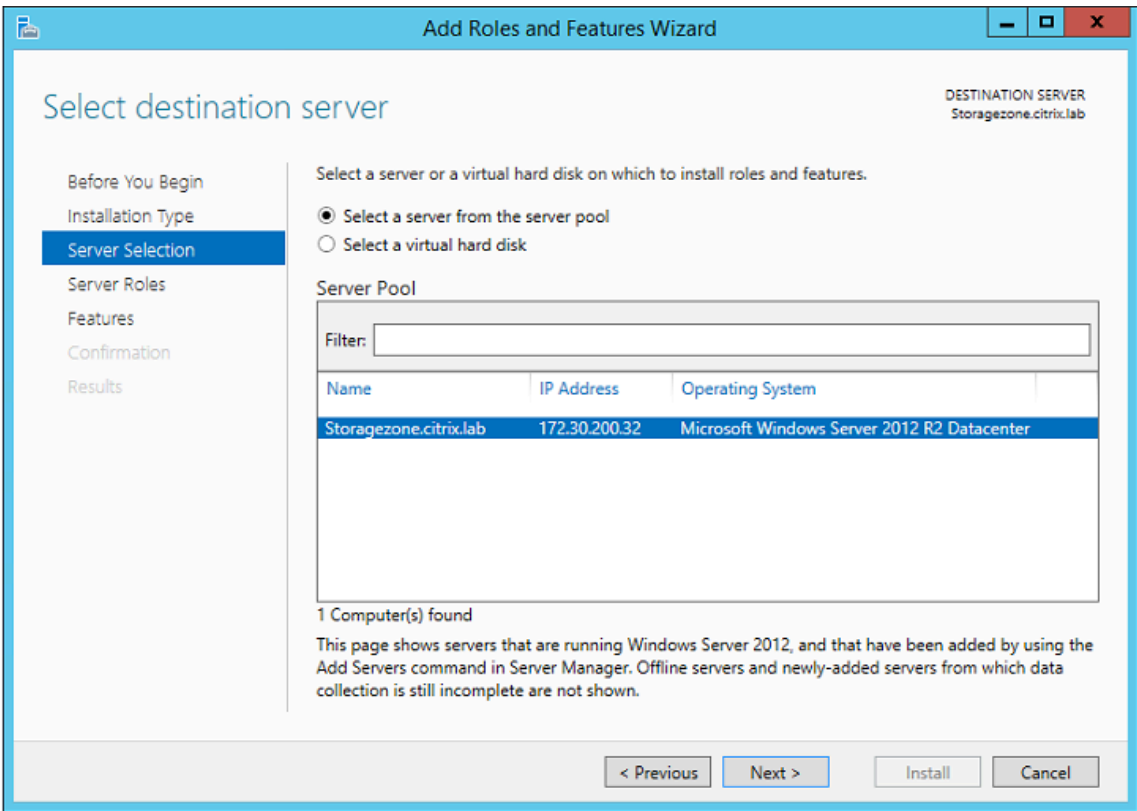
1. On the server where you install the storage zones controller, log on with an account that has local administrator privileges.
2. Open the Server Manager console Dashboard and then click **Manage > Add Roles and Features** to open the Add Roles and Features Wizard.
3. In the Add Roles and Features Wizard, click **Next**.



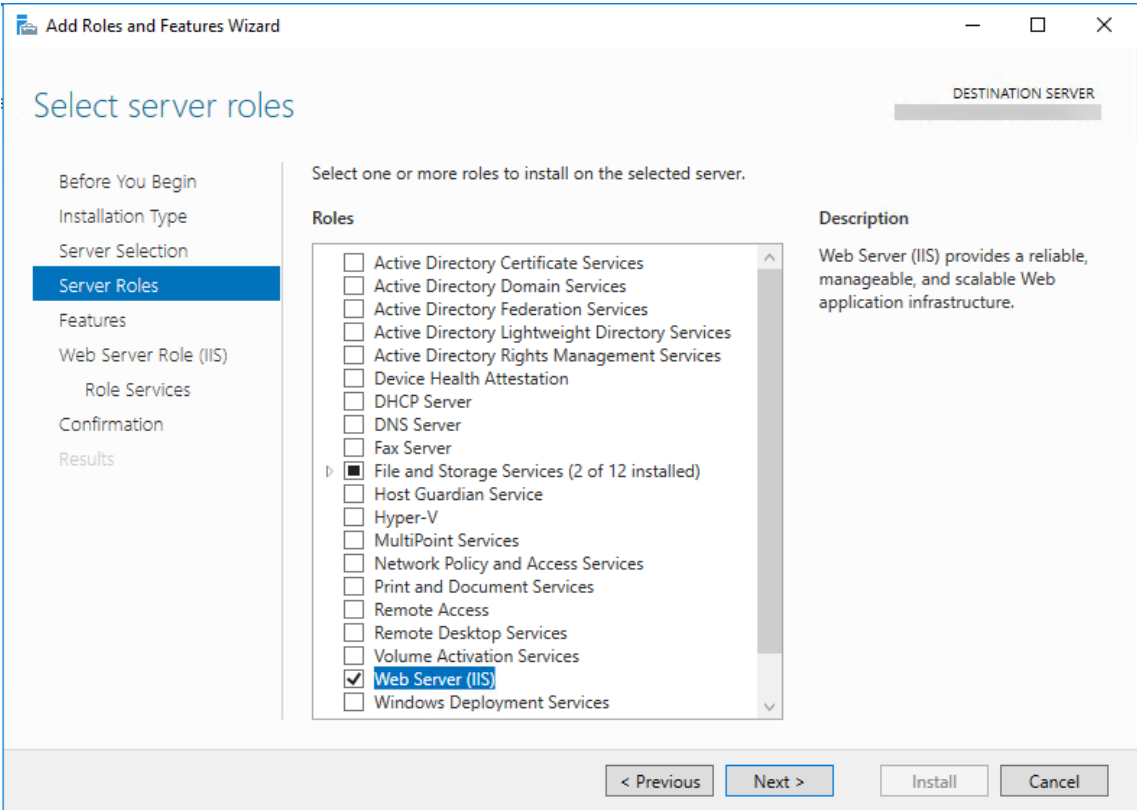
4. On the Select installation type page, click Role-based or feature-based installation and then click **Next**.



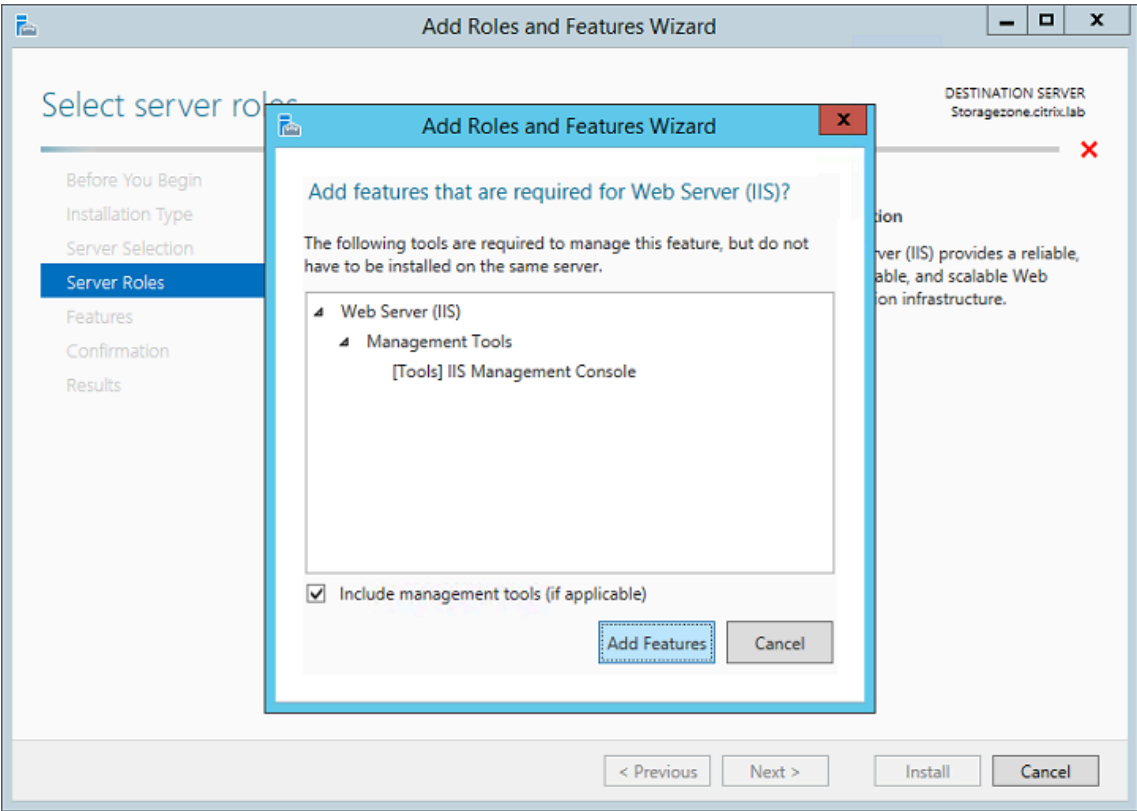
5. On the Select destination server page, choose your server from the server pool and then click **Next**.



6. On the Select server roles page, select the Web Server (IIS) check box then click **Next**.

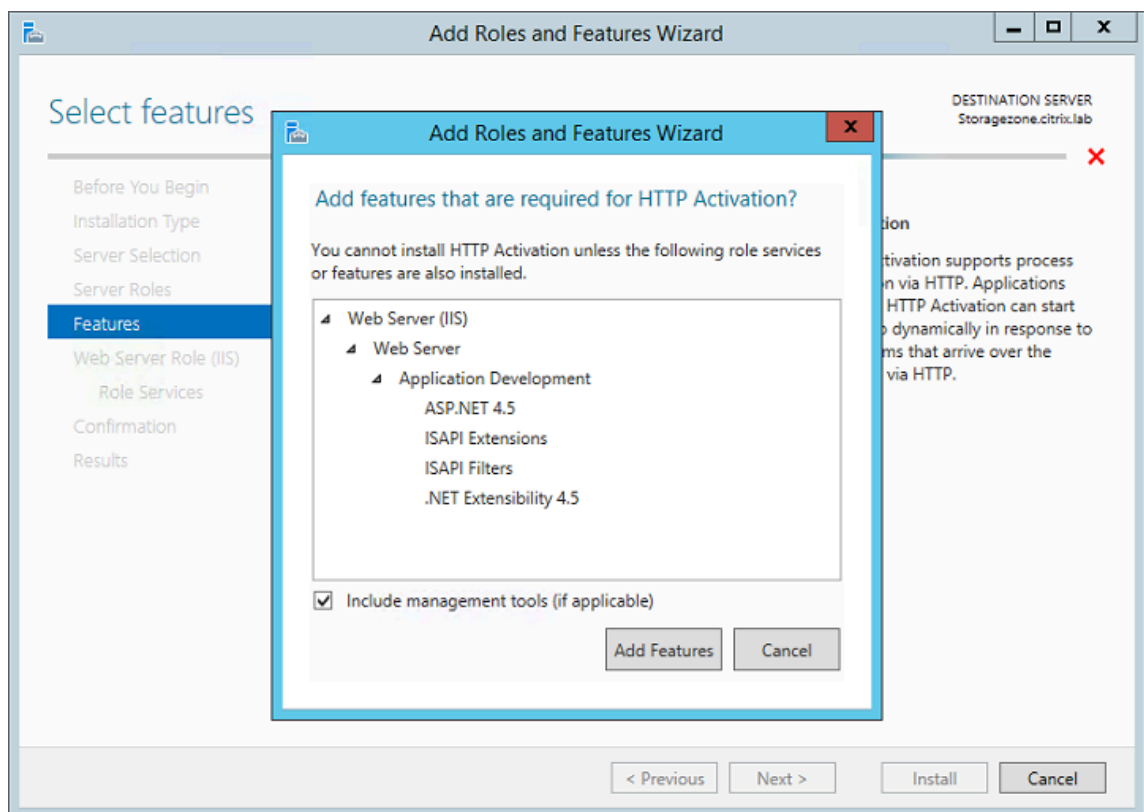


7. Click **Add Features** to add the features required for IIS.

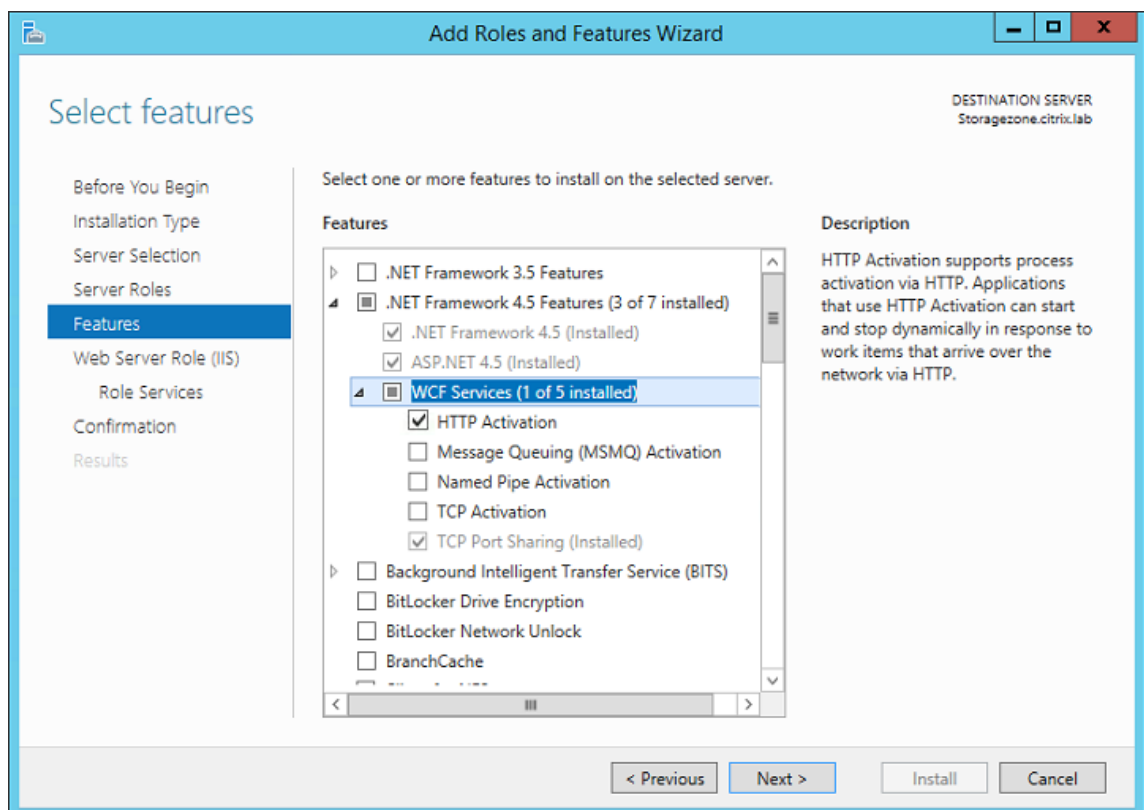


8. Click **Add Features**. The Select features page appears.

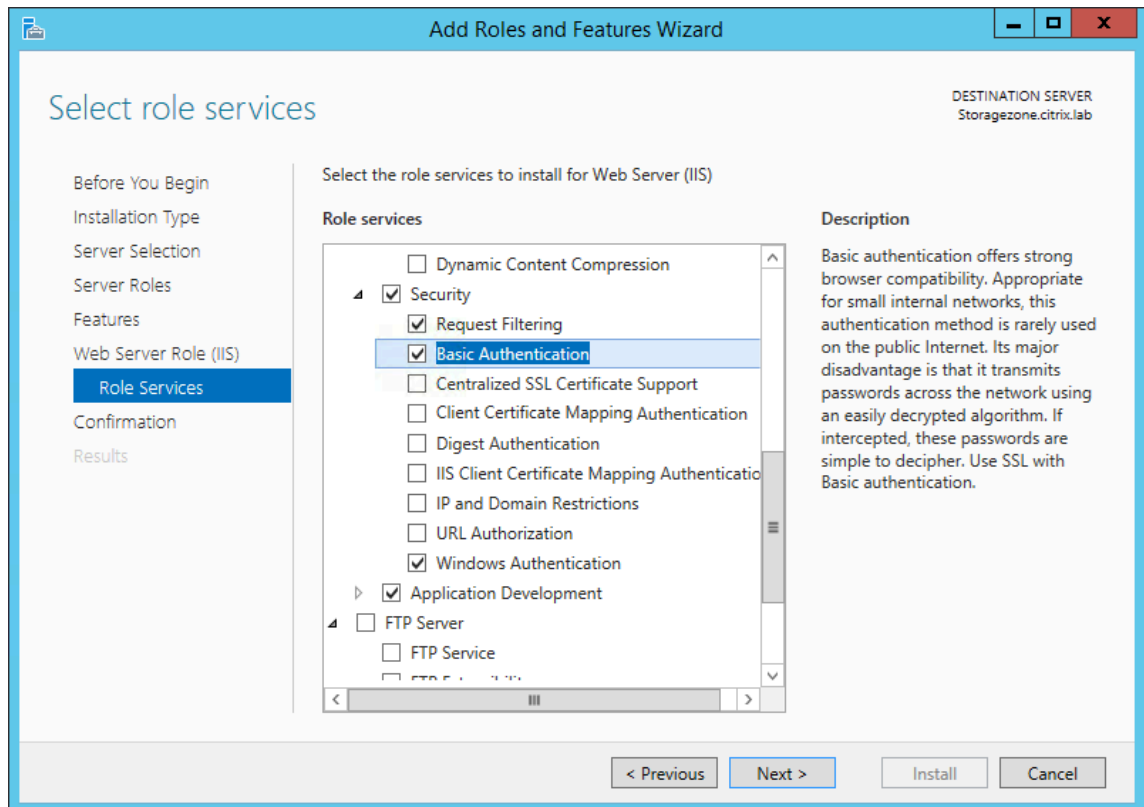




9. Select the required settings shown in the following screen, and then click **Next**.



10. On the Web Server Role (IIS) page, click **Next**.
11. On the Select role services page, select the Basic Authentication and Windows Authentication check boxes, and then click **Next**.

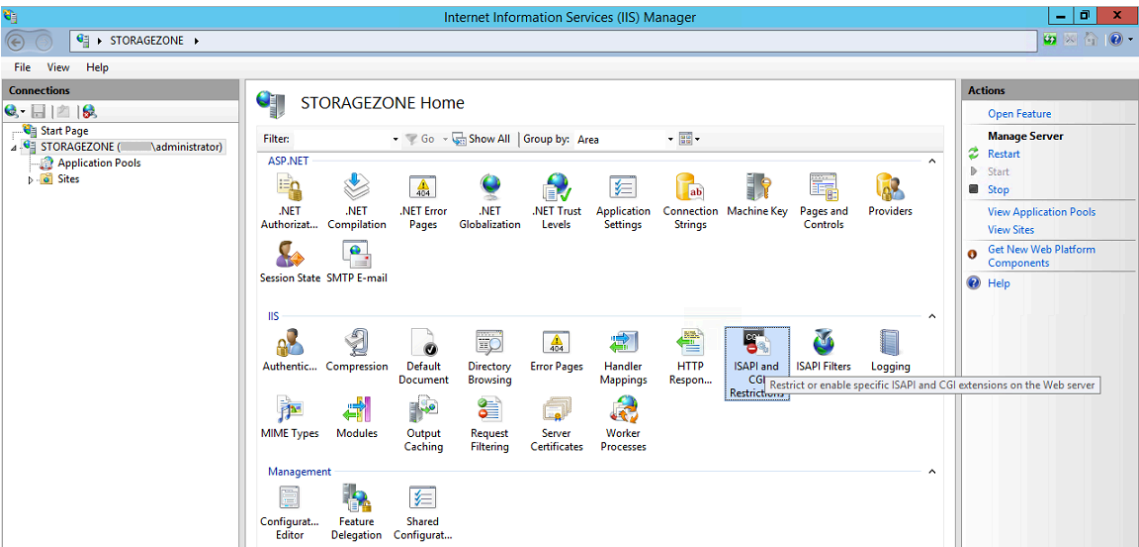


12. On the Confirm installation selections page, click **Install**.
13. When the installation completes, click **Close** and then restart the server.

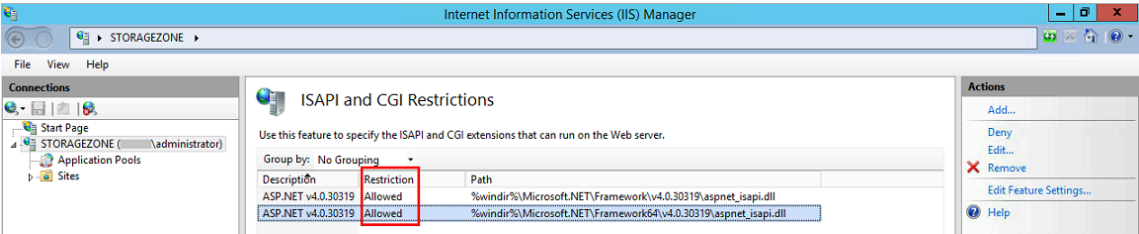
## To configure IIS

After you enable the Web Server (IIS) role and the ASP.NET role service, configure IIS.

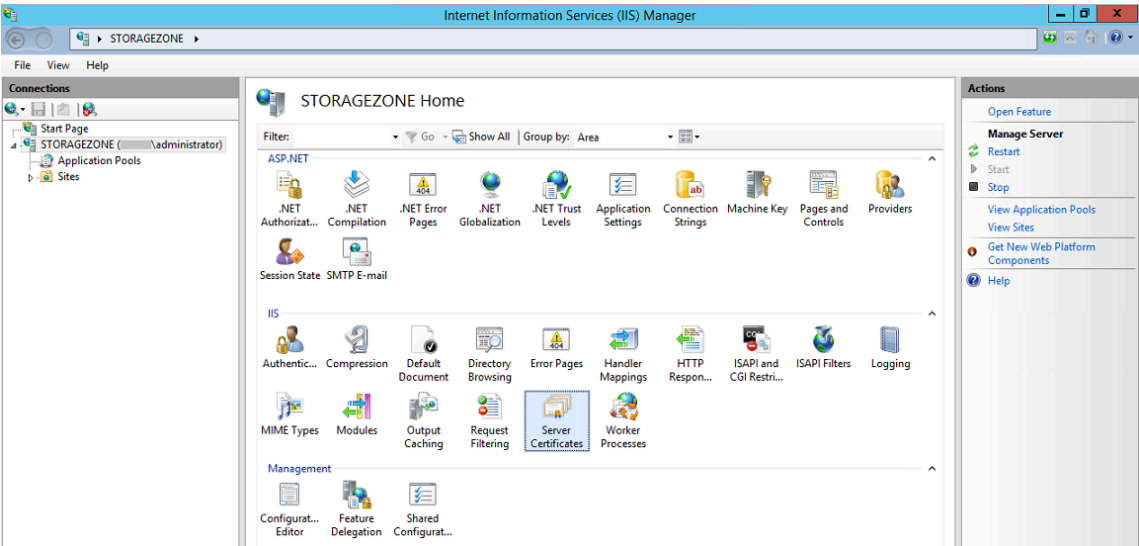
1. Open the IIS Manager console, click the storage zone controller server node, and then double-click ISAPI and CGI Restrictions.



