ShareConnect

July 28, 2022

Contributed by: V C J

IN THIS ARTICLE

IMPORTANT:

ShareConnect reached End of Life (EOL) on June 30, 2020. For details, see **EOL and deprecated apps**.

With ShareConnect, users can securely connect to their computers through iPads, Android tablets, and Android phones to access their files and applications. Users can:

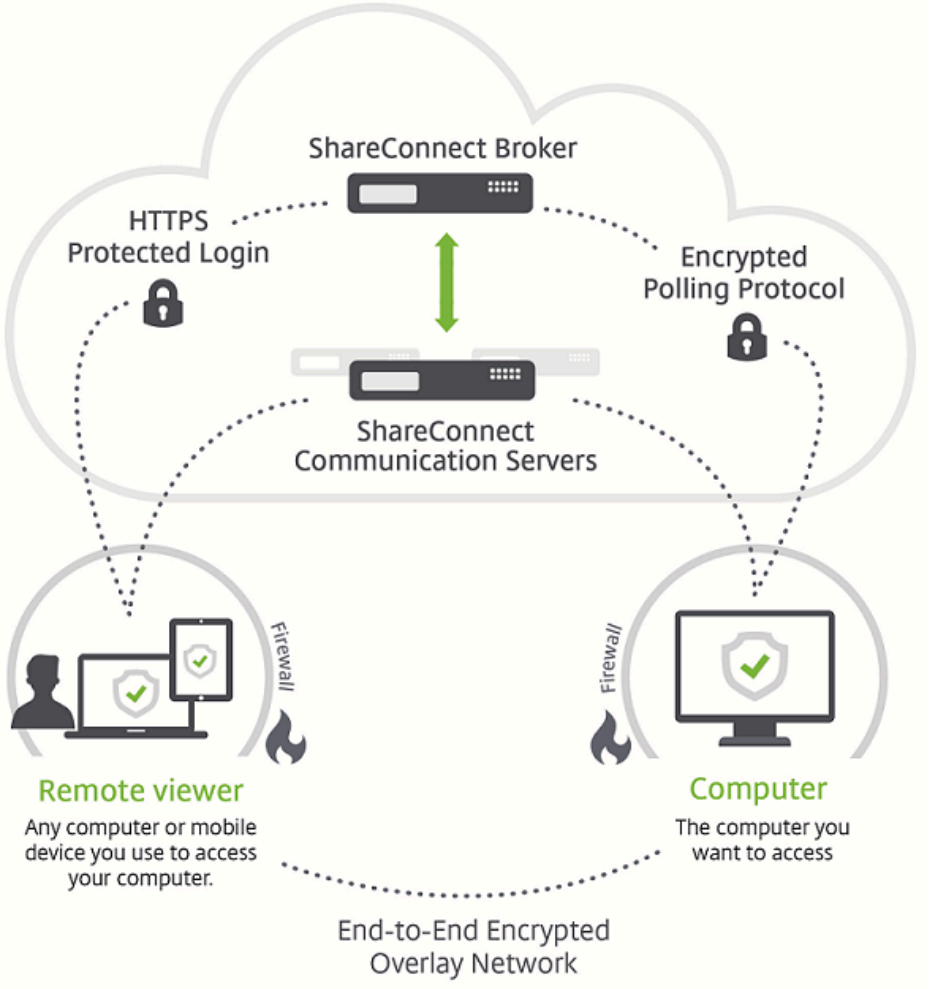
- Work on files that reside on both their computers and on connected and networked drives
- Run apps from the target machine within ShareConnect.
- Have mobile app access without the need to wrap other mobile productivity apps.
- Run ShareConnect on Citrix Virtual Desktops for mobile-optimized access.

You can download the MDX version of ShareConnect from the **Endpoint Management downloads** page.

For general information on how to install and use ShareConnect, see the **Citrix Knowledge Center**.

