Traverse 3rd Party Compatibility

Date

December 18, 2024

Copyright and Trademark Notice

Table of Contents

Traverse Web App Compatibility

The following are hardware and software compatible with the Traverse web app.

Web Browser

- Edge (latest version) on Windows 10 or greater
- Chrome (latest version) on Windows 10 or greater
- Safari (latest version) on iPadOS 13 or greater

> *Northwoods recommends you whitelist/allow the following domains:* ***northwoodstraverse.com*** *in the firewall,* ***no-reply@northwoodstraverse.com*** *in the email filter, and* ***login.northwoodstraverse.com*** *in the intrusion detection or prevention system.*

Web Browser for Training Videos

- To validate if your web browser can access the Traverse training videos, see the supported browsers for Vimeo.

Scanner

Scanner Devices

- Any Ricoh[1] scanner that supports the PaperStream IP (TWAIN) driver should work with Traverse. However, Northwoods prefers these scanners:
  - Ricoh fi-7030
  - Ricoh fi-7160
  - Ricoh fi-8170

Scanning Software

- Ricoh PaperStream IP (TWAIN) driver (latest version supported for scanner device)
- Dynamsoft Dynamic Web TWAIN (version 1.7.1026 **only**)
- TWAIN.org Twacker Utility (32-bit version)

> *See Setting up scanners for installation and configuration instructions for scanner devices with Traverse.*

[1] These scanners were rebranded from Fujitsu to Ricoh in April 2023. See the press release.

Signature Pad

Signature Pad Devices

- Any Topaz Electronic Signature Pad that supports the SigWeb driver should work with Traverse.

  **Windows devices are supported.*

  **Citrix environment is not supported.*

Signature Pad Software

- Topaz Systems SigWeb driver 1.7.2.7

> *See Setting up and using signature pads for configuration and installation instructions.*

Traverse Virtual Printer

Required Windows Software

- Microsoft .NET Desktop Runtime 8.x.x
- Microsoft Visual C++ 2022
- Microsoft Edge WebView2 Runtime (If you use Microsoft products, you likely already have this installed. If not, install the Evergreen Bootstrapper.)

Deployment

- The Traverse URL can be added to an intranet site such as SharePoint.
- A shortcut to the Traverse URL can be pushed to users' workstations as a desktop icon.
- The Traverse URL can be distributed via email and saved as a web browser favorite.

Traverse Mobile App Compatibility

The following are hardware and software compatible with the next-generation[2] Traverse mobile app.

Devices Supported

- Apple iPhone running iOS 16 or greater
- Apple iPad running iPadOS 16 or greater
- Android phone or tablet running Android 13 or greater
    - 128 GB of internal storage
    - 8 GB of RAM
    - 8 cores x 1.8 GHz CPU
    - 64 MP camera

Deployment

- Northwoods recommends the use of Enterprise Mobility Management, such as AirWatch, to deploy to end users.

> *As with many mobile apps, Traverse releases user-facing updates frequently. Therefore, Northwoods recommends that customers keep automatic updates enabled on all devices to ensure users have access to the latest functionality. On occasion, Traverse will also release over-the-air updates that will be direct to the app and not require users to update their app versions.*

- The Traverse mobile app is an application available through the Apple App Store and Google Play Store.

Authentication

- The Traverse mobile app is compatible with single sign-on authentication, password authentication, and Microsoft Entra certificate-based authentication (CBA).

[2] For non-Windows devices, the legacy Traverse mobile app will no longer be supported after July 1, 2024. For Windows devices, the legacy Traverse mobile app will no longer be supported after August 1, 2025. Compatibility for this app is listed in Legacy Traverse Mobile App Compatibility.

Legacy Traverse Mobile App Compatibility

The following are hardware and software compatible with the legacy Traverse mobile app.

Please note: For non-Windows devices, the legacy Traverse mobile app will no longer be supported after July 1, 2024. For Windows devices, the legacy Traverse mobile app will no longer be supported after August 1, 2025.

Devices Supported

- Apple iPad running iPadOS 15 or greater
  - 4G/LTE data connectivity plan (recommended)
  - 64 GB of storage or greater (recommended)
  - Rear-facing camera (recommended)
- Windows tablet running Windows 10 (version 1809) or greater
  - Microsoft Surface Pro (recommended)
  - LTE data connectivity plan (recommended)
  - 128 GB of storage or greater
  - Rear-facing camera (recommended)

Deployment

- Northwoods recommends the use of Enterprise Mobility Management, such as AirWatch, to deploy to end users.

> *As with many mobile apps, Traverse releases user-facing updates frequently. Therefore, Northwoods recommends that customers keep automatic updates enabled on all devices to ensure users have access to the latest functionality.*

- The legacy Traverse mobile app is an application available through the Apple App Store, the Microsoft Windows Store, and the Microsoft Business Store.