2. Set each ASP.NET entry to Allowed.



3. Verify that a domain server or public certificate is installed on the server: In the IIS Manager console, click the storage zone controller server node, and then double-click Server Certificates.

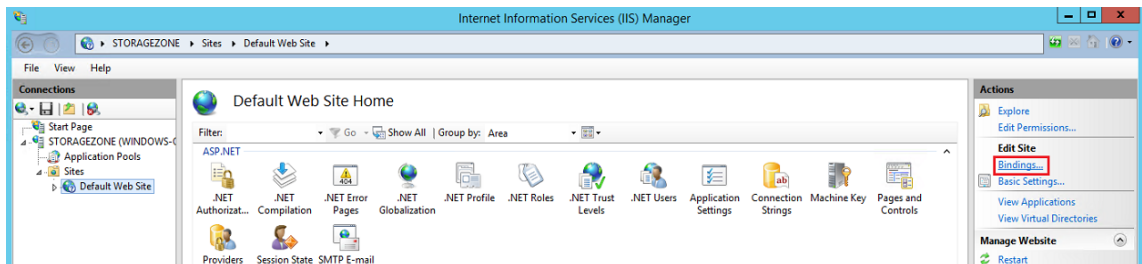


If there is no certificate associated with a public Certificate Authority, install a certificate on the server before proceeding. For more information, see [Install an SSL certificate](#).

**Note:**

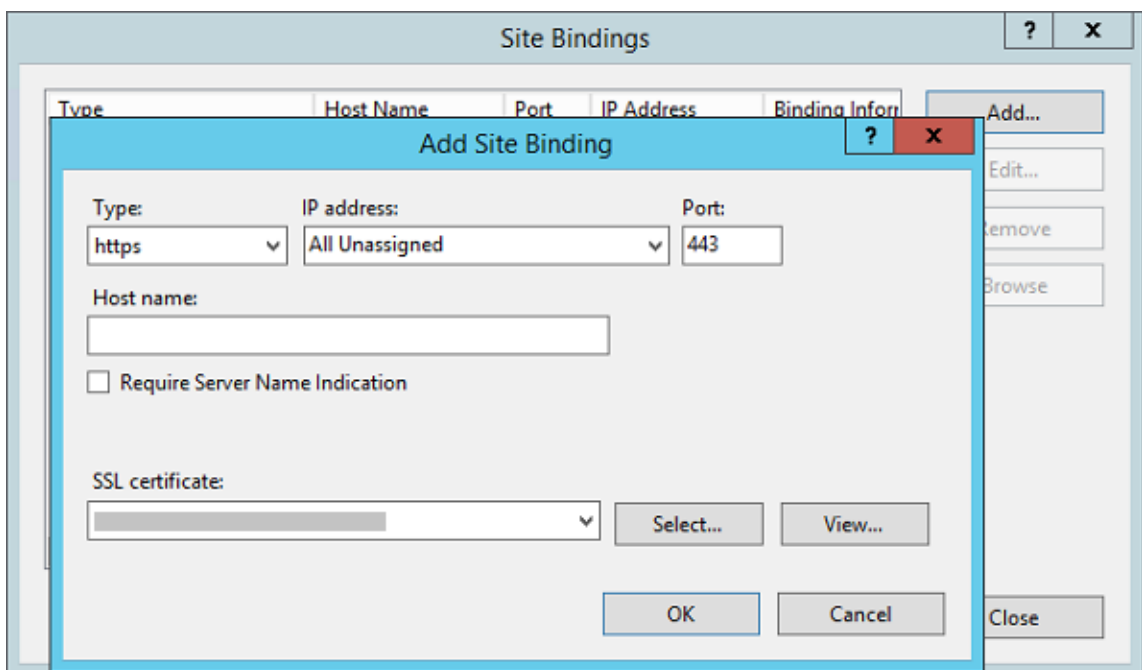
If you are using a Citrix Gateway or similar appliance with storage zones controller, you can use a domain server certificate. All internet traffic for standard zones must be handled using a public certificate.

4. In the IIS Manager console, click **Default Web Site** and then click **Bindings**.



5. Click Add and configure the site binding as follows:

- Type is https.
- IP address is All Unassigned.
- Port is 443.
- SSL certificate is your installed certificate.



6. To test the web server connection, navigate to <http://localhost/> and to <https://localhost/>. If the connection is successful, the IIS logo appears.

HTTPS displays a message about the certificate not matching the localhost name in the URL header. This is expected and you can safely continue to the website.

7. If you are installing storage zones controller on a VM, take a snapshot of the VM.

**NOTE:**

Storage zones controller uses CORS and requires **OPTIONS** http verb to be enabled. Please check IIS Request Filtering feature to make sure **OPTIONS** verb is not disabled.

## Install storage zones controller and create a storage zone

March 14, 2024

**Important:**

- Verify that your environment meets the [system requirements](#) before you start the installation.
- ShareFile storage zones controller uses application specific passwords. For more information, see [Create an application specific password](#).

When you install a storage zones controller, you either create a zone and configure a primary storage zones controller or [join secondary storage zones controllers to a zone](#).

While configuring a primary storage zones controller, you can enable either or both of these features:

- Storage zones for ShareFile Data, to specify private data storage, either a private network share or a supported third-party storage system.
- Storage zone connectors, to give users access to documents on SharePoint sites or specified network file shares.

The following steps describe how to install the storage zones controller, configure authentication for the IIS default website, create a zone, and enable features.

1. Download and install the storage zones controller software:
  - From the ShareFile download page at <https://dl.sharefile.com/storagezone-controller>, log on and download the latest storage zones controller installer.

**Note:**

Installing the storage zones controller changes the Default website on the server to the installation path of the controller.

**Anonymous Authentication** should be enabled on the default website.

2. On the server where you want to install the storage zones controller, run StorageCenter.msi.
  - The ShareFile storage zones controller Setup wizard starts.
  - For multitenancy, run the following command: ***msiexec /i StorageCenter\_5.0.1.msi MULTITENANT=1***

**Note:**

In the preceding command, you might need to update the version number (5.0.1 in the example) to match the number of the msi you are trying to install.

- Respond to the prompts. When installation is complete, clear the check box for **Launch storage zones controller Configuration Page** and then click **Finish**.
3. Restart the storage zones controller.
  4. To test that the installation is successful, navigate to <http://localhost/>. If the installation is successful, the ShareFile logo appears.
  5. If the ShareFile logo does not appear, clear the browser cache and try again.

**Important:**

If you plan to clone the storage zones controller, capture the disk image before you proceed with configuring the storage zones controller.

6. To use an S3-compatible storage provider with ShareFile, perform the following steps before creating or configuring a storage zone.
  - Open Windows Registry Editor (**Run > regedit.exe**).
  - Find the HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter registry key.
  - Create a new REG\_SZ value under this key:
    - Value name: **S3EndpointAddress**
    - Value type: **REG\_SZ**
    - Value data: Enter the HTTPS URL that corresponds to your S3-compatible storage endpoint.
  - If the storage provider supports only path-style container access (see <http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html>), create another value under this key.
    - Value name: **S3ForcePathStyle**
    - Value type: **REG\_SZ**

- Value data: **true**
- Restart the storage zones controller application pool (StorageCenterAppPool).
- Gather the following information from your S3-compatible storage system:
  - The name of an S3 bucket to use for ShareFile dataAccess key ID
  - Access key ID
  - Secret access key
- 7. Continue with the following steps to create a new storage zone. Choose Amazon S3 as the persistent storage location. storage zones controller uses the custom endpoint address you entered instead of the actual Amazon S3 service. When configuring the S3 details, choose the bucket name you created earlier.
- 8. Navigate to the storage zones controller console.
- 9. Open <http://localhost/configservice/login.aspx> or start the configuration tool from the Start screen or menu. For information about using the Start screen shortcut in Windows 8, see [Manage storage zones controllers](#).
- 10. On the **storage zones controller Logon** page, enter the **email address**, **password**, and **full account URL FQDN subdomain**, such as [subdomain.sharefile.com](#) or [subdomain.sharefile.eu](#), for your account. Click **Log On**.
- 11. To set up your primary storage zones controller, click **Create new Zone** and provide the zone information:

---

Option	Description
Zone	A name that appears in the ShareFile Administrator console.

Option	Description
Primary Zone controller	Defaults to <a href="http://localhost/ConfigService">http://localhost/ConfigService</a> . If you use SSL, change HTTP to https. Keep in mind that ShareFile supports only valid, trusted public SSL certificates for standard zones. If you have problems configuring a secondary storage zone host, ensure that you can resolve the ConfigService URL in a local browser on that server, with no SSL errors. localhost resolves to the server IP address. You can specify a server name instead (such as <a href="https://servername.subdomain.com/ConfigService">https://servername.subdomain.com/ConfigService</a> ). The server name must be resolvable by a secondary storage zones controller server.
Host name	A unique identifier for your storage zones controller. ShareFile recommends that you use the server host name as the identifier. This should be a friendly name and not the FQDN. This name appears in the ShareFile Administrator console.
External Address	The FQDN for this storage zones controller. If this storage zones controller will be used for standard zones, the URL must be accessible from the Internet. If you are using a load balancer, enter its address. When you submit the page, ShareFile validates the address.

12. To specify private data storage, do the following.

- Select the check box for **Enable storage zones for ShareFile Data**.
- To configure a standard zone, clear the check box.

**Note:**

After you configure a storage zones controller, you cannot change its zone type.

Storage zones controller uses the service account credentials to connect to the trusted Active Directory domain server for email address lookup.



- Choose a Storage Repository.
13. If you do not want to enable storage zone connectors, click **Register** to register storage zones controller with ShareFile and then continue with Step 14.
14. If you are using S3-compatible storage, create these additional registry entries after the storage zone registers:
- Open Windows Registry Editor (**Run > regedit.exe**).
  - Find the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\storage zone\CloudStorageUploaderConfig` registry key.
  - Create a new REG\_SZ value under this key:
    - Value name: **S3EndpointAddress**
    - Value type: **REG\_SZ**
    - Value data: Enter the HTTPS URL that corresponds to your S3-compatible storage endpoint.
  - If the storage provider supports only path-style container access (see <http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html>), create another value under this key.
    - Value name: **S3ForcePathStyle**
    - Value type: **REG\_SZ**
    - Value data: **true**
  - Restart the storage zones controller application pool (StorageCenterAppPool).
15. To enable storage zone connectors:
- Enabling the connectors creates the IIS apps “cifs”(connector for Network File Shares) and “sp” (connector for SharePoint).
- Select the check box for each connector type you want to use: Enable storage zone connector for Network File Shares and Enable storage zone connector for SharePoint. For information about the connector settings, see [Configure storage zone connectors](#), in this section.
  - Click **Register**. Your storage zones controller information appears.
  - If you specified **Allowed Paths or Denied Paths** for storage zone connectors, restart the IIS server.
16. To configure secondary storage zones controllers, refer to [Manage storage zones controllers](#).

**Important:**

A storage zones controller is installed on your local site and you are responsible for backing it up. To protect your deployment, you should take a snapshot of the storage zones controller server, [back up the storage zones controller configuration](#), and [prepare storage zones controller for disaster recovery](#).

## Configure storage zones for ShareFile Data

**Note:**

Storage zones for ShareFile Data is available for Citrix Endpoint Management Enterprise Edition and is not available for other Citrix Endpoint Management editions.

You can configure storage zones for ShareFile Data from the storage zones controller wizard when you create a storage zone or from the storage zones controller console. Use the ShareFile Data tab to configure settings for private network shares or supported third-party storage systems.

### Network share settings

---

Option	Description
Storage Repository	Choose Local network share. After you create the zone, you cannot change the Storage Repository option. For example, to switch from a local network share to third-party storage, you must create a new zone.

Option	Description
Network Share Location	<p>The UNC path to the network share you will use for private data storage and for data such as encryption keys, queued files, and other temporary items. Specify the path in the form <code>\\server\share</code>. storage zones controllers belonging to the same storage zone must use the same file share for storage. Caution: storage zones controller will overwrite any data in this path with a proprietary storage format. Never specify a path to a location with file data. Reserve this storage location for storage zones for ShareFile Data only. storage zones controllers access the Network Share using the Network Share username/password supplied on the config page. If no Network Share username/password is supplied on the config page, then the Network Service account will be used by default. The Network Service account must have full access to this storage location. Storage zones controller will also use the Network Service account by default for the StorageCenterAppPool. It is important to note that the only supported configuration is to use the Network Service account.</p>
Network Share user name and Network Share Password	<p>The credentials for the UNC path of your network share location. To use a named user account instead of the Network Service account to access the share, specify those credentials. You can continue to run the IIS application pool and the ShareFile Services using the Network Service account.</p>

Option	Description
Enable Encryption	Select the check box only if you want to encrypt the file content stored on your file share. In an enterprise environment where the network share is inside your network and already secured by third-party tools, we recommend that you do not encrypt the files on the share. This setting does not relate to metadata. Metadata is not encrypted for standard zones. Although this additional security is offered as an option for maximum security when required, encrypting files on the share will make the disk unreadable by third-party tools such as antivirus scanners and filer tools, including data deduplication tools. ShareFile uses a file encryption key to confirm the validity of download requests and encrypt the storage.
Passphrase	A phrase used to protect your file encryption key. The passphrase must contain more than six characters. Be sure to archive the passphrase and encryption key in a secure location. You must use the same passphrase for each storage zones controller in a zone. The passphrase is not the same as your account password and cannot be recovered if lost. If you lose the passphrase, you cannot reinstall storage zones, join additional storage zones controllers to the storage zone, or recover the storage zone if the server fails. Note: The encryption key appears in the root of the shared storage path. Losing the encryption key file, SCKeys.txt, immediately breaks access to all storage zone files. Be sure to back up the encryption key file as part of your normal data center procedures.

---

### Shared Cache configuration settings

Option	Description
Shared cache location	the path to a network share that will contain your storage cache and data such as encryption keys, queued files, and other temporary items. Specify the path in the form <code>\\server\share</code> . storage zones controllers belonging to the same storage zone must use the same file share for storage. Caution: storage zones controller will overwrite any data in this path with a proprietary storage format. Never specify a path to a location with file data. Reserve this storage location for storage zones for ShareFile Data only. The Network Service account (or the account the ShareFile Management Service is configured to run as) must have full access to this storage location.
Shared cache Logon and Shared cache Password	The credentials for the UNC path of your shared cache location.
Enable Encryption	Select the check box to encrypt the files stored in your shared cache.

### Windows Azure storage container settings

Option	Description
Storage Repository	Choose Azure storage container. After you create the zone, you cannot change the Storage Repository option. For example, to switch from a local network share to Azure-based storage, you must create a new zone.
Account Name	The name of your Azure storage account. These names are always lower case.
Access Key	The primary or secondary access key for your Azure storage. Copy the key from the Manage Access Keys screen of the Windows Azure Management Portal.

Option	Description
Validate	Click the button to validate the Azure access key. You cannot proceed with the configuration until the validation is completed and the Container Name menu includes all available containers for the specified account.
Container Name	Select the Azure container to use for all storage zones controllers in this storage zone. This list is empty until your Azure access key is validated.

### Amazon S3 storage bucket settings

Option	Description
Storage Repository	Choose the Amazon S3 storage bucket. After you create the zone, you cannot change the Storage Repository option. For example, to switch from a local network share to Amazon S3 storage, you must create a new zone.
Access Key Id	The access key ID for your Amazon S3 storage.
Secret Access Key	The secret access key for your Amazon S3 storage.
Validate	Click the button to validate the Amazon S3 secret access key. You cannot proceed with the configuration until the validation is completed and the Bucket Name menu includes all available buckets for the specified account.
Bucket Name	Select the Amazon S3 bucket to use for all storage zones controllers in this storage zone. This list is empty until your Amazon S3 secret access key is validated.

### SMTP settings

---

Option	Description
SMTP server address and SMTP port number	Your local SMTP server host name and port.
Use SSL	Select the check box to connect to the SMTP server over a secure connection.
User name and Password	The user name and password for your local SMTP server.
Authentication mode	The Default authentication mode uses the most secure method available to connect from the storage zones controller to the SMTP server.
Sender address	The email address that appears in the From field.

---

## Google Cloud platform

Generate an access key and secret from **Google Cloud Platform > Settings > Interoperability**.

Before running storage zones Configuration, set the **S3EndpointAddress** registry value to <https://storage.googleapis.com> and then restart IIS.

### Option 1

#### Description

##### Storage repository

Choose **Amazon S3 storage bucket**. After you create the zone, you cannot change the **Storage Repository** option. For example, to switch from a local network share to Amazon S3 storage, you must create a new zone.

##### Access Key ID

The Access Key ID from your Google Cloud Platform storage.

##### Secret Access Key

The Secret from your Google Cloud Platform storage.

##### Validate

Click the button to validate the Google Cloud Platform secret access key. You cannot proceed with the configuration until the validation is completed and the **Bucket Name** list includes all available buckets for the specified account.

##### Bucket Name

Select the correct bucket to use for all storage zones controllers in this storage zone. This list is empty until your Google Cloud Platform secret access key is validated.

## Configure storage zone connectors

Storage zone connectors give users access to documents on SharePoint sites or specified network file shares. You do not have to enable storage zones for ShareFile Data to use storage zone connectors.

**Note:**

Storage zones for ShareFile Data and the storage zones connectors features can share a zone. However, storage zones controller keeps the data and access rules for the two data types separate.

You can configure storage zone connectors when you create a zone using the storage zones controller wizard or from the storage zones controller console.

To control access to particular network file shares or SharePoint document libraries, specify a list of Allowed Paths or Denied Paths. After you save your changes, restart the IIS server.

In-bound connections to storage zone connectors are first checked against the allowed paths. If the connection is allowed, the path is then checked against the denied paths. For example, to provide access to `\\myserver\teamshare` and all of its subfolders, specify an allowed path of `\\myserver\teamshare`.

- All connections are allowed by default, indicated by an Allowed Paths value. The value is not valid for Denied Paths.
- If the allowed and denied paths conflict with each other, the most restrictive path is enforced.
- Entries are comma-separated.
- For connectors to network file shares, specify the allowed UNC paths.

Example with FQDN: `\\fileserver.acme.com\shared`

You can use the following variables in the UNC path:

- %UserName%

Redirects to a user's home directory. Example path: `\\myserver\homedirs\\%UserName%`

- %HomeDrive%

Redirects to a user's home folder path, as defined in the Active Directory property Home-Directory. Example path: `%HomeDrive%`

- %TSHomeDrive%

Redirects to a user's Terminal Services home directory, as defined in the Active Directory property ms-TS-Home-Directory. The location is used when a user logs on to Windows from a terminal server or Citrix XenApp server. Example path: `%TSHomeDrive%`



In the Active Directory Users and Computers snap-in, the ms-TS-Home-Directory value is accessible on the Remote Desktop Services Profile tab when editing a user object.

- %UserDomain%

Redirects to the NetBIOS domain name of the authenticated user. For example, if the authenticated user logon name is “abc\johnd”, the variable is substituted with “abc”. Example path: `\\myserver%UserDomain%_%UserName%`

The variables are not case sensitive.

- For a connector to a root-level SharePoint site, specify the root-level path.

Example: `https://sharepoint.company.com`

- For a connector to a SharePoint site collection:

Example: `https://sharepoint.company.com/site/SiteCollection`

- For connectors to SharePoint 2010 document libraries, specify the URLs (not including path terminators, such as file.aspx or /Forms).

Examples:

- `https://mycompany.com/sharepoint/`
- `https://mycompany.com/sharepoint/sales-team/Shared Documents/`
- `https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx`

The default SharePoint 2013 URL (when Minimal Download Strategy is enabled) is in the form:

`https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`.

## Security recommendation to remove the server header

IIS/ASP.NET by default exposes the Server header in HTTP responses. This header could become useful to an attacker. The header discloses the sending server type and in some cases the version number. This header is not necessary for production sites and can be disabled.

Unfortunately, the storage zones controller installer is not able to remove this header automatically. But we can provide recommendations to customers to remove this header in our storage zones controller documentation/installation guide.

Refer to the following article for the specific steps that we should provide in our documentation:

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

## Verify your storage zones controller setup

July 9, 2019

Verify that a storage zones controller registered with ShareFile, and then check for other configuration issues before you continue.

1. In the storage zones controller console, click the **Monitoring** tab.

2. Verify that Heartbeat Status has a green checkmark.

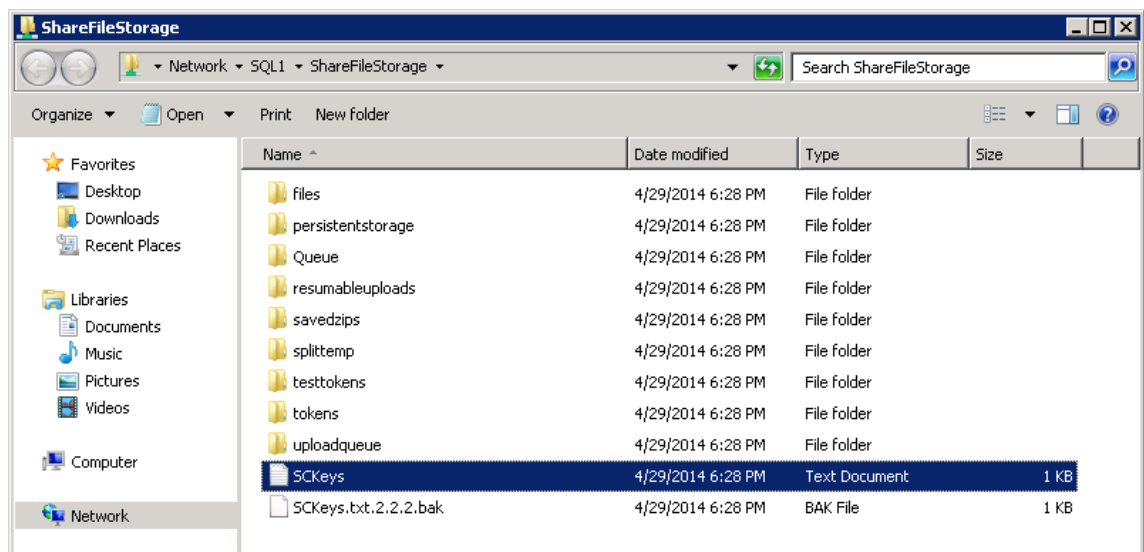
A red icon indicates that ShareFile.com is not receiving the heartbeat messages. In that case, verify network connectivity from your storage zones controller to [www.ShareFile.com](http://www.ShareFile.com) and from an outside PC to the URL of your storage zones controller. For standard zones, storage zones controller must be accessible on port 443 with a valid, trusted public SSL certificate.