Architecture overview

ShareConnect components include the Citrix-owned ShareConnect Broker and the ShareConnect Communication Servers, as shown in the following figure. The ShareConnect Broker is an application server and database that maps users to computers. The application then lets users know whether their host computer is online or offline. ShareConnect Communication Servers are used to exchange data between host and client computers. That data can flow through a secure micro VPN tunnel between the host and client computers based on **Endpoint Management** settings.



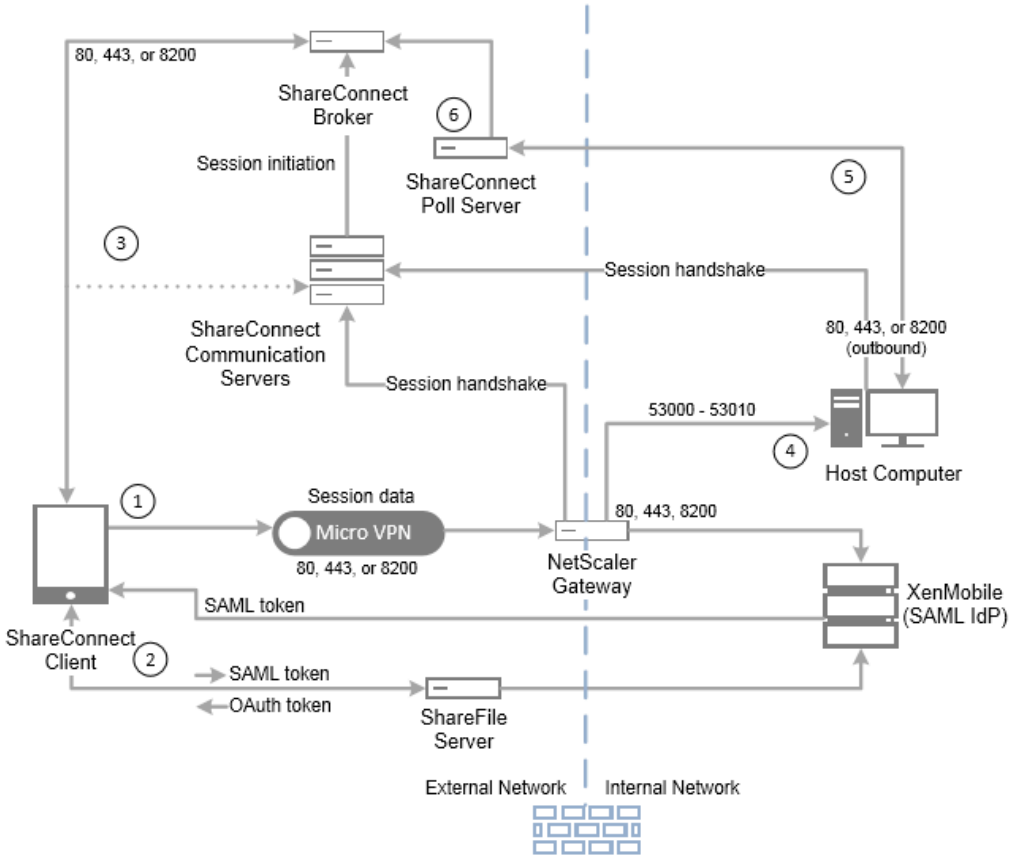
In addition, Citrix Files can provide user authentication through single sign-on (SSO) with a SAML Identity Provider (IdP), such as Endpoint Management or Active Directory Federation Services (ADFS). Access to resources outside of the network is provided through Citrix Gateway in a deployment with Endpoint Management.

How connections work in ShareConnect

ShareConnect establishes either direct or indirect connections:

- **Direct connections.** ShareConnect establishes a direct connection between the client computer and host computer if the computers are on the same LAN or Wi-Fi network. In this scenario, data flows directly between the client computer or mobile device being used to access a host computer. Data does not flow through the ShareConnect Communication Servers, resulting in optimal performance. For direct connections, Endpoint Management uses Citrix Gateway to provide secure access to resources outside of the local network.
- **Indirect connections.** ShareConnect establishes an indirect connection between the client computer and host computer if the computers are not directly reachable. In this scenario, data flows through the ShareConnect Communication Servers.

