BlackBerry AtHoc Desktop App
Installation and Administration Guide

7.2 (Windows), 2.4.1 (Mac)

Contents

Troubleshoot desktop app issues... 29

Appendix B: Desktop client URL parameters... 35

BlackBerry AtHoc Customer Support Portal.. 37

Documentation feedback...38

Legal notice.. 39

What is the BlackBerry AtHoc desktop app?

The BlackBerry AtHoc management system provides authorized users with the ability to quickly notify large numbers of people in widely dispersed locations during emergencies and other critical situations. BlackBerry AtHoc also helps those users monitor alerts for threat conditions while also providing basic notifications services for non-emergency situations.

The BlackBerry AtHoc desktop application (also called the desktop app or desktop client) is a small desktop application that runs continuously on your computer. When a new alert targeted at user desktops is published in the BlackBerry AtHoc system, a notification screen opens on your desktop, accompanied by an audio notification.

You can then close the pop-up or click a link to obtain additional information about the alert. For emergency alerts, the pop-up screen might contain response options that you must select from in order to acknowledge receipt of the alert.

This guide is intended for IT administrators who are responsible for installing, setting up, and maintaining the BlackBerry AtHoc desktop app for end users. To find information about using the desktop app to receive alerts, see the *BlackBerry AtHoc Desktop App User Guide*.

Note: BlackBerry AtHoc desktop app release 7.1 or later is compatible with BlackBerry AtHoc release 7.9 (OnPrem) and 7.14 or later release.

Install the desktop app

Every desktop must have the desktop app installed so that personnel can receive and respond to alert messages.

In most setups, the IT group pushes the app to user desktops during off-hours using an SMS package that includes the app MSI, the SMS script, and a `run.bat` file (Windows) or the PKG installer package (Mac).

- Windows: You can adjust the installation parameters in the `run.bat` file to configure the desktop app to run immediately after the installation or at the next start up. The MSI can be run manually. There is also an option to allow manual entry of connection parameters during installation. For more information on installation parameters, see Installation settings (Windows).
- Mac: You can adjust the installation parameters such as the Base URL, Provider ID, and Manual Registration while creating the PKG installer package. Run the PKG installer package by double-clicking it and then following the instructions in the wizard.

Request a new desktop app

To request a new desktop app, contact BlackBerry AtHoc customer support and be prepared to provide the information in the following tables.

Windows

Element	Description
Contact Information	Full name and email address. You will receive an email when the new desktop app is available.
Client Name	The name of the organization. The Windows installer displays the client name in the list when running the installer manually. The client name is not an installation parameter.
Version	Desktop app version. Always choose the latest version unless there is a reason to choose an older one.
Edition	Select one of the following: • 1_BlackBerry AtHoc • 2_BlackBerry AtHocAlt • 3_BlackBerry AtHocAux
Base URL	The URL that the desktop app should connect to. **Format**: `http://<server_name_or_ip>/config/baseurl.asp`.
Provider ID	The identifier of the organization that the desktop app should connect to. **Format**: Integer. For example, 1234567.

Element	Description
Audio	Audio files are downloaded with an alert but can be packaged with the Windows installer. This increases the size of the installer substantially. Select from the following options: **Default**, **All**, or **None**.
silent_installation	Optional. Select this option to hide the the MSI user interface from the user. If this option is selected, there is no UI.
run_after_install	Optional. Select this option to configure the desktop app to start when the installer completes the installation. This element cannot be used to prevent the desktop app from starting when the machine starts. The desktop app is always added to the list of applications that start when the machine starts.
mandate_ssl	Optional. Select this option to require that the URLs used for Sign On, Check Update, and Get Update use the HTTPS protocol.
validate_cert	Optional. Select this option to require that the client certificate cannot be expired, revoked, or otherwise invalid.
uninstall_option	Optional. Select this option to allow users to remove the desktop app using the Control Panel.
MSI Installer Customizations: schedule_reboot	Optional. Select this option to configure the installer to reboot Windows automatically after a manual installation.
MSI Installer Customizations: manual_selection	Optional. Select this option to allow the user to overwrite the request form configuration and specify the new base URL and organization ID.
vps_list_header	Optional. Enter text that appears above the organization list on the organization dialog that appears during manual installation. The default is no text.
connection_instructions	Optional. Enter text that appears above the organization list on the organization dialog that appears during manual installation. The default is "Please select your system from the list below."

Note: For more information about these options, see Installation settings (Windows) and Run.bat.

Mac

Element	Description
Contact Information	Full name and email address. You will receive an email when the new desktop app is available.
Client Name	The name of the organization.
Release	Desktop app version. Always choose the latest version unless there is a reason to choose an older one.
Edition	Select BlackBerry AtHoc.
Base URL	The URL that the desktop app should connect to. **Format**: `http://<server_name_or_ip>/config/baseurl.asp`.
Provider ID	The identifier of the organization that the desktop app should connect to. **Format**: Integer. For example, 1234567.
Replace Previous Setting	Optional. Select this option to use the new settings when the Mac desktop app is installed before uninstalling an existing instance. Leave this option unselected to use the current settings. The current settings are specified in the `Configuration.plist` file.
Manual Registration	Optional. Select this option to present the end user with a registration screen. The end user must enter their email address and then reply to a verification email before the desktop app for Mac connects. If this option is not selected, the desktop app for Mac connects automatically after installation.
Manual Registration URL	URL of the server used during manual registration process. **Format**: `http://<server_name_or_ip>`.

Installation methods

You can choose from the following methods to install the BlackBerry AtHoc desktop app:

1. Windows: Automatic installation using Microsoft System Center Configuration Manager (SCCM) or similar systems management software product. BlackBerry AtHoc provides a `run.bat` file that includes the `msiexec.exe` command line. Work with a BlackBerry AtHoc Implementation Engineer (IE) to determine the values. See Management system desktop app settings for information about the available options.