After an upgrade, the ShareFile Connectivity from File Cleanup Services status might temporarily show a red icon. This occurs if Windows starts that service before storage zones controller establishes a network connection. The status will return to a green icon after the controller server is back on the network.

3. Check connectivity to your private zone: Navigate to the external URL (in the form of <https://server.subdomain.com>) of your private zone.

If Internet traffic is allowed to pass to and from a storage zones controller, you will see the ShareFile logo. If storage zones controller is not configured correctly, you might see an IIS logo or a Citrix ADC logon screen. Make sure that inbound and outbound HTTPS traffic is allowed over port 443. If your external URL points to Citrix ADC, look for hits on the content switching and load balancing virtual server for data. For more information, see “Storage zones controller does not upload data to ShareFile” in [Troubleshoot installation and configuration](#).

4. Verify that the network share you created for private data storage has a folder structure and a few files created by storage zones controller, including SCKeys.txt, which must reside in the root folder of the shared storage.



SCKeys.txt is created when storage zones controller is installed, provided there are no credential or access rights issues. If SCKeys.txt is not present, verify the access control lists on your file share and then reinstall storage zones controller.

5. Check the status of storage zone connectors from the ShareFile interface:
  - a) Log on to your ShareFile Enterprise account, navigate to **Admin > Storage zones**, and verify that the Health column includes a green check mark.
  - b) Click the site name and verify that the Heartbeat message indicates that the storage zones controller is responding.
6. Test a file upload: Log on to the ShareFile web interface, create a shared folder assigned to the zone you just configured, upload a file to that folder, and then verify that the file appears in the folder.

## Change the default zone for user accounts

March 14, 2024

By default, existing and newly provisioned user accounts use the ShareFile-managed cloud storage as the default zone. Change the default zone as follows:

- To specify the default zone for user accounts provisioned from AD, during user provisioning, select the storage location. For more information, see **Edit User Rule Options** in the [ShareFile Policy Based Administration](#) article.
- To change the default zone for an individual user, open the ShareFile administrator console and go to **Manage Users**.

## Specify a proxy server for storage zones

February 3, 2021

The storage zones controllers console enables you to specify a proxy server for storage zones controllers. You can also specify a proxy server using other methods.

Primary and secondary storage zones controllers communicate with each other using HTTP. If all HTTP traffic is configured to go through an outbound proxy server that does not support connections back to an internal server, you must configure both the primary and secondary storage zones controllers to bypass the proxy server so they can communicate with each other, as described in the following steps.

### Important:

The bypass list settings appear only for the latest storage zones controller release. If you are using StorageZones Controller 2.2 through 2.2.2, you must manually add a bypass list to Web.config for each secondary server, as described in [Web.config](#).

1. In the storage zones controller console (<http://localhost/configservice/login.aspx>), click the **Networking** tab.

### Note:

If you are using storage zones controller 5.11.17, changing any proxy requires authentication. When prompted, enter the email address, password, and full account URL FQDN subdomain, such as subdomain.sharefile.com or subdomain.sharefile.eu, for your account. Click Log On.

2. Select the Enable Proxy check box and enter the proxy server Address and Port.
3. Select an Authentication Mode and specify your Windows account designated for ShareFile proxy access.
4. If your site proxies all outbound HTTP traffic and a zone has multiple storage zones controllers, configure bypass settings:
  - If all storage zones controller traffic is on the same subnet, select the **Bypass proxy...** check box so the controllers can communicate with each other.
  - If the storage zones controllers are on different subnets, enter the primary storage zones controller host name or IP address in Bypass Address.
5. Restart the IIS server of all zone members.

## Configure the domain controller to trust the storage zones controller for delegation

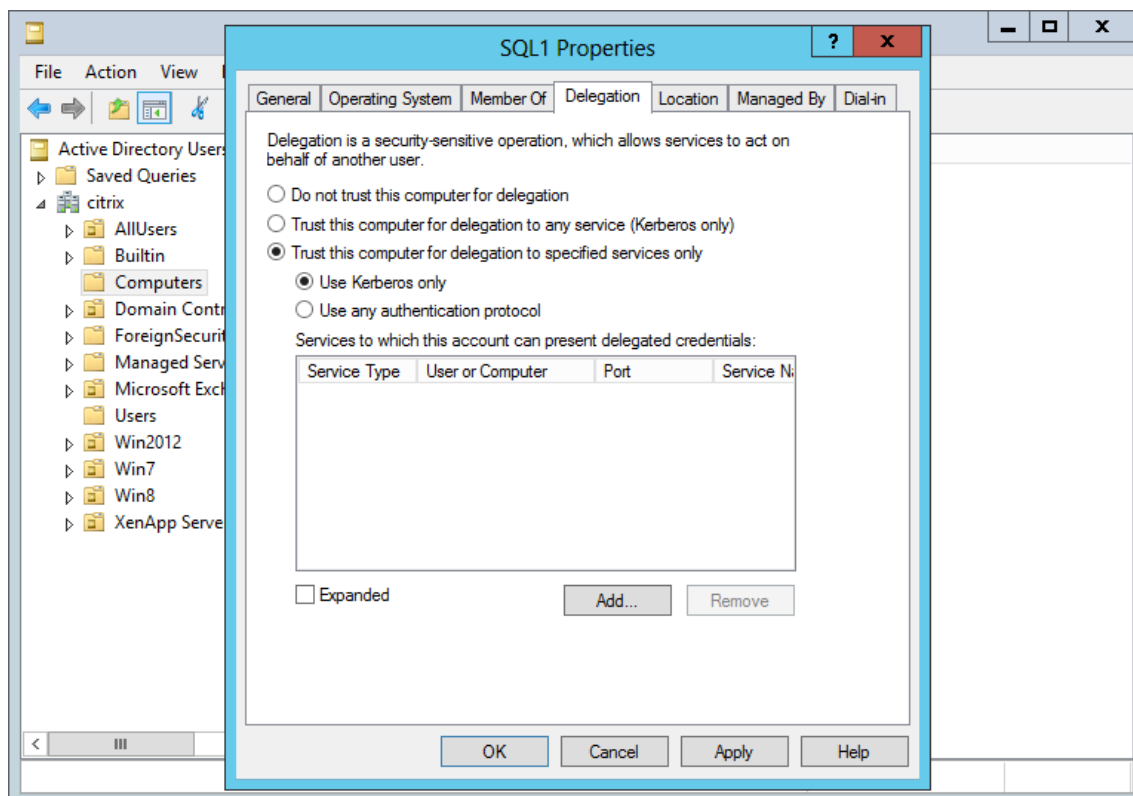
July 27, 2020

**Note:**

This section applies only to storage zone connectors.

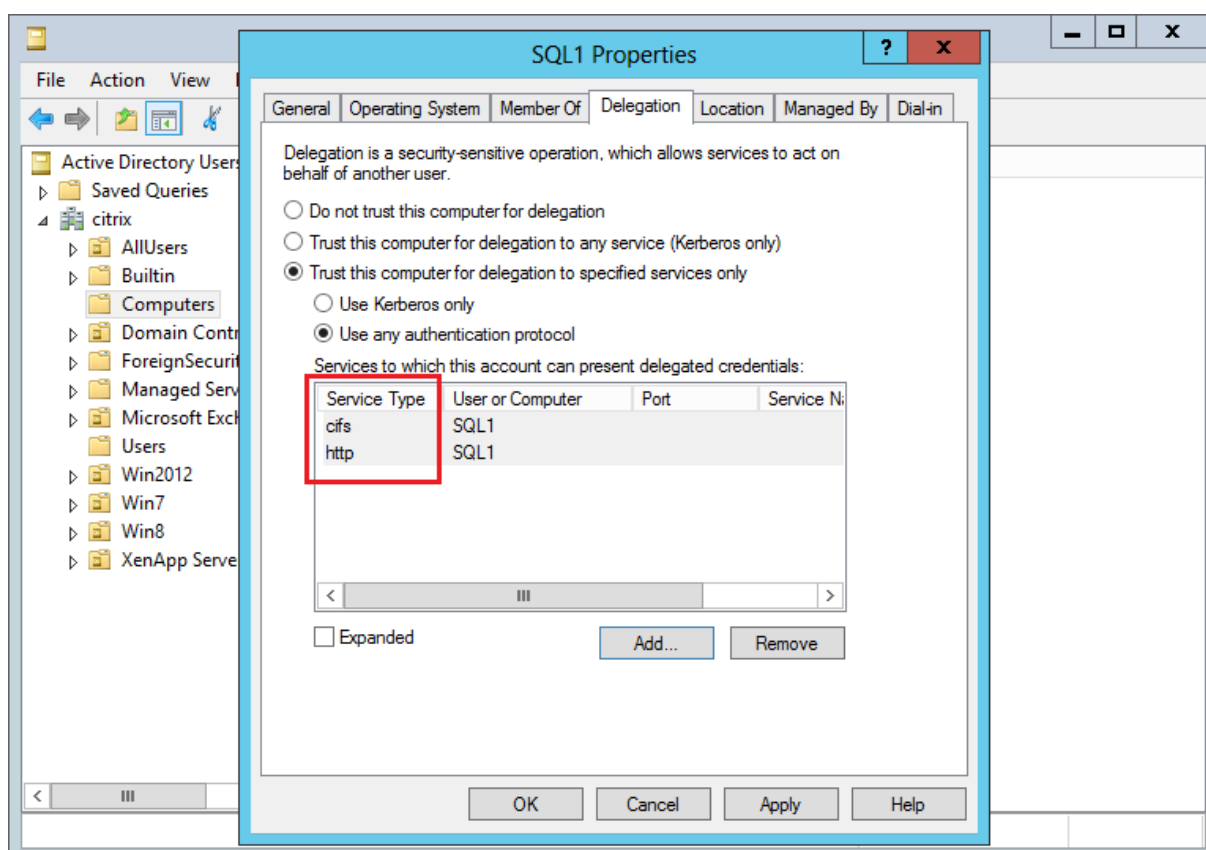
To support NTLM or Kerberos authentication on network shares or SharePoint sites, configure the domain controller, as follows.

1. On the domain controller for the storage zones domain, click **Start > Administrative Tools > Active Directory Users and Computers**.
2. Expand the domain, and expand the Computers folder.
3. In the right pane, right-click the storage zones controller name, select **Properties**, and then click the **Delegation** tab.
4. For Kerberos, select **Trust this computer for delegation to specified services only**.



5. For NTLM:

- a) Select **Trust this computer for delegation to specified services only** and **Use any authentication protocol**. Click **OK**.
- b) Click the **Add** button. In the **Add Services** dialog box, click **Users or Computers** and then browse to or type the host name for the network share or SharePoint server. Click **OK**.  
If you have multiple file servers or SharePoint servers, add a service for each.
- c) In the Available Services list, select the services used: CIFS (for connector for Network File Shares) and HTTP (for connector for SharePoint). Click OK.



## Configure storage zones controller for Web App previews, thumbnails, and view-only sharing

March 14, 2024

On-premises file previews are rendered by your on-premises Microsoft Office Web Apps (OWA) Server. When previewing files stored on a Citrix-managed storage zone, previews will be rendered by Citrix-managed or Microsoft-managed OWA servers.

**Important:**

**Whitelisting requirements:**

\* [\\*.sf-api.com](https://*.sf-api.com) must be accessible by your Office Online Server for previewing and editing to function properly on storage zones version 5.0 or later.

## Requirements

### Supported filetypes for on-premises file preview

- doc, .docm, .docx, .dot, .dotm, .dotx, .odt
- .ods, .xls, .xlsb, .xls, .xslm, .xlsx
- .odp, .pot, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx
- .pdf
- Image Files (bmp, gif, jpg, jpeg, png, tif, tiff)

### Supported file types for on-premises file edit

- .docm, .docx, .odt
- .ods, .xlsb, .xslm, .xlsx
- .odp, .ppsx, .pptx

### Supported environments

- Standard Zones
- Multitenant Zones
- Web Application

### Whitelisting / network considerations

- OOS Server should be able to reach [https://\\*.sf-api.com](https://*.sf-api.com) (or .eu)
- SZC Server should be able to reach [https://\\*.sf-api.com](https://*.sf-api.com) and [https://\\*.sharefile.com](https://*.sharefile.com) (or .eu)
- SZC Server should be able to reach OOS Server <https://<Customer OOS / OWA Endpoint>/hosting/discovery> (for example, <https://oos.sharefileexample.com/hosting/discovery>)

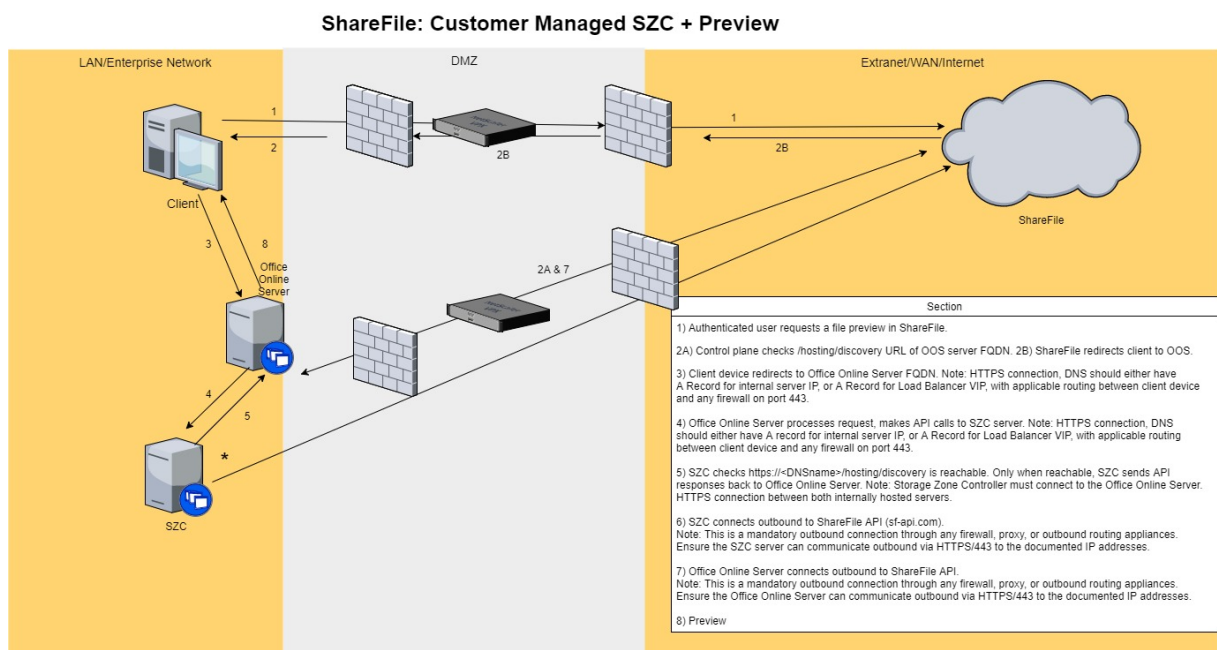
To edit on-premises files, [File Versioning](#) must be enabled on your ShareFile account.

The setting for turning on Microsoft Office Online Editing within the ShareFile Web App Advanced Preferences menu does not impact the ability to edit on-premises files. That specific toggle will **not** control your ability to edit on-premises files, but will apply to the editing of any files stored in a public cloud. Enabling the editing of on-prem files is exclusively controlled by the storage zones controller Admin using the steps outlined below.

## Microsoft server compatibility

- **Microsoft Server 2016:** supports the ability to both edit and preview files. Editing can also be disabled.
- **Microsoft Server 2013:** only supports the ability to preview files.

## Architectural and network diagram



1. Authenticated user requests a file preview in ShareFile.
2. ShareFile issues a redirect to the client device with Office Online Server FQDN
3. Client device redirects to Office Online Server FQDN.

### Note:

HTTPS connection, DNS should either have A Record for internal server IP, or A Record for Load Balancer VIP, with applicable routing between client device and any firewall on port 443.



4. Office Online Server processes request, makes API calls to storage zones controller server.

**Note:**

HTTPS Connection, DNS should either have A Record for internal server IP, or A Record for Load Balancer VIP, with applicable routing between client device and any firewall on port 443.

5. Storage zones controller checks <https://\<DNSname\>/hosting/discovery> is reachable. Only when reachable, SZC sends API responses back to Office Online Server.

**Note:**

Storage zone controller must connect to the Office Online Server. HTTPS connection between both internally hosted servers.

6. Storage zones controller connects outbound to ShareFile API (sf-api.com).

**Note:**

This is a mandatory outbound connection through any firewall, proxy, or outbound routing appliance. Ensure the storage zones controller server can communicate outbound via HTTPS/443 to the documented IP Addresses above.

7. Office Online Server connects outbound to ShareFile API.

**Note:**

This is a mandatory outbound connection through any firewall, proxy, or outbound routing appliance. Ensure the Office Online Server can communicate outbound via HTTPS/443 to the documented IP addresses above.

8. Preview occurs.

To have storage zones controller stream file bytes to OOS rather than OOS calling ShareFile control plane for downloading the contents: We need to update a key in one of the config files on the storage zones controller.

The **C:\inetpub\wwwroot\Citrix\StorageCenter\WopiServer\AppSettingsReleaseOnPrem.config** needs to be updated.

This config file has a key **downloadFileFromSC** which is currently **false**. Change the key to **true** and restart IIS.

Doing so updates the configuration. OOS also no longer calls the ShareFile control plane to download the file contents.

When using this option, would it be correct in stating there would be no inbound traffic from the control plane to OOS?

If the above option is used, OOS no longer makes outbound connections to ShareFile control plane.

However, ShareFile control plane still makes outbound connections to OOS, irrespective of whether the above option is used or not.

Are there pros or cons of using one method vs. the other?

In this approach, OOS isn't downloading file contents directly. Storage zones controller downloads and streams the file bytes to OOS. Thus, it will increase load on the storage zones controller servers.

Downloading and streaming file bytes is a resource-intensive task. Depending on the number of users and number of preview and editing operations, the load increases on storage zones controller servers.

## Enable on-premises previewing and editing

To support in-browser document and image preview, thumbnails, view-only sharing of data stored in customer-managed storage zones, and on-premises file editing, configure the storage zones controller as follows:

1. In the storage zones controller console, click the **ShareFile Data** tab.
2. In the **Local Network Share Configuration** section, enable **Configure office web apps previews**.
3. Enter the external URL of your Microsoft Office Web Apps (OWA) server.
  - Users must download and configure the OWA server software via their Microsoft Office MSDN subscription.
4. Select **Enable Office Online Editing** (if needed)
5. Verify that the OWA URL is externally accessible.
6. Verify that your Office Online Servers can communicate with **\*.sf-api.com**.
7. In the storage zones controller Console, click the **Monitoring** tab.
8. Verify that **OWA Server Connectivity** has a green checkmark.

### Note:

Editing on-premises files will require [File Versioning](#) to be enabled for the ShareFile account. If File Versioning is disabled for the account, on-premises Editing will not work.

## Important:

### Configure Clock Synchronization:

- Verify that the Time on your storage zones controller is synced with time.windows.com or another NTP server. [Click here for information on configuring clock synchronization.](#)

### **Modifying the OWA URAL or Disabling Previews:**

- Either of the above actions requires that the IIS service be restarted for each Primary and Secondary controller.

### **Limitations**

- Mobile apps do not support in-browser editing.
- Connectors do not support in-browser previews.

WOPI Previews are not supported for VDR accounts.

For information on how to configure your Citrix ADC for View-Only Sharing, see [Configure Citrix ADC for storage zones controller.](#)

### **Troubleshooting OWA and OOS issues**

If you are experiencing issues previewing or editing on-prem files, the following steps will assist in the identification and correction of specific problems.

To troubleshoot your configuration, first sign into the OWA or OOS machine.

1. Verify that the Office WebApps or OfficeOnline Windows services are running within services.msc.
2. In a new browser, open the <http://localhost/hosting/discovery> page. If this page successfully loads, an XML response should be returned.
3. Run PowerShell as an Administrator and execute the following command:

`Get-OfficeWebAppsFarm`

If you receive a WARNING or ERROR message in the response, review your configuration settings for any errors or mistakes.

### **Network considerations:**

- OOS Server should be able to reach [https://\\*.sf-api.com](https://*.sf-api.com) (or .eu)
- SZC Server should be able to reach [https://\\*.sf-api.com](https://*.sf-api.com) and [https://\\*.sharefile.com](https://*.sharefile.com) (or .eu)
- SZC Server should be able to reach OOS Server <https://<CustomerOOS/OWAEndpoint>/hosting/discovery>. For example, <https://oos.sharefileexample.com/hosting/discovery>.

## Configure multitenant storage zones

March 14, 2024

A multitenant storage zone is a ShareFile storage zones controller feature that enables Citrix Service Providers (CSPs) to create and manage a single storage zone that is shared by all tenants.

If you are a CSP with a partner account provisioned by ShareFile, you can host one multitenant standard storage zone on your domain that supports an unlimited number of tenants. Using a multitenant zone enables you to:

- Provide each tenant with a unique ShareFile account and leverage all the great ShareFile features, such as custom branding, file retention preferences, and security settings.
- Maintain a single storage repository for all of your tenants.
- Onboard new customers faster and reduce the cost and management complexity of creating a separate storage zone for each customer account.

### Create a partner account

You must have a partner account before you can register a multitenant storage zone.

To create a partner account, you must register with the CSP program and order a stocking SKU with your preferred distributor that entitles you to offer ShareFile as a service.

If you are already registered as a CSP and have ordered the appropriate ShareFile for CSPs stocking SKU a partner account has already been created for you. If you are unable to locate this new partner account, please contact ShareFile Account Services at [acctsvcs@sharefile.com](mailto:acctsvcs@sharefile.com).

As you begin to provision customer accounts under your CSP ShareFile offering, we recommend creating a generic service account admin user on your partner account. In this way, the admin user can be the official partner admin of all of your customer accounts. Ensure that this service account admin user has the Manage Tenants permission turned on. With that, we encourage partners to create this partner admin now before filling out the CSP customer account request form (in step 4).