The following figure shows the connections used when users access a host computer from a computer or mobile device running ShareConnect using direct connections. Connection steps are described after the figure.



① In this scenario, Endpoint Management is configured to act as a SAML IdP for Citrix Files, to provide SSO from Secure Hub. ShareConnect requests a SAML token from Secure Hub, which in turn passes the request to Endpoint Management through Citrix Gateway. Endpoint Management then sends the SAML token to ShareConnect.

② ShareConnect sends the SAML token to Citrix Files for validation and to exchange the SAML token for an OAuth token.

③ ShareConnect sends the OAuth token to the ShareConnect broker, which then sends a session token to ShareConnect.

④ ShareConnect gets a list of host computers from the ShareConnect Broker and prompts for host computer credentials. ShareConnect then establishes a direct connection with the ShareConnect Communication Server. After the host computer validates the credentials, ShareConnect gets a list of files and apps from the host computer. After the user opens a file or app, a direct connection occurs between ShareConnect and the host computer.

⑤ The ShareConnect agent on the host computer sends status messages to ShareConnect Poll Server to indicate whether it's online or offline.

⑥ The ShareConnect Poll Server sends load-balanced requests from the ShareConnect agent to the ShareConnect Broker and sends host status updates to the ShareConnect Broker.

ShareConnect security

ShareConnect uses built-in 128-bit AES encryption so that all data sent between the ShareConnect client and a host computer running the ShareConnect agent is fully encrypted from end-to-end. The encryption key is unique for each connection. Even the most sophisticated devices cannot intercept the data necessary to decode the encryption.

You typically configure ShareConnect so that data is routed directly between the ShareConnect client and a host computer. Data is not routed through the ShareConnect Communication Servers unless you configure the Network access policy for unrestricted access. For policy details, see Add ShareConnect to Endpoint Management in this article.

For direct or indirect connections, encrypted metadata, such as the IP addresses and ports needed to establish connections, is sent to ShareConnect servers.

Also, MDX wrapping of ShareConnect provides data encryption through the MDX vault. The vault encrypts MDX-wrapped apps and associated stored data on both iOS (pre-iOS 9) and Android devices. The encryption occurs by using FIPS-certified cryptographic modules provided by the OpenSSL.

Information on Security Settings and Admin controls can be found in the following security whitepapers.

ShareConnect Security Whitepaper

ShareConnect Administrator Guide

Port requirements for ShareConnect

Open the following ports to allow ShareConnect communications. The port requirements differ depending on the type of connection. The connections can be direct connections, if the computers are on the same LAN or Wi-Fi network. Or they can be indirect connections, if the client and host computers cannot directly reach each other.

For direct connections

TCP port 80 - Used for outbound connections from Citrix Gateway to app.shareconnect.com.

Source - Citrix Gateway

Destination - app.shareconnect.com

TCP port 80, 443, 8200 - At least one of these ports is required for outbound connections from Citrix Gateway to the ShareConnect Communication Server.

Source - Citrix Gateway

Destination - ShareConnect Communication Servers

TCP port 80, 443, 8200 - Used for outbound connections from ShareConnect host computers to Citrix servers.

Source - ShareConnect host computers

Destination - poll.shareconnect.com, ShareConnect Communication Servers

TCP port 443 - Used for outbound connections from Citrix Gateway to required sites.

Source - Citrix Gateway

Destination - crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

TCP port 53000 - 53010 - Used for outbound connections from Citrix Gateway to ShareConnect host computers.

Source - Citrix Gateway

Destination - LAN-based ShareConnect host computers

TCP port 53000 - 53010 - Used for inbound connections from Citrix Gateway to ShareConnect host computers.

Source - Citrix Gateway

Destination - LAN-based ShareConnect host computers

For indirect connections

TCP port 80 - Used for outbound connections from the ShareConnect agent to app.shareconnect.com.

Source - ShareConnect agent

Destination-app.shareconnect.com

TCP port 80, 443, 8200-At least one of these ports is required for outbound connections from the ShareConnect agent to the ShareConnect Communication Server.