Authentication

- The legacy Traverse mobile app is only compatible with single sign-on and password authentication. It is not compatible with Microsoft Entra certificate-based authentication (CBA).

Traverse Capture Compatibility

The following are hardware and software compatible with Traverse Capture.

Devices Supported

- Apple iPhone running iOS 15 or greater
- Apple iPad running iPadOS 15 or greater
- Android device running Android 11 or greater

Deployment

- Northwoods recommends the use of Enterprise Mobility Management, such as AirWatch, to deploy to end users.
    - Traverse Capture is an application available through the Apple App Store and Google Play Store.

Traverse Integration Server Requirements

On-premise agent(s) are installed on a local server and handle all communication between the iPaaS (Integration Platform as a Service) provider and the Traverse architecture. The following are the technical requirements for server(s) for the on-premise Traverse Integration Agent.

Operating System

- Windows Server 2016 or greater

Software

- Microsoft .NET Framework 4.7.2 (full version)
- Microsoft Windows Identity Foundation (WIF)

Minimum Hardware

- Quad Core CPU or better with a 24/7 business-grade internet connection
- 8 GB of RAM
- 8 GB free storage

Ports

All ports listed in the table below will need to be opened for outbound traffic. Allow the traffic to *.amazonaws.com, api.sendgrid.com, and smtp.sendgrid.net regardless of the destination IP address.

For customers with Palo Alto Firewalls, allow application identification for SendGrid. Add a custom URL category with these two domains: *.sendgrid.com and smtp.sendgrid.net.

To retrieve instructions and update the iPaaS provider with its current status, the integration agent needs access to one or more of the following endpoints:

- https://agent.scribesoft.com
- https://endpoint.scribesoft.com
- https://api.scribesoft.com

For a list of all possible current iPaaS destination IP addresses, please contact Northwoods. For a list of all possible current SendGrid destination IP addresses, please visit the DNS checker.

The ports listed in the table below require the firewall to be stateful.

Port	Description	Endpoint
TCP 25	This port is used by the integration agent email alerts through SendGrid.	smtp.sendgrid.net
TCP 80	This port is required for outbound integration agent communication and SSL certificate validation. This uses the Online Certificate Status Protocol to make GET requests. This port is also used by the integration agent to send email alerts through SendGrid, keep the application updated using AWS CodeDeploy, and send integration statistics to an AWS RDS database.	• smtp.sendgrid.net • api.sendgrid.com • comodoca.com • usertrust.com • *.amazonaws.com
TCP 443	This port is required for secure outbound integration agent communication. This port is also used by the integration agent to send email alerts through SendGrid, keep the application updated using AWS CodeDeploy, and send integration statistics to an AWS RDS database.	• smtp.sendgrid.net • api.sendgrid.com • *.servicebus.windows.net • agent.scribesoft.com • endpoint.scribesoft.com • api.scribesoft.com • *.amazonaws.com
TCP 465	This port is used by the integration agent email alerts through SendGrid.	smtp.sendgrid.net
TCP 587	This port is used by the integration agent email alerts through SendGrid.	smtp.sendgrid.net
TCP 2525	This port is used by the integration agent email alerts through SendGrid.	smtp.sendgrid.net
TCP 5671 and 5672	These are outbound ports used by the integration agent to communicate with the Enterprise Service Bus (ESB).	*.servicebus.windows.net
TCP 9350 - 9354	These are outbound ports used by the integration agent to communicate with the Enterprise Service Bus (ESB).	*.servicebus.windows.net

Database

If required, the integration agent may need access to a database located on the internal network. This is mainly used as either a staging or source database for the data involved with the integration.

For Oracle, the following apply:

- Authentication: Read-only access (Oracle role with Select privileges granted for intended tables in the source database).
- Versions:
  - Oracle Database 18c
  - Oracle Database 12c
  - Oracle Database 11g Release 2

For Microsoft SQL Server, the following apply:

- Authentication: Microsoft Windows (recommended) or Microsoft SQL Server. The minimum access rights are public server role and db_owner database role. The Microsoft SQL Server user must have Insert, Select, Update, and Delete access in the source database. In addition, this user (or equivalent) must be able to create tables, indexes, and views for the source database during the project.
- Versions:
  - Microsoft SQL Server 2017: Enterprise, Standard, and Express*
  - Microsoft SQL Server 2016: Enterprise, Standard, and Express*
  - Microsoft SQL Server 2012: Enterprise, Standard, and Express*
  - Microsoft SQL Azure

> **Note: Express edition would only be used only if the database is for staging data and the database size remains under 10 GB.*