### Install and set up a Multi-Tenant storage zone

- Create a new multitenant storage zone and associate it with your partner account. For details, see [Install storage zones controller and create a storage zone](#).
- Install the storage zone controller in multitenant mode. Be sure to run the following specified command prompt in the Install article mentioned in the preceding step.

```
msiexec /i StorageCenter\\_5.0.1.msi MULTITENANT=1
```

**Note:**

In the preceding command, you might need to update the version number (5.0.1 in the example) to match the number of the msi you are trying to install.

## **Configure the new storage zone and associate it with your partner account**

For details, see step 10 in [Install storage zones controller and create a storage zone](#).

Log into your partner account where you want to register the new zone.

**Important:**

This account must have the following ShareFile permissions: Manage Tenants and Create and Manage Zones.

You can now log in to your partner account and see the new multitenant storage zone. Click the **Admin settings > Storage zones > Partner-managed** tab.

## **Request Tenant Accounts for the multitenant zone**

To request tenant accounts, fill out the [CSP Customer Account Request form](#).

When you request a tenant account, you must also specify a Partner Admin user. This partner admin must be an admin user on your partner account with the Manage Tenants permission enabled. When a tenant account is created, this partner admin user will be automatically provisioned on the account as an Admin user and will be able to sign in and manage the tenant account. Since there cannot be two users on an account with the same email address, the partner admin email specified on the form cannot be the same as the customer admin on the same form.

To ensure the quickest turnaround, ensure that you provide the correct Org ID and the multitenant zone name that you want to use as the storage zone for the tenant account.

You will receive an email after Citrix provisions the requested accounts. The email will include details on the tenant subdomain and an activation link to set up access. ShareFile will send you and your customers' administrative users separate emails.

Your customers can then begin using ShareFile. Any new users provisioned to a tenant's account will use the multitenant zone you specified as the default location for the user's files.

## **Previewing Office files and PDFs with an Office Online Server**

This functionality is supported with supported Office Online Server environments. [Click here for setup information](#).

## Connector sharing

This functionality is supported with multitenant zones.

## Manage tenants

Within the partner account, there is a Tenant Management dashboard located under **Admin Settings > Advanced Preferences**. This centralized dashboard allows you to check the status of all tenants linked to your partner account. The dashboard includes the license consumption, default storage zone, storage consumption, and account status (Paid or Trial) for each tenant.

### Note:

The dashboard is only available to users in your partner account that have the **Manage Tenants** user permission enabled.

## Multitenant limitations

The ShareFile Information Rights Management feature (IRM) is not supported for multitenant storage zones.

## Troubleshooting

### Failed to create zone: Forbidden

Upon storage zone registration, if you receive the following error: “Failed to create zone: forbidden”, check that your user permissions include the “Manage Tenants” permission.

## Upgrade

March 14, 2024

### Upgrade storage zones controller 5.10 or later to the latest version

#### Notes:

ShareFile recommends taking a snapshot of the server before the update and backup the Storage Zone Server configuration. To learn how to back up the storage zone configuration, see [Back up a primary storage zones controller configuration](#)

For issues with upgrading your storage zones controller, see [Troubleshooting ShareFile Storage Zone Controller Upgrades](#).

Upgrade storage zones controller 5.10 utilizing the following steps.

1. Download the latest version of the Storage Zone controller Software from the [ShareFile download page](#).

**Note:**

Storage zone controllers are unavailable during the upgrade and server reboots. To avoid a data loss, we recommend scheduling a maintenance window with users. Let them know the zone is unavailable for file transfers during the upgrade.

2. Install the MSI file on the Windows server that has the storage zone controller installed. If you have multiple servers, the update should be installed first on the primary server and then on the others. There are two ways to identify which server is the primary server:

- a) Identify the primary storage zones controller from the **Configuration** page:

- On a controller server, navigate to <http://localhost/configservice/login.aspx> or start the configuration tool from the Start menu. The permission to “create and manage zones” is required to access the configuration.
- On the **Data** tab, check the Primary Zone Controller field. The field lists the primary zone controller’s server host name as <http://server/ConfigService>.



The screenshot shows a configuration interface with two fields. The first field is labeled "Zone: \*" and has a dropdown menu with "Private Zone" selected. The second field is labeled "Primary Zone Controller: \*" and has a text input containing "http://localhost/ConfigService/". Both fields have a question mark icon to their right.

Note the localhost in <http://localhost/ConfigService> indicates this server is the primary zone controller.

- b) Identify the primary storage zones controller from the Registry:

- On a controller server, open Registry Editor (regedit.exe).
- Locate the Registry key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter
- Verify the key value [isPrimaryConfigServer](#) is true.

3. Start the upgrade on the primary storage zone controller:

- a) Run StorageCenter.msi to start the ShareFile storage zones controller Setup wizard.
- b) Respond to the prompts. When the installation completes, the wizard displays the message “Completed Citrix ShareFile storage zones controller Setup Wizard.”

- c) Restart the server.
4. On each secondary storage zone controller (if needed):
  - a) Run StorageCenter.msi to start the ShareFile storage zones controller Setup wizard.
  - b) Respond to the prompts and then select **Finish**.
  - c) Restart the server.
5. On all storage zone controllers, restart the IIS server of all zone members.
  - a) Launch the CMD prompt and Run as Administrator.
  - b) Type `iisreset` then hit the **Enter** key. If successful, the prompt indicates “Internet services successfully restarted.”
  - c) Verify the registry settings on the primary storage zones controller are correct after the upgrade.
6. After the upgrade installation, choose to Launch the storage zones Configuration page on any zone member to log in and modify any configuration settings.
  - To return to the storage zones controller console at any time, open <http://localhost/configservice/login.aspx>. After you click **Finish** or return to the storage zones controller console, the Logon page opens.

**Note:**

Keep in mind that in order to login to the storage zone controller configuration page, you need to use an application specific password. If you need to create a new application specific password, see the following support article: [Create an application specific password](#).

- To change any of the displayed information, select **Modify**, make your changes, and select **Save**.

**Note:**

Verify data transfers to each storage zone controller are functional before ending the maintenance window.

## Manage storage zones controllers

August 10, 2021



After you install your primary and any secondary storage zones controllers, use the following procedures to manage the controllers and prepare them for disaster recovery.

To open the storage zones controller console, go to <http://localhost/configservice/login.aspx> or start the configuration tool from the Start menu.

## Manage storage zones controller

- [Join a secondary storage zones controller to a storage zone](#)
- [Change the address or passphrase of a primary storage zones controller](#)
- [Demote and promote storage zones controllers](#)
- [Disable, delete, or redeploy a storage zones controller](#)
- [Transfer files to a new network share](#)
- [Back up a primary storage zones controller configuration](#)
- [Recover a primary storage zones controller configuration](#)
- [Replace a primary storage zones controller](#)
- [Prepare storage zones controller for file recovery](#)
- [Recover files and folders from your ShareFile Data backup](#)
- [Reconcile the ShareFile cloud with a storage zone](#)
- [Configure antivirus scans of uploaded files](#)
- [Migrate ShareFile Data](#)
- [Connector favorites](#)

## Join a secondary storage zones controller to a storage zone

July 9, 2019

To configure a storage zone for high availability, connect at least two storage zones controllers to it. To do that, you must:

1. Install a primary storage zones controller and create a zone (as described in [Install a storage zones controller and create a storage zone](#)).
2. Install storage zones controller on a second server and join that controller to the same zone.

### **Storage zones controllers belonging to the same zone must use the same file share for storage.**

In a high availability deployment the secondary servers are independent, fully functioning storage zones controllers. The storage zones control subsystem randomly chooses a storage zones controller to handle operation requests, including upload, download, copy, and delete operations.

If the primary server goes offline, you can easily promote a secondary server to primary. You can also demote a server from primary to secondary.

1. Open a web browser on the server to be a secondary storage zones controller. Then open <http://localhost/configservice/login.aspx>, and log on.
2. Click **Join existing zone** and select the storage zone.
3. Enter the requested information and then click **Register**.

For primary zone controller, you can enter just the host name or IP address, and ShareFile will fill in the full URL. To test a URL, enter it into the browser's address field. If the URL is correct, a ShareFile banner page appears. For standard zones: If the URL is incorrect and you specified https, verify that you are using valid, trusted public SSL certificates.

4. If you are using a proxy server for the primary storage zones controller, specify the proxy server for the secondary controller, as described in [Specify a proxy server for storage zones](#).
5. Restart the IIS server of all zone members.

A secondary storage zones controller inherits the configuration of the primary controller during startup.

## Change the address or passphrase of a primary storage zones controller

September 15, 2021

### Note:

Only the account administrator can make address or passphrase changes.

### To specify a different external or local address for a primary storage zones controller

You can change the external address of a primary storage zones controller by using this procedure or other server management tools.

1. On the primary storage zone controller server, open the **Configuration Page** or navigate to: <http://localhost/configservice/login.aspx>.
2. Login to Configuration Page with ShareFile administrator credentials.
3. On the Data tab select **Modify**.
4. Specify the new **External Address** or **Local Address** and then select **Save Changes**.
5. Repeat steps on all zone members.

6. Restart the IIS server of all zone members.

## To change the passphrase of a primary storage zones controller

### Note:

The current passphrase is needed to change the passphrase of a storage zones controller.

1. Open the storage zones configuration page: <http://localhost/configservice/login.aspx>.
2. Click **Modify**.
3. Specify a passphrase to be used to protect your file encryption key. Be sure to archive the passphrase and encryption key in a secure location.

The passphrase is not the same as your account password and cannot be recovered if lost. If you lose the passphrase, you cannot reinstall storage zones, join additional storage zones controllers to the storage zone, or recover the storage zone if the server fails.

### Note:

The encryption key appears in the root of the shared storage path. Losing the encryption key file immediately breaks access to all storage zone files.

4. If you changed the passphrase on the primary server: Log on to the storage zones configuration page for each of the other members and enter the passphrase when prompted.

You must use the same passphrase for each storage zones controller in a zone.

5. Restart the IIS server of all zone members.

## Demote and promote storage zones controllers

July 30, 2020

In a high availability deployment the secondary servers are independent, fully functioning storage zones controllers. To maintain or replace a primary storage zones controller, demote it first and then promote a secondary controller. If the primary server goes offline, you can promote a secondary server to primary.

### Caution:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use

of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. To demote a primary storage zones controller:

- a) Locate the Registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
- b) Set `isPrimaryConfigServer` to false.
- c) Set `PrimaryConfigServiceUrl` to the URL of the server that will be the new primary storage zones controller, using the form `https://IPAddress` or `https://hostname/ConfigService/`.
- d) Restart the IIS server of all zone members.

2. To promote a secondary storage zones controller:

- a) Locate the Registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
- b) Set `isPrimaryConfigServer` to true.
- c) Set `PrimaryConfigServiceUrl` to `http://localhost/ConfigService/`.
- d) Restart the IIS server of all zone members.

3. Modify all additional secondary storage zones controllers:

- a) Locate the Registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
- b) Set `PrimaryConfigServiceUrl` to the URL of the server that will be the new primary storage zones controller using the form `https://IPAddress` or `https://hostname/ConfigService/`.
- c) Restart the IIS server of all zone members.

## Disable, delete, or redeploy a storage zones controller

February 17, 2023

### To disable a storage zones controller

**Note:**

Use this procedure if each storage zones controller has a different external address. Disable a controller from the Citrix ADC interface if you use the same external address for all storage zones controllers.

Disable a storage zones controller before taking the server off-line for maintenance.

1. In the ShareFile web interface, click **Admin** and then click **Storage zones**.
2. Click the zone name and then click the storage zones controller host name.
3. Clear the enabled check box and then click **Save Changes**.
4. Restart the IIS server of all zone members.

### To delete a storage zones controller

Deleting a storage zones controller does not delete the data or SCKeys.txt. If you are deleting a primary storage zones controller, demote it before continuing.

1. In the ShareFile web interface, click **Admin** and then click **Storage zones**.
2. Click the zone name and then click the storage zones controller host name.
3. Click **Delete**.
4. Restart the IIS server of all zone members.

### To redeploy a storage zones controller

No information is lost when you redeploy a storage zones controller.

1. Uninstall storage zones from the server.
2. In the ShareFile web interface, click **Admin > Storage zones**, and then select your zone. Do not delete the zone.
3. Select the storage zones controller and delete it.
4. Install storage zones. Do not register it yet.
5. Run the storage zones controller configuration wizard to join the storage zones controller to a zone and complete the registration.
6. Restart the IIS server of all zone members.

## Transfer files to a new network share

July 8, 2020

Before setting up a new network share for private data storage:

## Requirements

- Storage zones controllers belonging to the same storage zone must use the same file share for storage.
  - Storage zones controllers access the share using the IIS Account Pool user. By default, application pools operate under the Network Service user account, which has low-level user rights. A storage zones controller uses the Network Service account by default.
  - The Network Service account must have **full** access to this storage location.
  - Disable storage zone controllers for new uploads before transferring any data to the new share. In the web application, navigate to **Admin Settings > StorageZones**. Select the zone name. Under **Storage Centers**, select each host server. To terminate traffic to each host server, deselect the option **Enabled** under **Server Settings**.
1. Open the storage zones configuration page: <http://localhost/configservice/login.aspx>.
  2. Click **Modify**.
  3. In **Storage Location**, enter the UNC path to your network share, in the form `\\server\share` and then click **Save**.

### Caution:

Storage zones controller overwrites any data in this path with a proprietary storage format. As a best practice, never specify a path to a location with file data. Reserve this storage location for storage zones for ShareFile Data only.

4. If the credentials for the UNC path of your new network share location differ from the previous one, specify the Storage Logon and Storage Password.
5. Restart the IIS server of all zone members.
6. Log in to the configuration page of all zone members.
7. Copy the entire directory structure, including SCkeys.txt, to the new server.

## Back up a primary storage zones controller configuration

June 14, 2023

A storage zones controller is installed on your local site and you are responsible for backing it up. To fully protect your deployment, you should take a snapshot of the storage zones controller server, back up your configuration, and [Prepare storage zones controller for file recovery](#).

It is critical that you back up your configuration as described in this topic. For example, if you do not have a backup and someone accidentally deletes a zone, you cannot recover the folders and files in that zone.

**Important:**

Be sure to use PowerShell 4.0 for this procedure. For more information about PowerShell requirements, see PowerShell scripts and commands in [storage zones controller system requirements](#).

The storage zones controller installer includes a PowerShell module with commands that back up and restore a primary storage zones controller configuration settings. Your backup includes configuration information for zones, storage zones for ShareFile Data, storage zone connector for SharePoint, and storage zone connector for Network File Shares.

The backup and restore commands require that you run the 32-bit version of PowerShell under the same user context as the storage zone controller. To set the user context, use the tool PSEXec. That tool is available for download from <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>.

**Note:**

These steps do not apply to a secondary storage zones controller. To recover a secondary storage zones controller, reinstall the storage zone controller on the server and then join the server to the primary storage zones controller.

1. The PowerShell script used in this procedure is unsigned, so you are required to change your PowerShell execution policy.

- a) Determine if your PowerShell execution policy allows you to run local, unsigned scripts:

```
PS C:\>Get-ExecutionPolicy
```

For example, a policy of RemoteSigned, Unrestricted, or Bypass allows you to run unsigned scripts.

- b) To change your PowerShell execution policy: PS C:\>Set-ExecutionPolicy RemoteSigned

2. Set the user context for this PowerShell session. In a command window, run one of the following commands.

- If using the default Network Service account:

```
PsExec.exe -i -u "NT AUTHORITY\NetworkService"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell
```

- If using a named user for the storage zones controller application pool:

```
PsExec.exe -i -u "domain\username"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell
```

A PowerShell window opens.

3. From the PowerShell prompt, import the module ConfigBR.dll: `Import-Module C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll`

You are required to import the module each time you open a new PowerShell window.

4. From the PowerShell prompt, run the Get-SfConfig command and complete the following prompts:

- **PrimaryZoneController** - Example inputs:
  - Connect to a local server: `http://localhost/ConfigService/`
  - Connect to a remote server: `http[s]://myservername.domain.com/ConfigService/`
  - Connect to a remote server if DNS issues prevent connection to a server name: `http[s]://10.40.37.5/ConfigService/`
- Passphrase - The passphrase specified for the storage zone controller.
- FilePath - Example `c:\szc-backup.bak`

Command parameters:

Parameters	Description	Examples
“server”	The primary storage zones controller server name or IP address. It can be in any of the following forms shown under Examples and must include the trailing slash.	Connect to a local server: <code>http://localhost/ConfigService/</code> ; Connect to a remote server: <code>http[s]://myservername.domain.com/ConfigService/</code> ; Connect to a remote server if DNS issues prevent connection to a server name: <code>http[s]://10.40.37.5/ConfigService/</code>
“passphrase”	The passphrase specified for the storage zone controller.	“MyPassphrase”
“fullpath”	A location to save the backup file.	“c:\szc-backup.bak”

The **Get-SfConfig** command creates the backup file.



To restore a primary storage zones controller configuration, see [Recover a primary storage zones controller configuration](#).

## Recover a primary storage zones controller configuration

June 7, 2021

### Important:

- Be sure to use PowerShell 4.0 for this procedure. For more information about PowerShell requirements, see the PowerShell scripts and commands in [Storage zones controller system requirements](#).
- For more information on implementing TLS system wide, see the Microsoft article on [How to enable TLS 1.2 on clients](#).

Storage zones controller provides these options for disaster recovery when a primary storage zones controller is deleted or fails:

- If a secondary storage zones controller is available, promote the secondary controller to a primary one.
- If a secondary storage zones controller is not available and you backed up your primary storage zones controller configuration (as described in [Back up a primary storage zones controller configuration](#)), recover the primary storage zones controller from the backup file.
- If you do not have a backup of your primary storage zones controller configuration and all of your storage zones controllers are accidentally deleted or become unusable, only partial recovery is possible. You can recover zones and the configuration for storage zones for ShareFile Data, but not storage zones connectors.

### To recover a primary storage zones controller from a backup file

#### Note:

These steps apply only to a primary storage zones controller. To recover a secondary storage zones controller, reinstall the storage zones controller on the server and then join the server to the primary storage zones controller.

1. The PowerShell script used in this procedure is unsigned, so it might be necessary to change your PowerShell execution policy.

- a) Determine if your PowerShell execution policy allows you to run local, unsigned scripts:  
`PS C:\>Get-ExecutionPolicy`  
For example, a policy of RemoteSigned, Unrestricted, or Bypass allows you to run unsigned scripts.
  - b) To change your PowerShell execution policy: `PS C:\>Set-ExecutionPolicy RemoteSigned`
2. Set the user context for this PowerShell session. In a command window, run one of the following commands.

**Note:**

Download PsExec.exe from <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec> and follow the installation instructions on that page.

- If using the default Network Service account:

```
1 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\  
SysWOW64\WindowsPowerShell\v1.0\powershell  
2 <!--NeedCopy-->
```

- If using a named user for the storage zones controller application pool:

```
1 PsExec.exe -i -u "domain\username" C:\Windows\SysWOW64\  
WindowsPowerShell\v1.0\powershell  
2 <!--NeedCopy-->
```

A PowerShell window opens.

3. From the PowerShell prompt, import the module ConfigBR.dll: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

You are required to import the module each time you open a new PowerShell window.

4. From the PowerShell prompt, run the `Set-SfConfig` command: `Set-SfConfig -PrimaryZoneController "server"-Passphrase "passphrase"-FilePath "fullpath"`

Where:

- server is the primary storage zones controller server name or IP address. It can be in any of the following forms and must include the trailing slash.

`http://localhost/ConfigService/`

`servername/` or `serverip/` (if you use HTTP)

`http[s]://servername.domain.com/ConfigService/`

```
http[s]://serverip/ConfigService/
```

- passphrase is the one specified for storage zones controller.
- fullpath is the backup file location and name. For example, `c:\szc-backup.bak`.

## To recover a primary storage zones controller without a backup file

If you do not have a backup file, you can recover zones and the configuration for storage zones for ShareFile Data, but not storage zones connectors.

1. Set the user context for this PowerShell session. In a command window, run one of the following commands.

- If using the default Network Service account:

```
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\
SysWOW64\WindowsPowerShell\v1.0\powershell
```

- If using a named user for the storage zones controller application pool:

```
PsExec.exe -i -u "domain\username" C:\Windows\SysWOW64\WindowsPowerShell
\v1.0\powershell
```

A PowerShell window opens.

2. From the PowerShell prompt, import the module ConfigBR.dll: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

You are required to import the module each time you open a new PowerShell window.

3. From the PowerShell prompt, run the Join-SfConfig command:

### Important:

The Join-SfConfig command currently does not support Azure or Amazon S3 storage. Contact ShareFile support if you need to use this command.

```
1 Join-SfConfig -ShareFileUserName "ShareFileUserName" -
  ShareFilePassword "ShareFilePassword" -subdomain "subdomain.
  sharefile.com" -ZoneId "ZoneId" -SCID "StorageCenterId" -
  Passphrase "passphrase" [-StorageZoneLocation "
  StorageZoneLocation"] [-StorageUsername "StorageUserName"] [-
  Storagepass "StoragePassword"] [-AzureAccountName "
  StorageAccount"] [-AzureSecretKey "PrimaryOrSecondaryAccessKey"
  ] [-AzureContainerName "Container"] [-S3AccessKey "S3AccessKey"
  ] [-S3SecretKey "S3SecretKey"] [-S3ContainerName "
  S3ContainerName"] [-S3EndpointAddress "S3EndpointAddress"] [-
  S3ForcePathStyle]
2 <!--NeedCopy-->
```

Where:

- ZoneID can be obtained as follows:
  - a) In the ShareFile web interface, click **Admin > Storage zones**, right-click the site name, and then choose **Properties**.  
  
The address displayed ends with the zone ID that looks like this: `zae4fb8c-8520-478f-8f87-aa589a8fd181`.
  - b) Copy and paste that ID into the Join-SfConfig command.
- StorageCenterId can be obtained as follows:
  - a) In the ShareFile web interface, click Admin > storage zones, click the site name, right-click the host name, and then choose Properties.  
  
The address displayed ends with the storage ID that looks like this: `scd344cf-8043-4ce2-974b-8f9cd83e2978`.
  - b) Copy and paste that ID into the Join-SfConfig command.
- StorageZoneLocation is needed only if storage zones for ShareFile Data are enabled for the zone.
- StorageUsername and StoragePassword are needed only if storage zones for ShareFile Data are enabled for the zone and your storage location requires authentication.
- AzureAccountName, AzureAccessKey, and AzureContainerName are needed only if storage zones for ShareFile Data are stored in a Windows Azure storage container.