Source-ShareConnect agent

Destination-ShareConnect Communication Servers

TCP port 80, 443, 8200-Used for outbound connections from ShareConnect host computers to Citrix servers.

Source-ShareConnect host computers

Destination-poll.shareconnect.com, ShareConnect Communication Servers

TCP port 443-Used for outbound connections from the ShareConnect agent to required sites.

Source-ShareConnect agent

Destination-crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

Integrating and delivering ShareConnect

To integrate and deliver ShareConnect with Endpoint Management, follow these general steps:

1. You can optionally enable SSO from Secure Hub. To do that, you configure Citrix Files account information in Endpoint Management to enable Endpoint Management as a SAML IdP for Citrix Files.

   Configuring the Citrix Files account information in Endpoint Management is a one-time setup. The one-time setup is used for all mobile productivity apps clients, Citrix Files clients, and non-MDX Citrix Files clients.

2. **Download** and wrap ShareConnect. For details, see **About the MDX Toolkit**.

3. Add ShareConnect to Endpoint Management and configure MDX policies.

4. Install the ShareConnect agent on host computers. The ShareConnect agent is an MSI package. Therefore, you can use your existing software deployment methods to distribute and install the agent. Users must then register the host computer by signing on to the Agent using their Citrix Files credentials within one hour of installation.

   Alternatively, users can install the ShareConnect agent on the computer to which they connect with ShareConnect. For details, see the “To install the ShareConnect agent on a computer” section later in this article.

Add ShareConnect to Endpoint Management

You add ShareConnect to Endpoint Management using the same steps as for other MDX apps. For details, see **Add an MDX app**. When adding ShareConnect, configure the MDX policies for it as shown in the following table.

Policy	Value	Results
Network access	Tunneled to the internal network or Unrestricted	Tunneled to the internal network uses a per-application VPN tunnel back to the internal network for all network access. This configuration provides direct connection between ShareConnect and a host computer. Unrestricted uses Citrix-owned Communication Servers to route encrypted data between a host computer and ShareConnect. Be sure to test your setup with unrestricted access to ensure everything works, even if you plan to use Tunneled to the internal network for network access.
Preferred VPN mode	Tunneled – Web SSO	Sets the initial connection mode appropriately for connections that require SSO.
Enable encryption	On	Encrypts the data stored on the tablet.

Policy	Value	Results
Cut and copy	Unrestricted	Enables cut and copy operations for ShareConnect.
Paste	Unrestricted	Enables paste operations for ShareConnect.
Document Exchange (Open In)	Unrestricted	Permits users to open any file on the connected computer or a connected network drive from ShareConnect.
Save Password	Off	Requires users to enter the user name and password for their computer each time they sign on to ShareConnect.

To install the ShareConnect agent on a computer

The following steps describe how a user installs the ShareConnect agent on each physical or virtual computer they want to connect to from a supported mobile device.

Before performing these steps, the user must first install Secure Hub. Then, they follow the prompts to allow the mobile productivity apps to install on the supported mobile device.

1. Sign on to Secure Hub on the tablet.
2. Open ShareConnect.
3. Tap Email download link.

   Citrix sends an email to you from no-reply@shareconnect.com.
4. From the host computer that you want to access from ShareConnect, open the email.
5. In the email, click Set up this computer.
6. Double-click **ShareConnect_Installer.exe** to begin the installation.