4. To recover storage zones connectors, use the storage zones controller console (<http://localhost/configservice/login.aspx>) to enable and configure connectors.

## Replace a primary storage zones controller

July 9, 2019

To replace a primary storage zones controller with one that is in a different location, such as on a different domain, use the backup and restore procedures. The following steps ensure that your configuration settings and all of your data is transferred.

1. Create a backup file for your existing storage zones controller configuration. See [Back up a primary storage zones controller configuration](#).
2. Install, but do not configure, a storage zones controller in the new network location.

3. Import the backed-up configuration onto the new controller. See [Recover a primary storage zones controller configuration](#).
4. Copy your data to the new network share, log on to the configuration console for the new storage zones controller, and enter the new storage path information. See [Transfer files to a new network share](#).
5. In the new storage zones controller configuration console, update the external URL of the controller. See [Change the address or passphrase of a primary storage zones controller](#).

## Prepare storage zones controller for file recovery

August 15, 2023

### Warning:

The ShareFile recovery feature does not automatically back up your persistent storage location. You are responsible for choosing a backup utility and running it every 1 to 7 days.

How you prepare for file recovery depends on where your data is stored:

- **A supported third-party storage system** —If you use a third-party storage system with storage zones controller, your third-party storage is redundant and a local backup is not required. However, be aware that a ShareFile user who deletes a file has the ability to recover the file from the Recycle Bin for a brief period. A file cannot be recovered from the ShareFile Recycle Bin after 45 days. After the recovery period, the file is removed from the zone and therefore from the redundant third-party storage. If that recovery time is not adequate, consider one of these solutions:
  - To prevent StorageZone Controller File Cleanup service from purging the actual file from your on premise storage location, change the value of the **Period** setting in `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\SCFileCleanSvc\\FileDeleteService.exe.config`. For more information, refer to [Customize storage cache operations](#). Keep in mind that increasing the retention time also increases the amount of third-party storage needed.
  - Create a local back up your StorageZone files every seven days and determine the appropriate retention policy for the backups.
- **On-premises storage** —If you use a locally-maintained share for private data storage, you are responsible for backing up your on-premises storage zones controller local file storage and registry entries. ShareFile archives the corresponding file metadata that resides in the ShareFile cloud for 3 years.

Important: To protect against data loss, it is critical that you take a snapshot of your storage zones controller server,

[back up its configuration](#), and back up your local file storage.

After you prepare your storage zones controller for file recovery as described in this topic, you can use the ShareFile Administrator console to:

- Browse your storage zones for ShareFile Data records for a particular date and time and then tag any files and folders that you want to restore. ShareFile adds the tagged items to a recovery queue. You then run a recovery script to restore the files from your backup to the persistent storage location.

For more information, refer to [Recover files and folders from your ShareFile Data backup](#).

- Reconcile the metadata stored on the ShareFile cloud with your on-premises storage when you cannot recover data from your on-premises storage. The ShareFile reconcile feature permanently removes from the ShareFile cloud the metadata for files that are no longer in a storage zone on a specified date and time.

For more information, refer to [Reconcile the ShareFile cloud with a storage zone](#)

## Prerequisites

- A dedicated physical or virtual machine with 2 CPUs and 4 GB RAM
- Windows Server 2012 R2 (Datacenter, Standard, or Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows PowerShell (32-bit and 64-bit versions) must support .NET 4 runtime assemblies. For more information, refer to “PowerShell scripts and commands” in [storage zones controller system requirements](#).
- PsExec.exe - PsExec enables you to launch PowerShell using the network service account. You can also use PsExec to schedule recovery tasks. Download PsExec.exe from <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec> and follow the installation instructions on that page.

## Summary of files used for disaster recovery

The following files, located in C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery, are used for disaster recovery.

File name	Description
DoRecovery.ps1	PowerShell script executed by Windows Task Scheduler to handle the recovery process. This file stores the file backup and storage locations.
Recovery.psm1	PowerShell module that handles the recovery queue operations.
recovery.log	Log file that stores the output of a recovery process.
recoveryerror.log	Log file that stores the errors in the recovery process.
LitJson.dll	A .Net library to handle conversions from and to JSON (JavaScript Object Notation) strings.

### To set up the backup folder

On the backup server, create the folder where you will back up the persistentstorage folder.

The storage zones for ShareFile Data file backup should follow the same layout as the storage zones controller persistent storage.

If your backup location does not follow the same layout as the storage zones controller persistent storage, you must perform an additional step during the recovery process to copy files from the backup location to the location that you specify in the Recovery PowerShell script.

Storage layout

Backup layout

```

1  \\\\PrimaryStorageIP
2  \\StorageLocation
3  \\persistentstorage
4  \\sf-us-1
5  \\a024f83e-b147-437e-9f28-e7d03634af42
6  \\fi3d85dc\\_1d6c\\_49b0\\_8faa\\_1f36ef3d83b5
7  \\fi7d5cbb\\_93c8\\_43f0\\_a664\\_74f27e72bc83
8  \\fi47cd7e\\_64c4\\_47be\\_beb7\\_1207c93c1270
9
10 \\\\BackupStorageIP
11 \\BackupLocation
12 \\persistentstorage
13 \\sf-us-1
14 \\a024f83e-b147-437e-9f28-e7d03634af42
15 \\fi3d85dc\\_1d6c\\_49b0\\_8faa\\_1f36ef3d83b5
16 \\fi7d5cbb\\_93c8\\_43f0\\_a664\\_74f27e72bc83
17 \\fi47cd7e\\_64c4\\_47be\\_beb7\\_1207c93c1270

```

```
18 <!--NeedCopy-->
```

**Important:**

The ShareFile recovery feature does not automatically back up your persistent storage location.

**You are responsible for choosing a backup utility and running it every 1 to 7 days.**

**To create a disaster recovery queue**

This one-time setup is required. The following command examples use the default storage zones controller installation folder.

1. On the storage zones controller, run PowerShell as an administrator.
2. The PowerShell script used in this procedure is unsigned, so you might need to change your PowerShell execution policy.

- a) Determine if your PowerShell execution policy allows you to run local, unsigned scripts:  
PS C:\>Get-ExecutionPolicy

For example, a policy of RemoteSigned, Unrestricted, or Bypass allows you to run unsigned scripts.

- b) To change your PowerShell execution policy: PS C:\>Set-ExecutionPolicy RemoteSigned
3. To verify that PowerShell has the correct CLRVersion, type:

\$psversiontable

The value for CLRVersion must be 4.0 or higher to enable PowerShell to load .NET assemblies in scripts. If it is not, change it for both Windows PowerShell 32-bit and 64-bit versions as follows:

- a) Run NotePad as an administrator.
- b) Create a file with the following content.

```
1 <?xml version="1.0"?>
2 <configuration>
3   <startup useLegacyV2RuntimeActivationPolicy="true">
4     <supportedRuntime version="v4.0.30319"/>
5     <supportedRuntime version="v2.0.50727"/>
6   </startup>
7 </configuration>
8 <!--NeedCopy-->
```

- c) Choose File > Save As, name the file powershell.exe.config, and save it to the following locations:

C:\Windows\System32\WindowsPowerShell\v1.0

C:\Windows\SysWOW64\WindowsPowerShell\v1.0



- d) Close the PowerShell window, open a new one as administrator, and type `$psversiontable` to verify that the CLRVersion is correct.
4. Close the PowerShell window and launch PowerShell using PsExec.exe as follows:
  - a) Open a Command Prompt window as administrator.
  - b) Navigate to the location of PsExec.exe and enter:  
`PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\p`
  - c) Click Agree to accept the PsExec.exe license agreement.
5. Navigate to the Disaster Recovery tools folder in the storage zones controller installation folder:  
`cd 'C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery'`
6. Import the Recovery.psm1 module:  
`Import-Module .\Recovery.psm1`
7. To create the recovery queue, enter: `New-SCQueue -name recovery -operation recovery`  
  
The output of that command includes the name of the queue created. For example: Queue 92736b5d-1cff-4760-92c8-d8b04dc92cb2 created  
  
To view the new folder, open a file browser and navigate to:  
  
`\\server\(Your Primary Storage Location)\Queue`. You will see the Queue folder, such as 92736b5d-1cff-4760-92c8-d8b04dc92cb2.
8. Customize the recovery PowerShell script for your location, as described in the next section.

## To customize the recovery PowerShell script for your location

The DoRecovery.ps1 PowerShell script is executed by the task scheduler to handle the recovery process. This file includes the file backup and storage locations which you must specify for your site.

1. On the storage zones controller, navigate to the recovery PowerShell script:  
`C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery\DoRecovery.ps1`
2. Edit the script as follows:
  - a. Set the `$backupRoot` parameter to point to the UNC path of your backup location. For example: `$backupRoot = "\\10.10.10.11\(YourBackupLocation)\persistentstorage"`
  - b. Set the `$storageRoot` parameter to point to the UNC path of your storage zones controller persistent storage. For example: `$storageRoot = "\\10.10.10.10\StorageLocation\persistentstorage"`

**To test the recovery process**

1. Create a test file and upload it to ShareFile.
2. After a hour or so, verify that the file appears in persistent storage (in the path specified for \$backupRoot).
3. Delete the file from ShareFile: In the ShareFile administrator tool, click **Recycle Bin**, select the file, and then click **Delete Permanently**.
4. Delete the file from the persistent storage.

This step recreates the action that ShareFile would perform 45 days after the file is deleted.

5. In the ShareFile administrator tool, go to **Admin > Storage zones**, click the zone and then click **Recover Files**.
6. Click in the **Recovery Date** text box and select a date and time before the file was deleted and after it was uploaded.

The file list for the storage zone on the specified date and time appears.

7. Select the check box for the file.
8. Select the folder to contain the restored files and then click **Restore**.

The file is added to the recover queue and is ready to be restored. When the file is recovered successfully, the screen changes to show the folder that now contains the recovered file.

9. To recover the file:
  - a. Open a Command Prompt window as administrator.
  - b. Navigate to the location of PsExec.exe and then type:

```
1  `` `
2  PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
   \WindowsPowerShell\v1.0\powershell
3  <!--NeedCopy--> `` `
```

- c. In the PowerShell window, navigate to:

```
cd C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery
```

- d. Run the recovery script:

```
.\DoRecovery.ps1
```

The PowerShell window will include the message “Item recovered”. The file is added to the persistent storage location.

10. Download the restored file from the ShareFile web site.

## Related PowerShell commands

The following PowerShell commands support disaster recovery.

- **Get-RecoveryPendingFileIDs**

Gets the list of file IDs needed for recovery. For syntax and parameters, use this command:

Get-Help Get-RecoveryPendingFileIDs -full

- **Set-RecoveryQueueItemsStatus**

Sets a status for all or specified items in the recovery queue. This overwrites the existing recovery status in the queue. For syntax and parameters, use this command:

Get-Help Set-RecoveryQueueItemsStatus -full

## To create and schedule a task for recovery

In the event a scheduled recovery task is needed, follow the steps below.

1. Start Windows Task Scheduler and in the **Actions** pane click **Create Task**.
2. On the **General** tab:
  - a. Type a meaningful name for the task.
  - b. Under **Security options**, click **Change User or Group**, and specify the user to run the task, either Network Service or a named user that has write permissions to the storage location.
  - c. From the **Configure for** menu, select the operating system of the server where the task will be run.
3. To create a trigger, on the **Triggers** tab, click **New**.
4. For **Begin the task**, choose **On a schedule** and then specify a schedule.
5. To create an action, on the **Actions** tab, click **New**.
  - a. For **Action**, choose **Start a program** and specify the full path to the program. For example: `C:\Windows\System32\cmd.exe`.
  - b. For **Add arguments**, type: `/c "c:\windows\syswow64\WindowsPowerShell\v1.0\PowerShell.exe -File .\DoRecovery.ps1" >> .\recovery.log 2>>.\recoveryerror.log`
  - c. For **Start in**, specify the Disaster Recovery folder in the storage zones controller installation location. For example: `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

### Delete Service Default Period

As of StorageZone Controller 4.0, the Delete Service timer will be set to 45 days. The 45 day default period will overwrite any previous settings. To modify the default period, edit FileDeleteService.exe.config at C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc

```
<!--No. of days to keep data blob in active storage after deletion-->  
  
<add key="Period"value="45"/>
```

### Modify Delete Service Default Period After Upgrade

In some upgrade scenarios, the DeletePeriod value will be set to null in the “FileDeleteService.exe.config”. When set to null, the Delete Period will default to 45 days, the default number of days before a file that has been deleted from ShareFile is removed from physical storage.

To modify the DeletePeriod on the storage zones controller, edit the FileDeleteService.exe.config file at the following location: C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config

Upon a clean installation of the storage zones controller, the Delete Service will run every 8 hours to clean up temporary files and folders. To modify the timer, edit the FileDeleteService.exe.config file at the following location: C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config

## Recover files and folders from your ShareFile Data backup

July 9, 2019

The ShareFile Administrator console enables you to browse your storage zones for ShareFile Data records for a particular date and time and tag any files and folders that you want to restore. ShareFile adds the tagged items to a recovery queue. You can then run the provided script to restore the files from a backup to the storage location.

#### Important:

Be sure to use PowerShell 4.0 for this procedure. For more information about PowerShell requirements, see the PowerShell scripts and commands in [Storage zones controller system requirements](#).

## Prerequisites

- Complete the setup and testing described in [Prepare storage zones controller for file recovery](#). The setup includes instructions for creating a folder to contain the recovered files.

1. In the ShareFile web interface, click **Admin** and then click **Storage zones**.
2. Click the zone name and then click **Recover** Files.
3. Click in the **Recovery Date** text box and select a date and time.

The file list for the storage zone on the specified date and time appears.

4. Select the check box for each file to restore and then click Restore.
  5. Select the folder to contain the restored files and then click Restore.
- The folder list shows a spinning icon to indicate that the recovery is in process.
6. If your backup location does not follow the same layout as the storage zone persistent storage, copy the files from the backup location to the location you specified when editing DoRecovery.ps1.
  7. The DoRecovery.ps1 PowerShell script is unsigned, so you might need to change your PowerShell execution policy for this procedure.

- a) Determine if your PowerShell execution policy allows you to run local, unsigned scripts. In a PowerShell window: `Get-ExecutionPolicy`

For example, a policy of RemoteSigned, Unrestricted, or Bypass allows you to run unsigned scripts.

- b) To change your PowerShell execution policy: `Set-ExecutionPolicy RemoteSigned`
8. Set the user context for this PowerShell session. In a command window, run one of the following commands.

- If using the default Network Service account:

```
1 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\
  SysWOW64\WindowsPowerShell\v1.0\powershell
2 <!--NeedCopy-->
```

- If using a named user for the storage zones controller application pool:

```
1 PsExec.exe -i -u "domain\username" C:\Windows\SysWOW64\
  WindowsPowerShell\v1.0\powershell
2 <!--NeedCopy-->
```

A PowerShell window opens.

## 9. Recover the file:

- a) Open a Command Prompt window as administrator.
- b) Navigate to the location of PsExec.exe and enter:

```
1 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\  
SysWOW64\WindowsPowerShell\v1.0\powershell  
2 <!--NeedCopy-->
```

- c) In the PowerShell window, navigate to:

```
cd C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster  
Recovery
```

- d) Run the recovery script:

```
.\DoRecovery.ps1
```

The PowerShell window will include the message “Item recovered”. Recovered files are copied from the backup to the persistent storage location. After you refresh the console, the spinning icons disappear from the ShareFile web interface for files successfully recovered.

If a file that is deleted from the ShareFile web application has not yet been deleted by the storage zones controller delete service, the file is still in the persistent storage location. In that case, file recovery is immediate and a spinning icon does not appear in the ShareFile web interface.

If you cannot recover a file, refer to the help file provided in the Disaster Recovery folder.

## Reconcile the ShareFile cloud with a storage zone

July 9, 2019

A problem, such as a disk failure, that causes data loss in your local storage results in an inconsistent state between your local storage and the metadata stored in the ShareFile cloud. You can automatically reconcile those differences so that metadata for files no longer in your storage zone on a specified date and time are permanently removed from the ShareFile cloud.

**Caution:**

Perform a reconcile only if you have irrecoverable data loss in your local file storage. A reconcile permanently erases the metadata from the ShareFile cloud for any files that are not found in your local file storage as of the date and time that you specify.

1. Click **Admin** and then click **Storage zones**.
2. Click the zone name and then click **Reconcile Files**.

3. Click in the **Reconcile Date** text box and select a date and time.
4. Click **Reconcile**. A confirmation dialog box appears.

## Windows Server 2012R2 Migration Guide for ShareFile storage zones

August 29, 2023

### Important:

Microsoft is ending support for Windows Server 2012R2 on October 10, 2023. It is important to migrate your server to a newer version before the end of support date.

This article provides guidance on how to migrate your ShareFile Storage Zone server from Windows Server 2012R2 to a newer version.

To migrate to a newer version of Windows Server, you must add a secondary storage zone controller to the new server and then promote it as the primary controller.

### System requirements

The Storage Zones Controller Server supports the following versions:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

### Instructions

#### Note:

The following steps **DO NOT** cover migrating the ShareFile Data Repository. If you have the ShareFile Data Repository on the same server as the storage zone controller you are planning to migrate or have a storage zone data repository on a File Server running Windows Server 2012R2 to migrate, see [Transfer files to a new network share](#) for more information.

### Step 1 - Prepare the new server for the ShareFile Storage Zone Controller

Prepare the new server using the steps provided in [Prepare your server for ShareFile data](#).

## **Step 2 - Install the Storage Zone Controller on the new server and add it as Secondary**

After preparing the new server for ShareFile, you need to add it to the storage zone as a secondary server. See [Join a secondary storage zones controller to a storage zone](#) for more information.

## **Step 3 - Promote the new server to Primary, demote the old server to Secondary**

After adding the new server as secondary, the next step is to promote it to primary. The older server must also be demoted to secondary. For more information on this step, see [Demote and promote storage zones controllers](#).

### **Note:**

ShareFile recommends that you test the functionality of the new storage zone server on its own, without using the older server as a secondary. You can do this by temporarily disabling the older server. For more information, see [To disable a storage zone controller](#)

## **Step 4 (optional) - Add additional secondary servers**

If necessary, for each additional secondary server, return to [Step 2 - Install the Storage Zone Controller on the new server and add it as Secondary](#).

## **Step 5 (optional) - Update NetScaler service group members**

If you have a NetScaler, ensure the new storage zone servers are added to the ShareFile service group. See [To add members to a service group by using the configuration utility](#) for more information.

## **Step 6 - Delete the old storage zone controller server from the ShareFile Admin Portal**

Once the Storage Zone servers have successfully migrated, the older servers can be deleted from the ShareFile Admin Portal. See [To delete a storage zones controller](#) for more information.

## **Configure antivirus scans of uploaded files**

February 18, 2022

### **Important:**

Due to updates to the application code in StorageZones 4.2, some customers must update the



permission level the tool runs at from local administrator to system network service. Failing to update permissions will result in antivirus scans failing to start.

## Requirements / Summary

- User utilizing StorageZones Controller 4.2 or later
- SFAntivirus must be run as a Network Service using PSEXec
- Update log file location

### Run SFAntivirus as a Network Service using PSEXec:

Clients updating to SZ 4.2 or later with existing scheduled tasks linking to SFAntivirus need to change the user level that the tool runs at from local administrator to system network service.

To obtain Network Service Rights, use PSEXec to launch PowerShell (x86) under the same user context as the storage zones controller and obtain Network Service Rights using the following command:

```
PSEXec.exe -i -u "NT AUTHORITY\NetworkService" C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell
```

### Update log file location

Administrators must also change log file location by editing log4net.config entry, if they were logging to a directory outside of the default SZC log directory, by modifying the following line:

```
<file value="..\..\SC\\logs\\avscantool-"/>
```

Storage zones controller installation includes several files that support antivirus scans. The files are installed by default in C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus.

After you customize the configuration file and use the Windows Task Scheduler to schedule the scans, as described in the following steps, each file upload request causes the storage zones controller to queue the file for an antivirus scan. If issues are reported for a scanned file, the Folders view includes a warning icon for the file. If a user tries to download the file, a warning message appears.

As of StorageZones Controller 4.0, the antivirus log file location can be configured. To modify the log location, edit the SFAntivirus.exe.config file at C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus.

The antivirus scan does not remove the file.

Use of the ICAP protocol with antivirus scanning platforms that have been coded to the RFC standard for ICAP is supported on StorageZones Controller 4.2 or later. Information on configuring an ICAP AV can be found further down in this article.

**Note:**

After configuring antivirus on your zone, any newly uploaded items are scanned. Antivirus configuration is not retroactive. Configuring it does not scan files and items that already exist on the zone.

## To prepare the configuration for your location

1. To run virus scans on a server other than the storage zones controller:

- a) Copy the folder C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus to the other server.
- b) On the storage zones controller, open C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.c and set QueueSDKRestricted to 0: `<add key="QueueSDKRestricted" value="0" />`

2. On the server where you run virus scans, edit SFAntiVirus.exe.config with the values for your storage zones controller configuration:

- a) For CommandFile: Specify the full path to the antivirus software. That software must reside on the same server as the ShareFile antivirus folder.
- b) For CommandOptions and return codes: The command line settings provided in the configuration file are an example. Provide the appropriate settings for your antivirus software and environment.
- c) For ScanFileTimeout: Larger files can take longer to scan. Tune this setting according to the file sizes expected in your storage. **Otherwise, this could increase the risk of a large file not getting scanned.**

3. In a command line window, run the following command to set up virus scans: `SFAntiVirus.exe -register SFusername SFpassword`

## Use ICAP for AV scans instead of command line tools

Storage zones controller 5.3 and later support the use of the ICAP protocol with antivirus scanning platforms that have been coded to the RFC standard for ICAP. Customers can still use the CLI method if they want. This feature is supported for tenant zones as of storage zones controller 5.0.1 and later.

To enable an ICAP AV scanner on your storage zone controller, navigate to the storage zones controller configuration page.

Select the **Enable Antivirus Integration** check box and enter the address of your antivirus server in the **ICAP RESPMOD URL** field. This is the URL of the ICAP response modification service: **ICAP://SERVER/RESPMOD**.

Click **Test Connectivity** to confirm your setting.

## To create and schedule a task for virus scans

### Note:

Creating scheduled tasks for virus scans is only necessary when utilizing command line tools. This is not required when utilizing ICAP.

1. Start the Windows Task Scheduler, and in the **Actions** pane click **Create Task**.
2. On the **General** tab:
  - a) Provide a meaningful name for the task.
  - b) Under **Security** options, click **Change User or Group**, and specify a Windows user to run the task. The user must have full access permission on the storage location.
  - c) Select **Run whether user is logged on or not**. Leave the **Do not store password** check box cleared.
  - d) Select **Run with highest privileges**.
  - e) From the **Configure for menu**, select the operating system of the server where the task will be run.
3. To create a trigger: On the **Triggers** tab, click **New**. Then, for **Begin the task**, choose **On a schedule** and specify a schedule.
4. To create an action: On the **Actions** tab, click **New**.
  - a) For **Action**, choose **Start** a program and specify the full path to the program. For example:  
`C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus\\SFAntiVirus.exe`
  - b) For **Start in**, specify the location of SFAntiVirus.exe: `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus`
5. On the **Settings** tab, for **If the task is already running**, then the following rule applies, choose **Do not start a new instance**.

## AV command-line integration into Scan Service

### Prerequisites

- Before installing or upgrading storage zones controller 5.2, ensure that you stop or delete the existing command-line AV if it is running as a scheduled task or a cron.
- Install .NET 4.6.2 (or later) on a host machine.

The Scan Service in the on-premises storage zones controller includes support for using a command-line AV Tool, like the Symantec command-line AV Scan. In addition, the Scan Service provides scans with ICAP supported antivirus products.

To enable this feature, add the following configuration key and value in the AntiVirus/OnPrem/AVScanService/AVScanService/appSettings.config

```
<add key="use-command-line-av" value="true"/>
```

### Command-line tool specific configuration

The upgrade or new installation of storage zones controller 5.2 includes a new configuration file:

AntiVirus/OnPrem/AVScanService/AVScanService/avCommandLineSettings.json

This file handles the necessary settings for the AV command line.

The configuration key values are explained below with example values included.

- Set this point to your command-line app.

```
"command-file": "c:\\\\vscan\\\\scan.exe"
```

- Check the documentation for the command-line app to see what options or switches it supports and then add them in this location.

```
"command-options": "/ALL /ANALYZE /MIME /NOMEM /NORENAME /SECURE",
```

- Include the output values that indicate a clean scan.

```
"scanner-codes-for-clean-file": "0, 19",
```

- Include output values that indicate infected file.

```
"scanner-codes-for-infected-file": "12, 13",
```

- Include output values that indicate not scanned files.

```
"scanner-codes-for-notscanned-file": "2, 6, 8, 15, 20, 21, 102"
```

## Notes on enforcing max file size, excluding extensions

Before version 5.2, you could not enforce extension exclusion or maximum file size enforcement on the command-line AV. You could only do so on the ICAP Scan service. With version 5.2, the same settings that applied to the ICAP scan service regarding excluded extensions and max file size in bytes apply to the AV command-line service.

These settings were named as:

```
<add key="icap-exclude-extensions"value=""/>
```

```
<add key="icap-max-file-size-bytes"value="0"/>
```

A new installation of storage zones controller 5.2 renames these settings to the following. The renamed settings reflect the fact that they are applicable both to ICAP-based AV and to the command-line AV.

```
<add key="exclude-extensions"value=""/>
```

```
<add key="max-file-size-bytes"value="0"/>
```

On an upgrade, these settings are not renamed. Although manual renames work, the same settings would also work for the AV command line in addition to ICAP.

```
<add key="icap-exclude-extensions"value=""/>
```

```
<add key="icap-max-file-size-bytes"value="0"/>
```

## Migrate ShareFile data

September 17, 2021

There are multiple ways to migrate ShareFile data from one on-premises zone to another.

- Migrate via Web Portal or User Management Tool
- Migrate via PowerShell Script
- Migrate via ZoneFix Tool

## Prerequisites

- Make sure that the source zone is reachable from the destination zone and unblock the outbound connections to the source Storage Center.
- To test the connection between zones, access the source zone's external address by navigating to it in a browser on the destination zone. If the connection is successful, the ShareFile logo appears.

## Migrate via Web Portal or User Management Tool

In the ShareFile web application, you can initiate the migration of data between zones for an individual user, or for a specific folder.

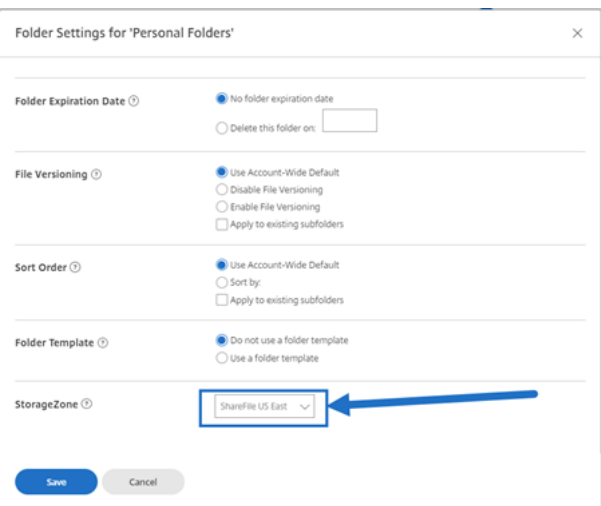
### Important:

Saving the following changes immediately triggers an asynchronous migration operation to upload existing files to the new zone. New files uploaded to the folder during this migration period proceeds to the new zone.

**Migrate data for a specific user** - Navigate to **People**, then locate the **Employee** user. Click the user to view their profile page. Under **Storage Location**, select a new zone (if one has already been installed and configured.)



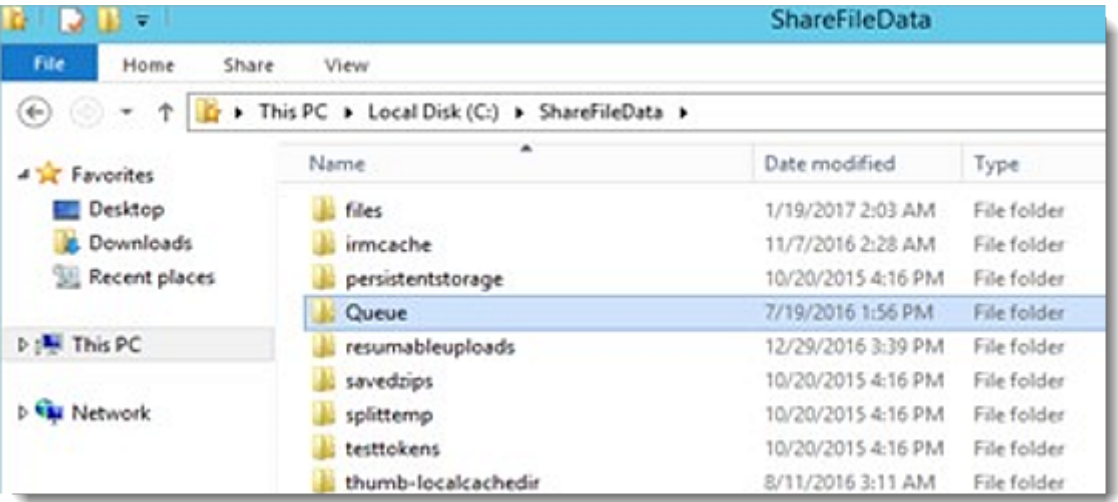
**Migrate data for a specific folder** - Navigate to the folder and access the **More Options** menu to the right of the folder name. Click **Advanced Folder Settings**. Using the menu, select a new zone.



## Migration process

First, files queued for migration create a placeholder file in a **Queue** folder within the **Storage Location** of the original zone.

Once the placeholder file is successfully processed, the migrated file is deleted from the `persistentstorage` of the original zone and added to the `persistentstorage` of the new zone.



### Migrate via PowerShell

The ShareFile PowerShell SDK allows users to download large folder structures from their original zone location and upload those folders to a new zone.

**Requirements** - PowerShell 4+ and .NET 4.x+ is required to run and install the SDK. PowerShell 5.x can be downloaded [here](#) as part of the Windows Management Framework 5.1.

### Migrate via Zone Fix tool

The Zone Fix tool is a command line tool. Written by storage zones developers, the tool leverages the ShareFile API to target folder IDs for migration to a specific zone.

For optimal performance, this method is recommended for folders less than 2 GB in size.

### Connector Favorites

September 1, 2021

As of storage zones controller 5.0, users can make connector folders as Favorites under **Network Shares**, **SharePoint**, and **Documentum Connectors** within the ShareFile WebApp. For details, see this Citrix Support Knowledge Center [article](#).

Adding a Connector Folder to your Favorites is supported on ShareFile Mobile.

## Manage storage zones for ShareFile data

October 2, 2023

You can use storage zones for ShareFile Data with or instead of the ShareFile-managed cloud.

### Note:

If you are deleting a primary storage zone controller, demote it before continuing. For more information, see [Demote and promote storage zone controllers](#).

## Move home folders and File Boxes between zones

Use the following steps to move home folders and File Boxes between zones. Alternatively, use the ShareFile User Management Tool to migrate users between zones.

1. Click **Home** and then navigate to the folder.
2. In the right navigation pane, click **Edit Folder Options**.
3. From the storage zone menu, select a zone and then click **Save**.

## Create a folder in a storage zone

1. Click **Home** and then click **Folders**.
2. On the **Folder** tab, click **Add Folder**.
3. Specify the folder information. For **Storage Site**, select the storage zone where you want this folder and its contents to be stored.
4. Click **Create Folder**.
5. Configure the folder as usual. When you create a folder, you can choose whether to use the ShareFile-managed cloud storage or your local storage zone.

## Rename or delete a storage zone

### Important:

Before deleting a storage zone, back it up. Deleting a zone erases all files and folders in that zone and you cannot undo the operation.

1. Click **Admin** and then click **Storage zones**.
2. Click the zone name.
  - To rename the zone: Click **Edit Zone**, type a new name, and then click **Save Changes**.
  - To delete the zone: Click the zone name and then click **Delete Zone**.



## Limitations

Storage zone controllers cannot be renamed/deleted if:

- **ShareFile data migration is in progress** - Complete the data migration before attempting to delete the storage zone.
- **ShareFile data exists on the zone** - Migrate or delete all existing data before attempting to delete the Storage Zone.

## Customize storage cache operations

ShareFile user requests are managed with the storage zones controller. This includes: file uploads, downloads, and deletions. The storage zones controller then communicates with the connected storage. For example, if the connected storage is a supported third-party storage system and a ShareFile user uploads a file, the ShareFile client sends the file to the persistent storage cache. Storage zones controller then uploads the file to the third-party storage system.

Storage zones controller manages the persistent storage cache using configurable settings in `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`. The settings that are specific to a supported third-party storage system are noted in this discussion.

For uploaded files:

- Storage zones controller places uploaded files in a persistent storage cache (the PersistentStorage folder).
- The following settings control the timing of delete service operations:
  - `MinDeletionAge` specifies the minimum time span between when a file was last accessed and when it can be deleted. Defaults to 1 day. Minimum setting is 8 hours.
  - `OffPeakTimeOfDayStart` and `OffPeakTimeOfDayEnd` specify the start and stop times for file deletion. Defaults to 2 a.m. and 4 a.m.
  - `ProducerTimerInterval` and `DeleteTimerInterval` control the frequency of delete service operations. Please contact support if the default values (1 day) are not appropriate for your site.
- The delete services also manages folders that contain temporary items such as encryption keys and queued files. The delete service removes those items 24 hours after they are created.
- For supported third-party storage systems only:
  - The delete service determines whether a file in the storage cache has a corresponding blob in the supported third-party storage.

- By default, every 10 seconds (`CheckSizeThresholdTimer`) the delete service determines if the storage cache has exceeded a disk threshold of 10 GB (`DiskSpaceDropoutThreshold`). If the threshold is exceeded, the delete service removes files that have not been accessed in the past hour (`CacheCleanupFileThresholdPeriodUnexpected`). Delete service runs as the result of normal scheduling (and not because the disk size reached the threshold). The service deletes files that have not been accessed in the past 24 hours (`CacheCleanupFileThresholdPeriodNormal`) if the blob is in supported third-party storage. If the blob is not in the third-party storage, the file remains in the storage cache.

For downloaded files:

- When storage zones controller receives a download request, it downloads the file from the persistent storage cache if the file is there. If the file is not in that cache, the controller downloads the file from the third-party storage system to the persistent storage cache. The delete service removes files that have not been accessed for the past 24 hours (`CacheCleanupFileThresholdPeriodNormal`).

For deleted files:

- The delete service gets from the ShareFile application a list of files that were deleted 45 days ago (`Period`).
- The delete service then removes the corresponding files from the storage location or the corresponding objects from the third-party storage.

## Delete Service default period

The Delete Service timer is set to 45 days. The 45 day default period overwrites any previous settings.

### Note:

If the delete period is configured to less than 45 days, please contact support to reduce the number of days items are displayed in **Recycle Bin** so both time frames are equal.

1. To modify the default period, edit `FileDeleteService.exe.config` at `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`
  - `<!--No. of days to keep data blob in active storage after deletion-->`
  - `<add key="Period"value="45"/>`

## Create and manage storage zone connectors

March 16, 2021

Storage zone connectors provide access to documents and folders in:

- SharePoint sites, site collections, and document libraries
- Network file shares
- [Documentum connector \(requires SZC 4.1 or later\)](#)

Users with permission to view a connected resource can browse connected SharePoint sites, SharePoint libraries, and network file shares from the ShareFile web interface and ShareFile clients.

By default, connector browsing is disabled for the ShareFile web interface. To enable connector browsing, contact ShareFile Support.

Additional settings are available that allow users to specify which Domain controller to use for Active Directory look-ups. [Please refer to the Authentication section of this article](#). This setting requires SZ 4.1 or later.

### Connector System Requirements

Storage zone connectors do not support document sharing or folder sync across devices.

**Connectors must have a unique display name.** Users are blocked from using a connector name that is currently in use elsewhere on the account.

## Permissions to create storage zone connectors

To create and manage connectors, your Admin or Employee user **must have the following permissions**:

- **Create and Manage connectors**
- **Create root-level folders**

## To create a storage zone connector for SharePoint

### Prerequisites

- If you are using storage zones for ShareFile Data, create the zone to be used for the connector.

The following steps describe how to create a storage zone connector from the ShareFile web interface. ShareFile users can also create a connector from supported devices by typing the URL of the SharePoint site.

1. Sign in to your ShareFile account as an administrator with the Create and Manage connectors permission.
2. Navigate to **Admin Settings > connectors**.
3. Click **Add** for the SharePoint connector type.
4. If you are using storage zones for ShareFile Data, choose a Zone for the connector.

The zone for a connector must either be in the same domain as the SharePoint server or must have a trust relationship with it. If you have SharePoint servers in multiple domains and cannot configure trusts between the domains, create a storage zones controller for each domain.

5. For Site, specify the URL of a SharePoint root-level site, site collection, or document library, in the following forms.

- Example connection to a SharePoint root-level site: <https://sharepoint.company.com>

A connection to a root-level site gives users access to all sites (but not site collections) and document libraries under the root-level. ShareFile hides SharePoint system folders from users.

- Example connection to a SharePoint site collection: <https://sharepoint.company.com/site/SiteCollection>

A connection to a site collection gives users access to all subsites within that collection.

- Example connection to a SharePoint 2010 document library:

- <https://mycompany.com/sharepoint/>
- [https://mycompany.com/sharepoint/sales-team/Shared Documents /](https://mycompany.com/sharepoint/sales-team/Shared Documents/)
- <https://mycompany.com/sharepoint/sales-team/Shared Documents /Forms/AllItems.aspx>

- Example connection to a SharePoint 2013 document library:

The default SharePoint 2013 URL (when Minimal Download Strategy is enabled) is in the form: [https://sharepoint.company.com/\\\\_layouts/15/start.aspx\\#/Shared%20Documents/](https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/).

- Example connection that redirects to the NetBIOS name of an authenticated user:

Use the variable %UserDomain% to substitute the logon name of the authenticated user with the NetBIOS name of that user. The new variable enables you to create a site-level connector to a URL such as [https://example.com/%UserDomain%\\\\_%UserName%/Documents](https://example.com/%UserDomain%\\_%UserName%/Documents).

- Example connection when connecting to “My Site” or OneDrive for Business:

Use the variable `%URLusername%` to automatically resolve select special characters when connecting to SharePoint personal sites. This variable replaces spaces with `%20` and periods with underscores. Usage of the `%URLusername%` variable requires SZ v3.4.1.

If the user’s “domain\username” is “acme\rip.van winkle” then

`https://sharepoint.acme.com/personal/%URLusername%`

will be resolved to:

`https://sharepoint.acme.com/personal/rip van%20winkle`

6. Type a user-friendly name for the connector.

The name is used to identify the SharePoint site to users. The name should be brief so it displays well on mobile devices with small screens.

7. Click **Add connector**. The **View/Edit Folder Access** dialog box appears.

8. To make connectors visible to others: In View/Edit Folder Access, add users and distribution groups and then click **Save Changes**.

This step determines only whether a connector is visible to users. **Storage zone connectors inherit access permissions from the SharePoint server.**

## To enable SharePoint metadata tagging

When configuring the storage zones controller, ensure that SharePoint connectors are enabled.

Metadata tagging is supported for SharePoint 2013 and later mobile clients.

### Note:

For `en-us` only.

## To create a storage zone connector for network file shares

### Prerequisites

- If you are using storage zones for ShareFile Data, create the zone to be used for the connector.
- In order for network share connectors to work with the latest versions of Chrome, Edge, and Firefox browsers, apply the latest .NET update for your environment. For more information, see [KB articles that support SameSite in .NET Framework](#). Apply this to all of your storage zone connectors. This is necessary to allow the SameSite attribute to be set for cookies considering the latest version of the browsers.

- If you use version 5.10.1 or lower, add `<httpCookies sameSite="None"requireSSL="true" /` within `<system.web>` tag of `C:\inetpub\wwwroot\Citrix\StorageCenter\cifs\Web.config` file in all storage zone connectors. This is necessary to allow the SameSite attribute to be set for cookies considering the latest version of the browsers.

The following steps describe how to create a connector from the ShareFile Web interface. ShareFile users can also create a connector from supported devices by typing the path of a file share.

1. Log on to your ShareFile account as an administrator with the Create and Manage connectors permission.
2. Navigate to **Admin Settings > Connectors**.
3. Click **Add** for the Network Shares connector type.
4. If you are using storage zones for ShareFile Data, choose a Zone for the connector.

The zone for a connector must either be in the same domain as the file share or must have a trust relationship with it. If you have file shares in multiple domains and cannot configure trusts between the domains, create a storage zones controller for each domain.

5. For Path, type the UNC path.

Example with FQDN: `\\fileserver.acme.com\shared`

You can use the following variables in the UNC path:

- `%UserName%`

Redirects to a user's home directory. Example path: `\\myserver\homedirs\%UserName%`

- `%HomeDrive%`

Redirects to a user's home folder path, as defined in the Active Directory property Home-Directory. Example path: `%HomeDrive%`

- `%TSHomeDrive%`

Redirects to a user's Terminal Services home directory, as defined in the Active Directory property ms-TS-Home-Directory. The location is used when a user logs on to Windows from a terminal server or Citrix XenApp server. Example path: `%TSHomeDrive%`

In the Active Directory Users and Computers snap-in, the ms-TS-Home-Directory value is accessible on the Remote Desktop Services Profile tab when editing a user object.

- `%UserDomain%`

Redirects to the NetBIOS domain name of the authenticated user. For example, if the authenticated user logon name is "abc\johnd", the variable is substituted with "abc". Example path: `\\myserver\%UserDomain%\_%UserName%`

The variables are not case sensitive.

Important: Do not create a connector to the ShareFile Data storage location. Depending on user permissions, doing so can enable users to remove all ShareFile Data.

6. Type a user-friendly Name for the connector.

The name is used to identify the file share to users. The name should be brief so it displays well on mobile devices with small screens.

7. Click Add connector. The View/Edit Folder Access dialog box appears.

8. To make connectors visible to others: In View/Edit Folder Access, add users and distribution groups and then click Save Changes.

This step determines only whether a connector is visible to users. **Storage zone connectors inherit access permissions from the network share. Permissions for read/write access are determined by the security settings of the network share and are also affected by the ShareFile plan.**

## To enable file checkin and checkout for network file shares

### Prerequisites

Storage zones controller version 5.8 and Network File Shares connector must be configured.

### Steps

1. Sign in to Storage Center. The configuration page appears.
2. Click **Modify** on the configuration page.
3. Select the check box **Enable check in and check out for network file shares**.
4. Type the name of the domain where the users and network shares are located.
5. Type the user name and password of the service account. This service account is required to have read and write access on all files and folders present in the network share location.

## To create a storage zone connector for Documentum

### Note:

Only Basic Authentication is supported for Documentum connector setup. The Documentum Content Server is case sensitive, so the user name entered during authentication should match the case-sensitive credentials, unless case sensitivity is disabled on the Documentum content server.

## Prerequisites

1. Storage zones controller 5.3 or later
2. Documentum ECM Setting enabled by ShareFile Customer Support.
3. The Documentum Rest service must be deployed on your Documentum server. [Click here for additional information on the Documentum Rest Service.](#)
4. If using Citrix ADC, certain configuration changes are required. Those changes are detailed further down this article.

Once this feature has been enabled by ShareFile Customer Support, navigate to your storage zone controller and locate the storage zones connector menu. Click the check box for “Enable access to existing Enterprise Content Management (ECM) data sources.” Save your changes.

Next, sign into the ShareFile web application and navigate to **Admin Settings > Connectors**.

Click the **Add** button beside the Documentum connector type.

Specify the Path of your EMC server and enter a Name for your connector. Continue.

Next, grant users access to the Documentum connector.

Once the connector has been created, you can access it from the web and mobile apps.

## Supported actions

Mobile (iOS/Android/Universal Windows Platform):

- Browsing
- File Uploads/Downloads
- File and Folder Creation/Deletion
- Offline editing

WebApp

- connector Creation
- Browsing
- File Uploads/Downloads
- Folder Creation/Deletion

## Not supported

- Sharing files stored within a Documentum connector
- Whitelisting/Blacklisting of paths



**Note:**

The Documentum Content Server is case sensitive, so the user name entered during authentication should match the case-sensitive credentials, unless case sensitivity is disabled on the Documentum content server.

## Citrix ADC configuration for Documentum connector

If utilizing a Citrix ADC with your environment, make the following change to your Citrix ADC configuration:

1. Append the following to the \_SF\_CIFS\_SP policy under Content Switching > Policies:

```
HTTP.REQ.URL.CONTAINS("/cifs/") || HTTP.REQ.URL.CONTAINS("/sp/") ||  
HTTP.REQ.URL.CONTAINS("/documentum/") || HTTP.REQ.URL.CONTAINS("/  
ProxyService/")
```

2. Append the following to the \_SF\_SZ\_CSPOL policy under Content Switching > Policies:

```
HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("/sp  
/").NOT && HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT && HTTP.  
REQ.URL.CONTAINS("/documentum/").NOT
```

## To change a connector name

A connector name is used to identify a SharePoint site or network file share to users.