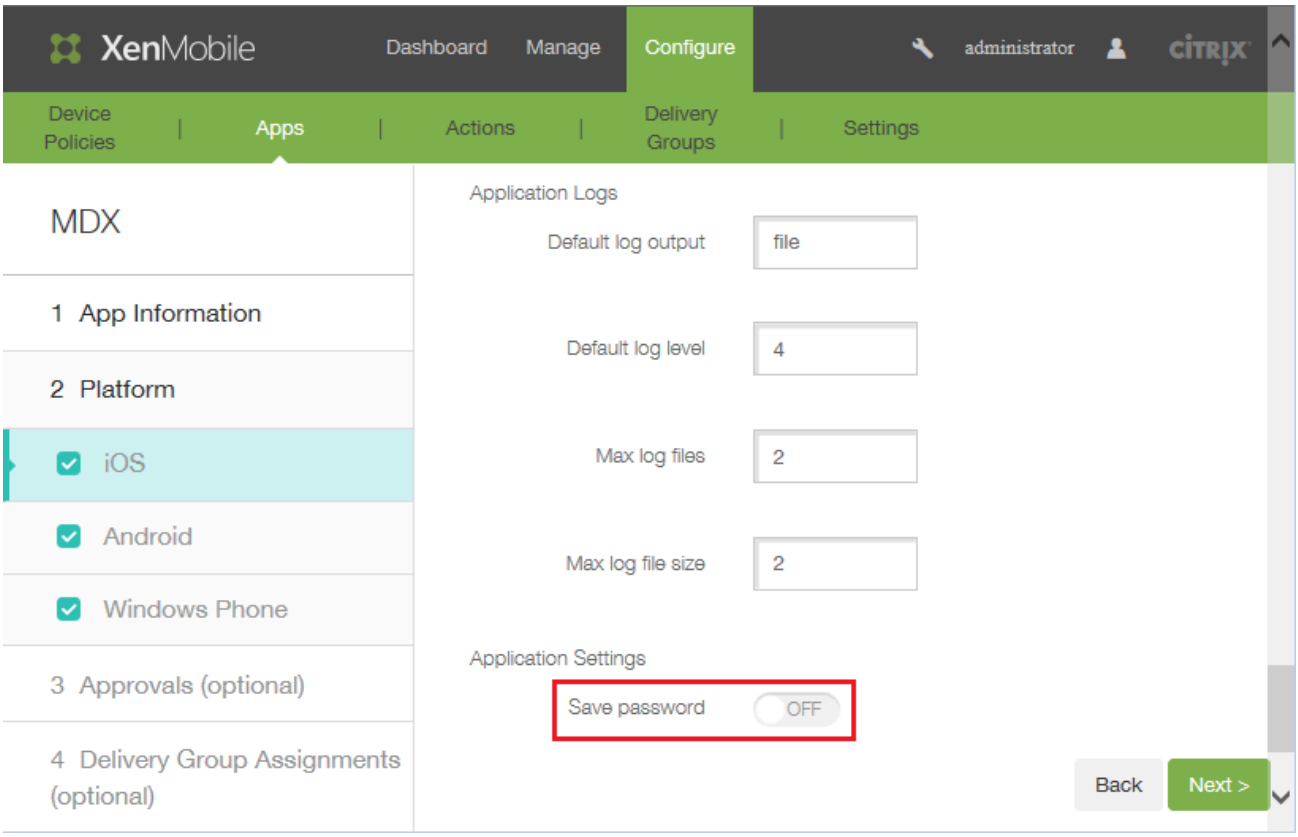
   The ShareConnect agent installs on your host computer. During the installation, ShareConnect prompts for an email address if Citrix Files SSO is configured. Or, ShareConnect prompts for Citrix Files credentials if Citrix Files SSO is not configured.
7. Follow the instructions provided in the ShareConnect and Get Started wizards.

The ShareConnect agent then registers the host computer. The host computer can connect from a ShareConnect client, if the host computer is powered on and can reach poll.shareconnect.com on at least one published port (80, 443, or 8200).