1. Sign in to your ShareFile account as an administrator and then click the connectors tab.
2. In the **Title** column, click the connector name.
3. Type a user-friendly name for the connector and then click **Save**.

## To delete a connector

Deleting a connector does not remove data from SharePoint or a network file share.

1. Sign in to your ShareFile account as an administrator and then click the connectors tab.
2. Select the check box for the connector, click **Delete**, and then click **OK**.

## Connector authentication

Admin users can now utilize the following setting to specify which Domain controller to use when performing AD look-ups for CIFS or SP authentication.

```
<add key="Domaincontrollers"value="DC01,dc02.domain.com,123.456.789.1"/>
```

The “Value=” above can be set to a single DC or multiple DCs identified by host name, FQDN, or IP Address. Multiple DCs should be separated by commas or semicolons.

If multiple DCs are specified, the look-up will be executed against the first DC. If an error occurs, the second DC is utilized, and so on.

The above property can be added to `C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config` so that it will be inherited by all storage zones controller IIS apps (including CIFS, SP, and ProxyService).

If the new app setting is not present, the default behavior of automatically selecting a DC continues.

### **Get a direct link from Network Share / SharePoint connectors**

Users can now “Get a Direct Link” from Network Share / SharePoint connectors while using the latest version of the ShareFile app for iOS or Android.

If the Admin would like to disable this feature, they can do so by adding:

```
<add key="disable-direct-link"value="1"/>
```

The above can be added to `C:\inetpub\wwwroot\Citrix\StorageCenter\sps\AppSettingsRelease.config`.

### **Basic authentication and localized user names**

Basic Authentication does not support non-ASCII characters. If using localized user names, it is suggested that users utilize NTLM and Negotiate.

## **Data Loss Prevention**

March 26, 2024

Data Loss Prevention (DLP) features in ShareFile let you restrict access and sharing based on the content found within a file.

You can scan the documents uploaded to your storage zone using any third-party DLP security suite that supports ICAP, a standard network protocol for inline content scanning. Then you adjust the sharing and access privileges based on the results of the DLP scan and your preferences for how strictly you want to control access.

## Supported DLP systems

Storage zones controller uses the ICAP protocol to interact with third-party DLP solutions. Using ShareFile with an existing DLP solution requires no changes to existing policies or servers. You might want, however, to dedicate ICAP servers for processing ShareFile data if you expect the load to be significant.

Popular ICAP-compliant DLP solutions include:

- Symantec Data Loss Prevention
- McAfee DLP Prevent
- Websense TRITON AP-DATA

Because ShareFile uses your existing DLP security suite, you can maintain a single point of policy management for data inspection and security alerts. If you already use one of the preceding solutions for scanning outgoing email attachments or web traffic for sensitive data, you can point the ShareFile storage zones controller to the same server. For these existing DLP systems, we also support secure ICAP (ICAPS) if the underlying DLP system itself supports ICAPS.

## Enable DLP

To enable DLP for ShareFile and storage zones controller, perform the following three actions:

1. Enable DLP capabilities on your ShareFile account.
2. Enable DLP on your storage zones controller server.
3. Configure the allowed actions for each file classification.

These actions are described in detail in the following sections.

### Enable DLP capabilities on your ShareFile account

To request or confirm that your ShareFile subdomain is enabled for DLP, send a request to [Citrix Support](#).

For some accounts, enabling DLP might also require enabling a newer user experience for the ShareFile website. After your account is enabled for DLP, you can proceed with enabling DLP on your storage zones controller server.

### Enable DLP on your storage zones controller server

Use the following steps to configure DLP settings on your storage zones controller deployment:

1. Install or upgrade to storage zones controller 5.3 or later.

2. In the storage zones controller console [http://\\*localhost\\*/configservice/login.aspx](http://*localhost*/configservice/login.aspx), click the **ShareFile Data** tab. Click **Modify** if the zone exists.
3. Select the **Enable DLP Integration** check box and type the ICAP address of your DLP server in the **ICAP REQMOD URL** field. The address format is:

```
1  icap://\<*name or IP address of your DLP server*\>:\<*port*\>/reqmod
2
3  OR
4
5  *icap://\<name or IP address of your DLP server\>:\<port\>/reqmod
6      *
7  The default ICAP port is 1344 (non-secure DLP) and the default
8      ICAPS port is 11344 (secure DLP).
9  For example, if your DLP server is dlp-server.example.com, type
10     the following into the ICAP REQMOD URL field:
11  icap://*dlp-server.example.com*:1344/reqmod
12
13  OR
14
15  *icap://dlp-server.example.com:11344/reqmod*
16  <!--NeedCopy-->
```

4. Click **Save** or **Register**.

After enabling DLP, confirm that the DLP server is reachable by checking the **DLP ICAP Server Status** entry on the **Monitoring** tab.

## Control access based on DLP scan results

After DLP is enabled on the account and storage zones controller, every version of every file uploaded to the DLP-enabled storage zone will be scanned for sensitive content. The results of the scan are stored in the ShareFile database as a data classification.

DLP settings constrain the normal permissions and sharing controls available for files based on their DLP classification. When sharing a document, a user can still choose to block anonymous access even if DLP settings would allow them to share it anonymously. But if the user attempts to share a file in a way that would violate DLP settings, ShareFile prevents them from doing so.

The data classifications are:

- **Scanned:** OK –Files that were scanned by a DLP system and passed OK.
- **Scanned: Rejected** –Files that were scanned by a DLP system and were found to contain sensitive data.

- **Unscanned** –Files that have not been scanned.

The **Unscanned** classification applies to all documents stored in Citrix-managed storage zones or other storage zones where DLP is not enabled. The classification also applies to files in the DLP-enabled storage zones that were uploaded before DLP is configured. The classification also applies to files that are waiting to be scanned because the external DLP system is unavailable or slow to respond.

Each item's classification is determined by the ICAP server response rule. If the DLP ICAP server responds with a message that the content should be blocked or removed, the file is marked as **Scanned: Rejected**. Otherwise, the file is marked as **Scanned: OK**.

For each data classification, you can set different access and sharing restrictions. For each of the three categories, the ShareFile administrator chooses which actions to allow:

- Employees can download or share the file.
- Third-party client users can download or share the file. Client sharing is disabled by default but can be enabled under **Admin > Advanced Preferences > Allow clients to share files**.
- Anonymous users can download the file

When a user shares a file, only users with download permissions can receive the file. Therefore, when you enable the sharing permission for a data classification, you must also grant at least one class of user download permission.

### To configure DLP settings in ShareFile

1. In the ShareFile web interface, click **Admin > Data Loss Prevention**.
2. Change the option for **Limit access to files based on their content** to **Yes**.
3. Configure the allowed actions for each data classification.

#### **Important:**

The ShareFile On-Demand Sync tool requires download permissions for normal operation. Enable employee downloads for all content classifications if your deployment includes ShareFile On-Demand Sync.

When the storage zones controller sends a file to the DLP system, it includes metadata indicating the owner of the file. The file also includes the folder path where the file resides in ShareFile. This information allows the DLP server administrator to view details specific to ShareFile about files that contain sensitive content.

## Advanced settings for DLP

To adjust the DLP scanning process, edit the settings file found on your storage zones controller at `wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`. The following table describes each setting related to DLP.

Setting	Description	Default value
scan-interval	How frequently the DLP service checks the DLP queue for new files and sends them to the DLP ICAP server for processing.	30 seconds
icap-response-timeout	How long the storage zones controller waits for an ICAP response before marking the ICAP server as unavailable.	30 seconds
icap-exclude-extensions	Comma-separated list of extensions to exclude from DLP scanning. The DLP server does not process files with names ending in one of these extensions, but marks the files as Scanned: OK. Example value: "exe,jpg,bin,mov"	None
icap-max-file-size-bytes	Maximum size of file (in bytes) to send to the DLP server for processing. A value of 0 means that there is no maximum and all file sizes are sent. When configured with a non-zero value, the DLP server does not process files larger than the configured size, but are marked as Scanned: OK.	31457280 (30 MB)

Setting	Description	Default value
x-queue-items-to-process	The maximum number of queued items to scan per each scan-interval iteration. Decrease this value to mitigate the impact on your DLP server when a large number of files is added to the StorageZone.	512
max-queue-processing-threads	Maximum number of concurrent processor threads to use for draining the DLP scan queue. Set this value based on the maximum number of simultaneous connections allowed to your ICAP server. It should be within reasonable limits to avoid blocking other network services that use the same ICAP server.	4
icap-reqmod-http-request-verb	By default, network calls are made with the PUT verb. You might change this setting to POST if needed.	PUT

## **DLPExistingFiles tool**

ShareFile storage zones controller provides options to integrate the storage center with Data Loss Prevention (DLP) providers through ICAP.

ICAP services, however, work through queues which get populated only by newly created files. This means files existing in a zone before ICAP is enabled won't be scanned by the services. This tool helps queue up those files for scanning, and also can queue up scanned files for rescanning.

As the name states, the tool only works for the DLP ICAP service.

## **Requirements**

The tool is a PowerShell script and hence needs PowerShell to run. [PsExec](#) or a similar tool is also needed as the script needs to be run as Network Service for access to the network share location.

## Location

For an installed storage zones controller, the tool can be found at `<storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1`.

The storage zones controller installation location is by default `C:\inetpub\wwwroot\Citrix\StorageCenter`.

## Considerations before running the tool

The tool might need to run multiple times for a single operation depending on the following.

- The limitations provided for the queue size limit.
- The number of items for the given criteria. This consideration is true unless the queue size limit is set to zero or less. In that case, the tool assumes a maximum size of 200,000 items in the queue directory.

For instance, if the tool is being used to queue up unscanned items, the queue size limit is set at 500 items. When there are more than 500 unscanned items, the tool stops after 500 items get filled up in the queue. To track of where it stopped, the tool stores the creation date of the last retrieved item. The tool stores the date in a temporary file at `<storage zones controller installation location>\SC` with the name `DLPExistingFiles-enddate.temp`.

Before each run, the tool looks for this file. If the file is present, the tool uses the creation date in it as the marker for the next batch of files. The tool doesn't delete the temp file on completion of a certain operation. Instead, the zone administrator can delete the file once all batches for a certain operation are completed. Due to this situation, when a full operation is completed, the temporary file, if present, should be manually removed before performing another different operation.

## Running the tool with PsExec

Open a Command window and run PsExec using the following command.

```
1 PsExec.exe -i -u "nt authority\network service"  
2  
3 "C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"  
4 <!--NeedCopy-->
```

This opens up PowerShell running as Network Service. To verify that it is indeed running as Network Service, run **whoami** and check the result.

Once PowerShell is open, run the tool there directly to perform any necessary task.

```
1 <storage zones controller installation location>\Tools\DLPExistingFiles  
  \DLPExistingFiles.ps1 <options>  
2 <!--NeedCopy-->
```



## Command-line options

The following options are available for running the tool:

- **-runscan** (Required): This option is used to specify which kind of files to queue up for scanning. Suboptions:
  - **Unscanned**: Unscanned files. For example, pre-DLP era files that weren't scanned.
  - **ScannedOK**: Scanned files that have been marked as clean.
  - **ScannedRejected**: Scanned files that have been marked as not clean.
  - **Scanned**: All scanned files.
- **-queueLimit** (Optional): This option is used to specify the number of items allowed in the queue before the tool stops.
- **-date** (Optional): The maximum creation date of the items to be queued up for scanning. For instance if the date is specified as "10/30/2017 11:30 AM", only those files which were created before this date/time will be queued up for scanning.

### Examples:

For all the examples, open **PowerShell as Network Service through PsExec**. For instructions, see the steps earlier in this article.

To queue up unscanned items in a zone, run the following command.

```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
   \DLPExistingFiles.ps1 -runscan Unscanned
2 <!--NeedCopy-->
```

To queue up all scanned items within a zone with a queue limit of 100, run the following command.

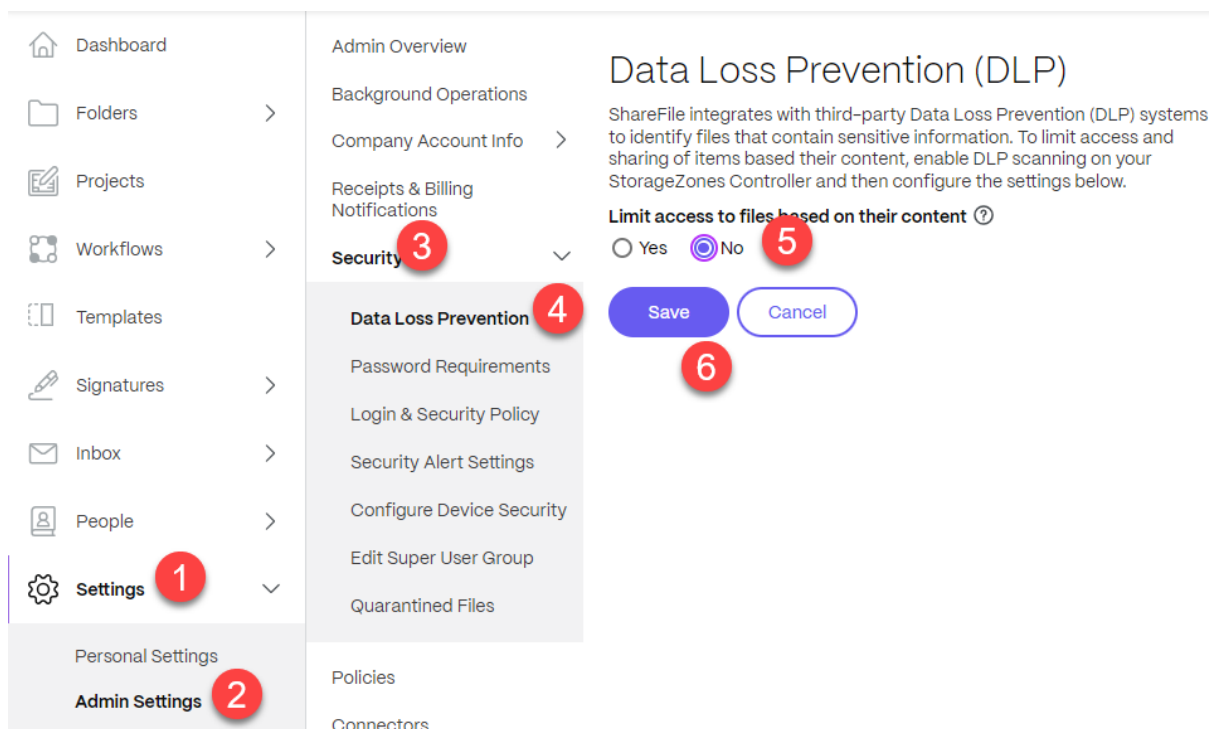
```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
   \DLPExistingFiles.ps1 -runscan Scanned -queueLimit 100
2 <!--NeedCopy-->
```

To queue up all scanned items created before 11:30 AM on 10/30/2017 with the following characteristics: marked as clean, in a zone with a queue limit of 200, run the following command.

```
1 <storage zones controller installation location>\Tools\DLPExistingFiles
   \DLPExistingFiles.ps1 -runscan ScannedOK -queueLimit 200 -date "
   10/30/2017 11:30 AM"
2 <!--NeedCopy-->
```

## Disable DLP

To disable DLP for ShareFile and storage zones controller, perform the following actions:



1. Log into your Sharefile account and click on **Settings**.
2. From the drop-down list that opens, select **Admin Settings**.
3. From the menu that opens click on **Security**.
4. From the Security menu, choose the **Data Loss Prevention** option.
5. From the DLP screen, go to the **Limit access to files based on their content** section and click on **No**.
6. Select **Save**.

## Monitor

September 10, 2021

Storage zones controller and the ShareFile administrator interface include several resources to help you monitor storage zones controller activity and troubleshoot issues:

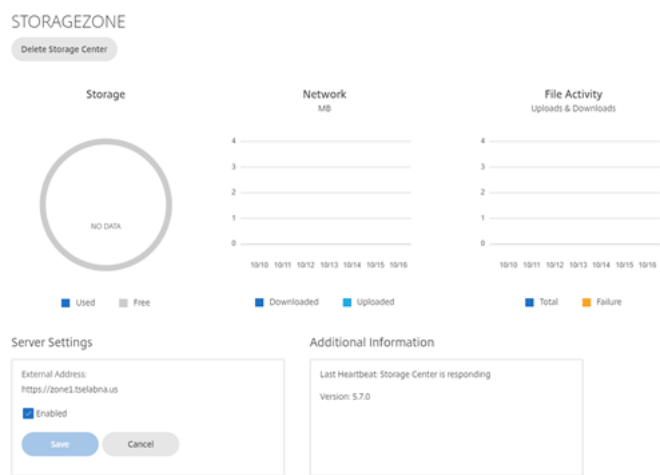
- **General component status** –The Monitoring tab on the storage zones controller console provides component status to help you start the troubleshooting process. Status is provided for items such as access permissions, service status, and Heartbeat Status, which indicates the storage zones controller outbound connectivity to the ShareFile control plane.

Storage zones controller sends updates to the ShareFile web application every 5 minutes. If the ShareFile web application does not receive an update within 10 minutes, it marks the storage

zones controller as offline.

For items on the Monitoring tab that appear in red, review the log files for detailed information. The Monitoring tab does not indicate whether a storage zone is working in terms of connectivity. This includes whether the ShareFile control plane can reach the external storage zones URL or whether a client is able to reach the zone.

- **Storage zones controller server information** –For information about the storage use, network use, and file activity of the server: From the ShareFile interface, log on to your ShareFile Enterprise account, go to **Admin > StorageZones**, click the storage zone, and then click a storage zones controller host name.

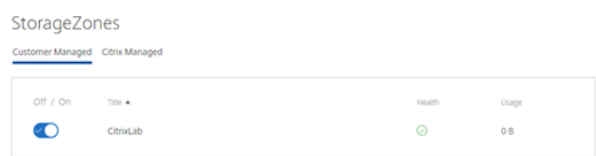


- **Zone information** –For information about the storage use, network use, and file activity for a zone: From the ShareFile interface, log on to your ShareFile Enterprise account, go to **Admin > StorageZones**, and click a zone name.



- **Storage zones controller health status** –To determine whether ShareFile.com is receiving heartbeat messages from the storage zones controllers joined to the zone, view the Health status: From the ShareFile interface, log on to your ShareFile Enterprise account, go to **Admin > StorageZones**, verify that the Health column has a green check mark, and then click the

site name to verify that the Heartbeat message indicates that the storage zones controller is responding.



- **Log files** –Log files provide detailed information about storage zones controller configuration and its components, as described in the next section.

Log files

The following log files for the storage zones controller are located by default in `C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs`:

Log file name	Contains logging information for
cfgsrv-%date%.txt	storage zones controller configuration actions, including modifying an existing storage zones configuration, creating a new Storage Zone, and joining a new storage zones controller to an existing primary storage zones controller
sc-%date%.txt	ShareFile data upload and download activity for standard zones
CIFS-%date%.txt	storage zone connectors for Network File Shares upload and download activity
sharepoint-%date%.txt	storage zone connectors for SharePoint upload and download activity
cloudstorageuploader-%date%.txt	Cloud Storage Uploader Service (to a supported third-party storage system)
copy-%date%.txt	ShareFile Copy Service
delete-%date%.txt	ShareFile Cleanup Service, for the persistent storage cache
s3uploader-%date%.txt	ShareFile Management Service. Includes heartbeat status messages

Extended logging is available for each of the following components and is useful when you need to provide detailed information to support.

---

Component	Location of AppSettingsRelease.config
ShareFile Data	C:\inetpub\wwwroot\Citrix\StorageCenter
storage zone connectors for Network File Shares	C:\inetpub\wwwroot\Citrix\StorageCenter\cifs
storage zone connectors for SharePoint	C:\inetpub\wwwroot\Citrix\StorageCenter\sp

---

### To enable extended logging

The following steps enable extended logging for all storage zones controller components and services:

1. On the storage zones controller server, open IIS.
2. Navigate to the default website and then open Application Settings.
3. Change the value for enable-extended-logging from 0 to 1.
4. Restart the Citrix ShareFile Management Service.
5. After you have resolved the issue, we recommend that you clear extended logging to reduce the amount of logging.

To enable extended logging for a particular component, edit its AppSettingsRelease.config file: Change the value of `<add key="enable-extended-logging" value="0"/>` from 0 to 1.

You can also check IIS logs to determine if traffic is reaching the storage zones controller. IIS logs show all incoming requests. IIS logs for the storage zones controller are in c:\inetpub\logs\LogFiles\W3SVC1.

To enable extended IIS logging, see <http://support.microsoft.com/kb/313437>.

### Troubleshoot installation and configuration

---

Issue	Description and resolution
“HTTP Error 404 - File or Directory not found” appears during storage zones controller configuration	The message typically results from an issue with IIS or <b>ASP.NET</b> . Make sure that the IIS role is enabled on the Windows installation and that the <b>ASP.NET</b> feature is enabled on IIS.
“HTTP Error 404.2 –Not Found” appears when browsing localhost on the storage zones controller	The message indicates that ISAPI and CGI restrictions for <b>ASP.NET</b> are not set to Allowed.

Issue	Description and resolution
“HTTP Error 413 –Request entity too large” appears after an upload attempt	The message can appear on a network trace after a failed upload attempt to a storage zone and can result from a client certificate setting in IIS. To work around this issue, on the storage zones controller server, open IIS. Navigate to the default website and then open SSL Settings. For Client certificates, select Ignore. Restart the Citrix ShareFile Management Service.
IIS errors occur during storage zones controller configuration	IIS errors typically indicate that <a href="#">ASP . NET</a> is not fully configured. Verify in the IIS Manager, under ISAPI and CGI Restrictions, that Restriction is set to Allowed for all of the <a href="#">ASP . NET</a> listings. Verify that <a href="#">ASP . NET</a> is registered in IIS: In IIS Manager, under Application Pools, verify that there are <a href="#">ASP . NET</a> listings. To manually register <a href="#">ASP . NET</a> , see the command lines following this table. If you continue to have issues, review your IIS and <a href="#">ASP . NET</a> setup.
“Failed to Save Storage Center Binding” appears during storage zones controller configuration	The message indicates a permissions problem on the IIS Account Pool user. By default, application pools operate under the Network Service user account. Storage zones controller uses the Network Service account by default. If you use a named user account instead of the Network Service account, the named user account must have full access to the network share used for private data storage.
“Access denied” appears during zone configuration	The message can occur if the ShareFile account you are logged on as does not have permission to create and manage zones. Use the ShareFile administrator console to set that permission.