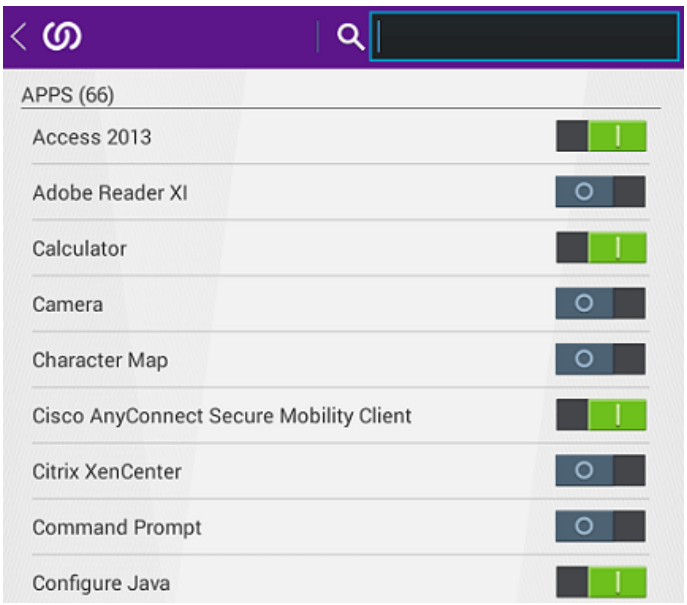
ShareConnect features

- **Add host computers**. Users can add and connect to remote host computers from supported mobile devices using ShareConnect.
- **Access files**. Users can view a list of recent files and browse and search for files on their host computer and connected drives.
- **Edit files**. From tablets, users can access desktop applications on their host computers to edit files. Users can use the applications in full screen.
- **Screen share**. Instead of viewing a single file or app, users can use the screen-sharing feature to view their host computer's desktop.
- **Citrix Files integration**. Users can move or share files between the host computer and Citrix Files.
- **Keyboard and mouse**. ShareConnect supports the simultaneous use of a Bluetooth keyboard and the Citrix XI Prototype Mouse.
- **Restricted ports**. ShareConnect uses ports 53000 to 53010 only.

- **Forced passwords for each sign-on**. For enhanced security, you can configure this option to require users to enter their computer passwords every time they sign on to ShareConnect. When the Save password policy is turned off, as shown in the following figure, users are forced to enter their sign-on credentials for every connection.



- **Add or delete apps**. Users can add or delete apps from their app tray in ShareConnect by toggling the switch beside each app to select or deselect it.



- **Cache previewed files**. ShareConnect caches already-accessed files so that the files don't download again if users preview other files and then come back to the earlier ones. This feature improves load times when users later access files.

Troubleshooting ShareConnect

ShareConnect agent installation issues

Issue	Description and resolution
If a user downloads the ShareConnect agent and waits an hour or more to start the installation, the user must enter their Citrix Files account name and password to register the ShareConnect agent.	The ShareConnect agent installer includes a token that expires one hour after download. If a user doesn't start the installation before the token expires, the user must sign on to their Citrix Files account twice, first to register the ShareConnect agent and then to sign on to the agent after the installation completes. If users download and install the ShareConnect agent within an hour, they are prompted to sign on only once.
During registration of the ShareConnect agent, the agent does not connect and an error message such as "Please check your connection and try again." appears.	Verify that the port to poll.shareconnect.com is not blocked. For details, see the System Requirements earlier in this article.

ShareConnect connection issues

IMPORTANT:

To test ShareConnect, we recommend that you set the Network Access policy to **Unrestricted** to rule out issues with ports and network settings. Unrestricted access forces ShareConnect to connect through the ShareConnect Communication Servers, which typically enable you to test the connection if the ShareConnect mobile device and host computer have Internet access.

Issue	Description and resolution
ShareConnect starts, but does not connect to the host computer and does not prompt for credentials.	Verify that your setup meets the port requirements detailed earlier in this article under System Requirements.
Users are unable to sign on to ShareConnect using their Citrix Files account credentials.	SSO to ShareConnect requires that your Citrix Files account is configured with a SAML IdP. For details about using Endpoint Management as a SAML IdP, see Citrix Content Collaboration for Endpoint Management. For details about configuring other IdPs, see this Knowledge Center article. If SSO is not configured for your account, ShareConnect for iOS prompts for the user's Citrix Files user name and password.
After users sign on to ShareConnect, ShareConnect cannot connect to the host computer.	When ShareConnect is configured for direct connections (that is, the Network access policy is set to Tunneled to the internal network), connection failures can occur if there are restrictions in network settings like firewalls blocking or proxy servers configured.