Issue	Description and resolution
Outbound requests are blocked	When outbound requests are blocked, the cfgsrv log includes System.Net.WebException: The remote server returned an error: (403) Forbidden. This issue is likely due to the proxy server blocking outbound requests. Verify that your firewall meets the requirements specified in storage zones controller system requirements
“Unable to connect to remote server” appears when you log on to the storage zones controller	The message typically indicates a proxy issue. Make sure that your proxy settings are configured. If the proxy settings are correct, verify that you can log into your ShareFile account from the storage zones controller. Verify that you have administrator-level permissions to configure the storage zones controller and that port 443 is open on the external firewall.
The folder named ShareFileStorage on your network share does not include SCKeys.txt after you enable and configure storage zones for ShareFile Data	storage zones controller creates SCKeys.txt during installation unless the account you used to install the storage zone controller is not in the access control list. Update the access control list and reinstall the storage zones controller.
File uploads to a shared folder fail after you create a zone	This issue indicates a problem with your internal DNS. You must have both an internal and external DNS record for the storage zones controller FQDN.

---

Issue	Description and resolution
On the <b>Monitoring</b> tab, the Heartbeat Status is red	A red icon indicates the storage zone controller isn't able to send heartbeat messages to the ShareFile website. Check if the icons for other components are red. If so, refer to the logs for more information. If the s3uploader log shows a failure to send the heartbeat, the storage zones controller server might not be able to contact the ShareFile website unless it goes through a proxy server. To specify a proxy server for the storage zones controller, open the controller console and go to the Networking tab. If the storage zones controller server cannot access the ShareFile website using a network service user, either allow the network service user to access the ShareFile website or set up a Windows user account with outbound access to the proxy server.



Issue	Description and resolution
A storage zone does not appear in the ShareFile administrator interface	<p>This issue can indicate a problem with the external address or firewall. First verify in the storage zones controller console that the External Address does not include the port. If it does, remove the port and then restart the controller. If the External Address does not include the port, make sure that your Windows firewall is configured correctly. By default, Windows firewall settings allow outbound traffic for the ShareFile services on port 443. Storage zones controller requires that setting. Verify the Windows firewall allows outbound traffic on port 443 for the following processes:</p> <p>C:\inetpub\wwwroot\Citrix\ StorageCenter\SCFileCleanSvc\ FileDeleteService.exe, C:\inetpub\wwwroot\Citrix\ StorageCenter\SCFileCopySvc\ FileCopyService.exe, C:\inetpub\wwwroot\Citrix\ StorageCenter\s3uploader\ S3UploaderService.exe, C:\inetpub\wwwroot\Citrix\ StorageCenter\ CloudStorageUploaderSvc\ CloudStorageUploaderService.exe, C:\inetpub\wwwroot\Citrix\ StorageCenter\SCProxyEmailSvc\ ProxyEmailService.exe</p>

Issue	Description and resolution
Storage zones controller does not upload data to ShareFile	<p>In the Citrix ADC console, right-click the load balancing virtual server for statistics, to verify whether traffic is reaching Citrix ADC from the ShareFile control plane, storage zones controller, and ShareFile clients. When you upload a file and the virtual server shows an increase in hits, then the traffic is passing through Citrix ADC. Verify the traffic for every point of the Citrix ADC connection: Content switching virtual server, load balancing virtual servers for connectors and for ShareFile data, HTTP callouts bound to one of the two virtual servers, responder policy bound to the ShareFile data virtual server, connectors virtual server binding to Citrix ADC AAA. Then, test uploads for ShareFile data by unbinding the responder policy in the load balancing virtual server for ShareFile data. (The responder policy drops incoming traffic that is not signed by the ShareFile control plane. From a web browser, type the external FQDN of storage zones controller. If there is connectivity, the ShareFile logo appears. From a web browser, type the URL for a connector. If the following URLs are successful to test accessibility of storage zone connectors, you will be prompted for credentials even if the back-end server is down. Or, if you are logged on as a user, you will get an API response. <a href="https://szc-address/cifs/v3/Items/ByPath?path=\\path">https://szc-address/cifs/v3/Items/ByPath?path=\\path</a>, <a href="https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server">https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server</a>. The API response is in this form: { "Name": "connectorName", "FileName": "FileName", "CreationDate": "date", "ProgenyEditDate": "date", "IsHidden": false, "Path": "", "StreamID": "id", "odata.metadata": "<a href="https://szc-address/cifs/v3/\$metadata#Items/ShareFile.Api.Models.Folder@Element">https://szc-address/cifs/v3/\$metadata#Items/ShareFile.Api.Models.Folder@Element</a>", "Id": "id"}. Other examples: <a href="https://szc-address/cifs/v3/getItems(itemID)">https://szc-address/cifs/v3/getItems(itemID)</a>, <a href="https://szc-address/sp/v3/getItems(itemID)">https://szc-address/sp/v3/getItems(itemID)</a>. For iOS: <a href="https://szc-address/cifs/v3/Items">https://szc-address/cifs/v3/Items</a></p>

Issue	Description and resolution
The ShareFile Connectivity from File Cleanup Services status is a red icon after you upgrade the storage zones controller	A red icon occurs if Windows starts the File Cleanup Service before the storage zones controller establishes a network connection. The status will return to a green icon after the controller server is back on the network.
“Path exceeds max length (1024)” appears during connector creation	The message can occur if the external address configured for storage zones controller points to the ShareFile website instead of the storage zones controller server FQDN.
“Invalid name” appears when configuring a new storage zones controller after deleting an old one.	The message can occur if entities related to the old storage zones controller still exist. To resolve this issue: Uninstall the new storage zones controller. Delete the shared network folder. Delete the folder c:\inetpub\wwwroot\Citrix. Open regedit and delete the key <b>HKEY_LOCAL_MACHINE/Software/Wow6432Note/Citrix</b> . Install and configure a new storage zones controller. If the issue persists, contact your support representative. This message occurs when storage zone servers cannot resolve the storage zone FQDN via DNS or the local hosts file.

### To manually register ASP.NET

```
1 cd /d C:\Windows\Microsoft.NET\Framework\v4.0.30319
2 iisreset /stop
3 aspnet_regiis -i
4 iisreset /start
5 %systemroot%\system32\inetsrv\appcmd set config /section:
  isapiCgiRestriction
6 /[path='%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll'].
  allowed:True
7 %systemroot%\system32\inetsrv\appcmd set config /section:
  isapiCgiRestriction
8 /[path='%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll'
  ].allowed:True
9 <!--NeedCopy-->
```

## Troubleshoot ShareFile clients and web app

If a mobile device won't connect to a connector, verify connectivity. Many connectivity issues are covered in the preceding table. Make sure the storage zone controller is on-line. Upload a file to the zone. If the upload works, the issue is specific to the connectors. Try to connect from the mobile device using both the cellular and company network. Check that the SharePoint server or file server is available.

If a "HTTP Error 401 –Unauthorized" appears when trying to access a connector, it might be any of the following issues that can prevent a user from accessing a connector from ShareFile clients or the ShareFile web app:

- Incorrect configuration of IIS: Verify that the Web Services (IIS) role has Basic Authentication and Windows Authentication enabled. If those options are not listed under Security, use Server Manager to install them and then restart IIS.
- Incorrect user permissions: Verify that the AD user has access to the share. From Server Manager, go to Share and Storage Management, and add the user or change the user permissions as needed.
- A problem with Citrix ADC authentication, authorization, and auditing group access.

If a "HTTP Error 403 –Forbidden" appears when connecting to a SharePoint site, the SharePoint server might be configured for basic authentication but the storage zone controller might not be configured to cache credentials. To resolve this issue, add `<add key="CacheCredentials" value="1"/>` to `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.

If a "HTTP Error 503 –Service unavailable" appears when mobile apps try to access a connector, then the connectors are sending a response but are unable to handle the HTTP request. This can occur if content switching policies, load balancing VIPs, or the responder policy are incorrectly configured or bound on the Citrix ADC. To resolve this issue, review the Citrix ADC configuration for ShareFile and correct the configuration.

## Reference: Storage zones controller configuration files

November 28, 2022

This reference provides an overview to the storage zones controller configuration files:

- Configure storage zone controller with ShareFile data on Microsoft Azure
- AppSettingsRelease.config
- FileDeleteService.exe.config

- SFAntiVirus.exe.config
- Web.config

The storage zones controller installer creates those files. Changes you make in the storage zones controller console are saved to the files.

To use or configure certain features, you must manually add or update some settings in the configuration files. This reference lists those settings and provides links to related information.

## ShareFile Data on Microsoft Azure Storage

Customer-managed storage zones supports hosting Citrix ShareFile data natively within your Microsoft Azure account. Using compatible third-party storage helps IT build a cost-effective and customized solution for their organization. This solution integrates ShareFile with Microsoft Azure's Binary Large Object (Blob) storage. This storage is a cloud service for storing large amounts of unstructured data that can be accessed from anywhere using HTTP or HTTPS.

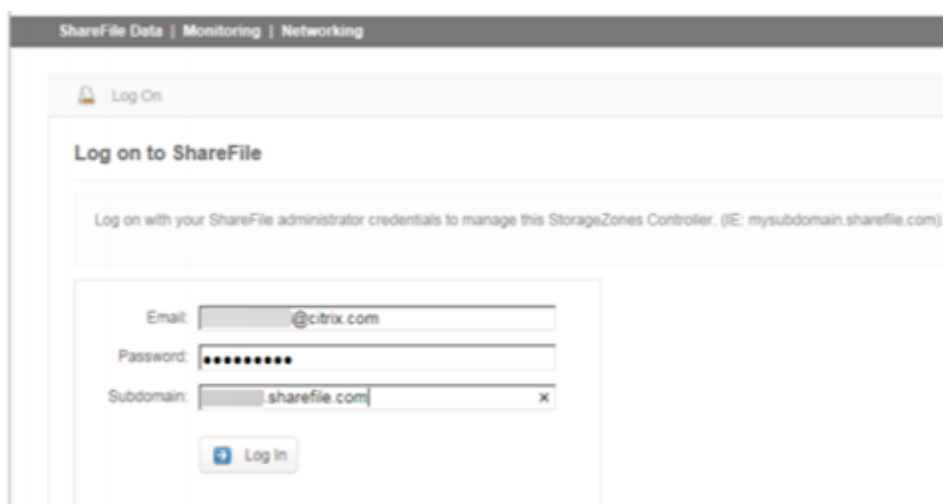
### Configure storage zone controller with ShareFile data on Microsoft Azure

Before creating a storage zone with ShareFile Data on Microsoft Azure, please review System Requirements and installation steps:

- Create a network share for storage cache. For more information, see [Create a network share for private data storage](#).
- Install necessary SSL certificates. For more information, see [Install an SSL certificate](#).
- Prepare server for storage zone installation. For more information, see [Prepare your server for ShareFile data](#).

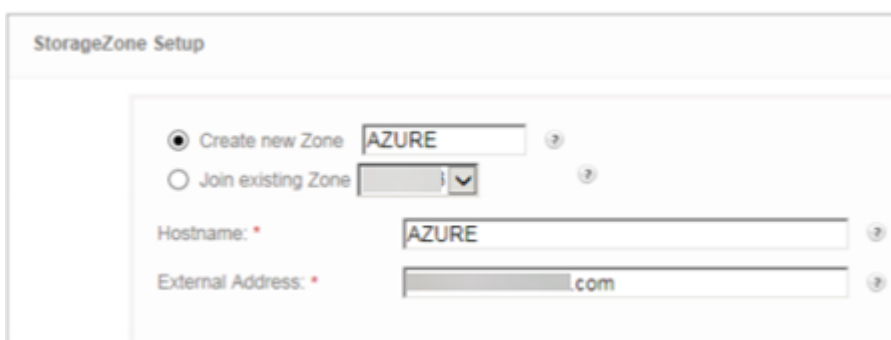
Once the storage zones controller software is installed go to **Citrix ShareFile Storage Zones Controller** and select **Configuration Page**.

1. Log on to ShareFile using your assigned administrator account.



The screenshot shows the 'Log On to ShareFile' interface. At the top, there's a navigation bar with 'ShareFile Data | Monitoring | Networking'. Below it, a 'Log On' button is visible. The main heading is 'Log on to ShareFile'. A sub-header reads: 'Log on with your ShareFile administrator credentials to manage this StorageZones Controller. (IE: mysubdomain.sharefile.com)'. The login form includes three fields: 'Email:' with a text input containing '@citrix.com', 'Password:' with a masked input (dots), and 'Subdomain:' with a text input containing 'sharefile.com' and a dropdown arrow. A 'Log In' button is at the bottom.

2. Select the option to **Create New Zone** and enter a unique name for the new zone.
3. Enter the **Hostname**, typically the computer name of the server will be used.
4. Enter the **External Address** for this zone. This is the publicly resolvable FQDN address to this server or load balancer.



The screenshot shows the 'StorageZone Setup' form. It has two radio buttons: 'Create new Zone' (selected) and 'Join existing Zone'. The 'Create new Zone' option has a text input field containing 'AZURE'. The 'Join existing Zone' option has a dropdown menu. Below these are three required fields: 'Hostname: \*' with a text input containing 'AZURE', and 'External Address: \*' with a text input containing '.com'. Each field has a help icon (?) to its right.

5. Check the **Enable StorageZones for ShareFile Data** box.
6. Select **Windows Azure storage container** from the **Storage Repository** drop-down menu.
7. Enter the **Shared Cache Location** created during the pre-requisites installation, see [Create a network share for private data storage](#). Enter a username and password with access to the Shared Cache folder.

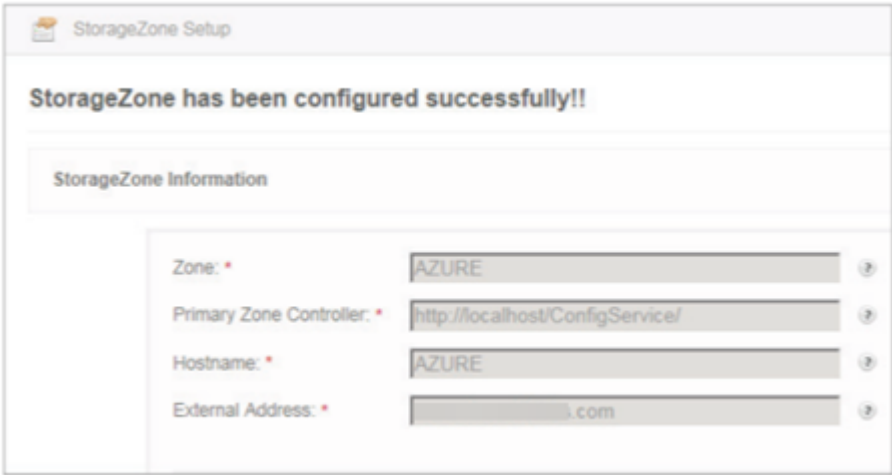
The screenshot shows a configuration window titled "Enable StorageZones for ShareFile Data". At the top, there is a checked checkbox with the same text. Below this, a "Storage Repository:" label is followed by a dropdown menu currently showing "Windows Azure storage container". A section titled "Shared Cache Configuration" contains three input fields: "Shared Cache Location:" with the text "\azure.\AzureCache", "Shared Cache Username:" which is empty, and "Shared Cache Password:" which is also empty. At the bottom of this section is an unchecked checkbox labeled "Enable Encryption".

8. Enter **Storage Account Name** and **Access Key**. This information comes from your Microsoft Azure account.
9. Select **Validate**.
10. Once validated you are presented with the containers you have available to you from Azure. Select the appropriate container from the **Container Name** drop down menu.

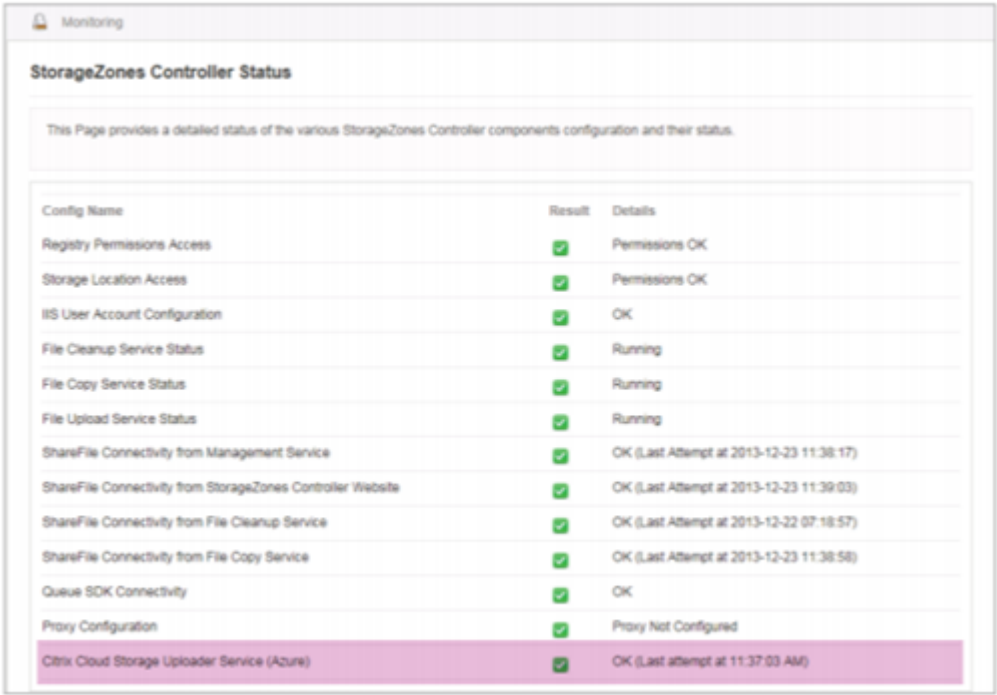
The screenshot shows a "Windows Azure Configuration" window. It has two input fields: "Storage Account Name:" and "Access Key:". The "Access Key:" field is filled with dots. To the right of the "Access Key:" field is a "Validate" button. Below these fields, the text "Validation successful." is displayed in green. At the bottom, there is a "Container Name:" label followed by a dropdown menu showing "azure-private".

11. At the bottom of the page, enter a Passphrase and re-enter it for verification.
12. Select **Register**.

Once complete the following message displays: StorageZone has been configured successfully!!

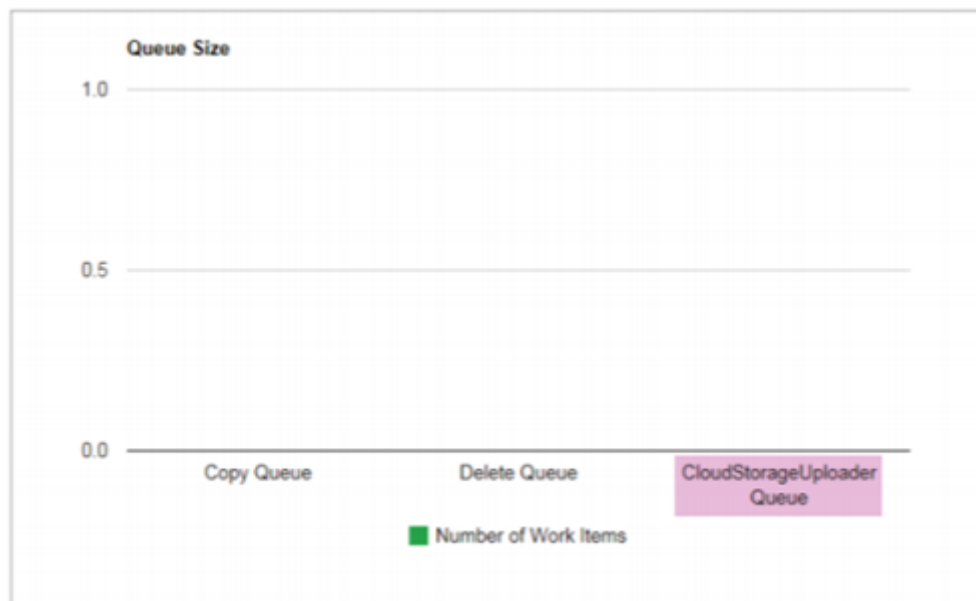


13. Select the **Monitoring** tab and verify the StorageZones Controller Status. The Citrix Cloud Storage Uploader Service (Azure) monitors the background uploader service for Azure.



The **CloudStorageUploader Queue** monitors the Azure upload queue folder.





### AppSettingsRelease.config

AppSettingsRelease.config files are contained in the following folders in the storage zones controller installation path (C:\inetpub\wwwroot\Citrix\):

- StorageCenter
  - Defines global settings for storage zones controller.
- StorageCenter\cifs
  - Defines settings for storage zones connectors for Network File Shares.
- StorageCenter\sp
  - Defines settings for storage zones connectors for SharePoint.

Before editing an AppSettingsRelease.config file, verify that you are working in the correct location.

### FileDeleteService.exe.config

FileDeleteService.exe.config provides controls used by storage zones controller to manage the persistent storage cache. This configuration file is located in: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`

For more information, see [Customize storage cache operations](#).

## SFAntiVirus.exe.config

SFAntiVirus.exe.config provides the scanner software with information about your storage zones controller configuration, the location of the scanner software, and various command options. This configuration file is located in: `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`

For more information, see [Configure antivirus scans of uploaded files](#).

## Web.config

In general, `C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` contains controls that typically should not be changed. You will, however, need to update it if you are using older storage zones controllers with a proxy server.

**For StorageZones Controller 2.2 through 2.2.2 only:** If a zone has multiple storage zones controllers and all HTTP traffic uses a proxy server, you must add a bypass list to Web.config for each secondary server.

Note: As of release 2.2.3, the bypass setting is included in the Network page of the storage zones controllers console.

1. Open the file in a text editor and locate the `<system.net>` section. Here is a sample of that section after a proxy server is configured:

```
1 <system.net>
2   <defaultProxy enabled="true">
3     <proxy proxyaddress="http://192.0.2.0:3128" />
4   </defaultProxy>
5 </system.net>
6 </configuration>
7 <!--NeedCopy-->
```

2. Add a bypass list to that section, as shown:

```
1 <system.net>
2   <defaultProxy enabled="true">
3     <proxy proxyaddress="http://192.0.2.0:3128" />
4     <bypasslist>
5       <add address="primaryServer" />
6     </bypasslist>
7   </defaultProxy>
8 </system.net>
9 </configuration>
10 <!--NeedCopy-->
```

The primaryServer is either an IP address or host name (servername.subdomain.com).

If you later change the primary storage zones controller IP address or host name, you must update that information in ConfigService\Web.config for each secondary server.

3. Restart the IIS server of all zone members.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).