2. Windows: Manual installation using MSI with no options, where options are preset and disabled. This is a compile option that must be requested. Installation using a `run.bat` file is supported with this option. The command line values in the `run.bat` file override the compiled values.
3. Windows: Manual installation using MSI, with fields available for manual entry of the Provider ID and Base URL. With this option, the user must know the values and enter them. This is a compile option that must be requested. Installation with the `run.bat` file is supported with this option. The command line values in the `run.bat` file override the compiled values.
4. Windows: Manual installation using MSI. With this option, the user selects from a list of providers. Fields for manual entry of the Provider ID and Base URL are disabled. This is the default option. Installation with the `run.bat` file is supported with this option. The command line values in the `run.bat` file override the compiled values.
5. Mac: Installation using PKG. Double-click the PKG installer package to launch the installation wizard and then follow the instructions in the wizard.

Platform support

The BlackBerry AtHoc desktop app for Windows can be installed on laptops and tablets running Windows operating systems. The BlackBerry AtHoc desktop app for Windows works with Internet Explorer, Firefox, Chrome, and Microsoft Edge.

The BlackBerry AtHoc desktop app for Mac can be installed on laptops and desktops running Mac operating systems. The BlackBerry AtHoc desktop app for Mac works with Safari version 10.x and later.

Desktop app version	Browser support	OS support
7.2 (Windows) 2.4 (Mac)	• Internet Explorer 10 and later • Safari 10.x and later • Firefox • Chrome • Microsoft Edge	Windows: 10, 7 Mac: macOS Mojave (10.14), macOS Catalina (10.15)

Installation artifacts

This section describes the artifacts that are created during the BlackBerry AtHoc desktop app installation process.

Folders

The folders in the following table are created during the installation of the BlackBerry AtHoc desktop app. These folders are used to store the installation artifact files.

Table 1: Installation artifact file folders

Folder name	Location	Contents	Example
(Windows) BlackBerryAtHocNotifier	In the 32-bit ProgramFiles folder	The BlackBerryAtHoc.exe file	C:\Program Files (x86)\ BlackBerryAtHocNotifier
Windows) BlackBerryAtHocNoti	In the CommonAppDataManufacturer folder	All other files included in the installer	C:\ProgramData \ BlackBerryAtHocNotifier
(Mac) AtHoc	/Library/Application Support	All client executable files	/Library/Application Support/ AtHoc

Registry keys (Windows)

The BlackBerry AtHoc desktop app installation process creates the following registry key:

`HKLM\Software\SysWow6432Node\BlackBerryAtHocNotifier`

The installation process creates several values under the registry key, including the BASEURL and PROVIDER ID. The desktop app uses these values at startup.

The desktop app log is created during the installation process. The app log is shared by all users and is located in an "BlackBerryAtHocNotifier" folder in the CommonAppDataManufacturerFolder. For example:

`C:\ProgramData\BlackBerryAtHocNotifier`

The installation process adds the following registry value to make the client run when the machine starts:

`HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run`

Install in an enterprise organization

To install and set up the desktop app in an enterprise organization, you must first enable user uniqueness.

When the desktop app starts, it sends up the ProviderID of an enterprise organization or sub organization. If the user exists in the enterprise organization, it attaches to the user. If the user does not exist, BlackBerry AtHoc attempts to create the user in the organization that is identified by the ProviderID. You must enable the "Create new user if an account is not found" flag in the organization specified by the ProviderID.

For more information about enabling user uniqueness, see the "Manage users in the enterprise" section of the *BlackBerry AtHoc Enterprise Planning and Management Guide*.

Uninstall the desktop app

Windows

You can uninstall the BlackBerry AtHoc desktop app from the Programs and Features utility in the Control Panel. However, uninstalling the app from the Control Panel may be disabled due to policy. For example, an administrator can use the UNINSTALLOPTION described in Installation settings (Windows) to disable removal of the desktop app from the Control Panel.

You can use the following methods to uninstall the desktop app:

- If you have the original MSI, you can use the following command:

  ```
  msiexec /uninstall BlackBerryAtHocNotifier_7.0.0.104.msi
  ```
- If you do not have the original MSI, you can use the following command that uses a cached copy of the MSI:

  ```
  msiexec /x [product_guid]
  ```
- You can find the product_guid here:

  ```
  HKLM\Software\Wow6432Node\BlackBerryAtHocNotifier\ProductCode
  ```
- Use the Uninstall shortcut that appears in the Start Menu. The shortcut runs the following command:

  ```
  msiexec /x [product_guid]
  ```

Note: Uninstalling the desktop app does not remove Start menu folder with the organization name.

Mac

You can uninstall the BlackBerry AtHoc desktop app from the Applications section in the Finder.

1. On your computer, search for **BlackBerryAtHocNotifier**.
2. In the search results, right-click **BlackBerryAtHocNotifier** and click **Uninstall**.
3. On the **Uninstall or change a program** window, click **BlackBerryAtHocNotifier**.
4. Click **Uninstall**.

Desktop app network traffic

The following sections describe the types of network traffic you can expect when installing or using the desktop app.

Sign-on traffic

The desktop app calls `config\baseurl.asp` and receives a response that is about 1339 bytes. The desktop app then makes a SignOn call (99=SO) and receives a response that is about 294 bytes (total 1633 bytes.)

Check-update traffic

The desktop app makes Check Update requests to the server and receives a response that indicates whether an update is available.

Windows: The response that is about 564 bytes.

Mac: The response is about 676 bytes.

If the response indicates that there is an update pending, a Get Update (GU) call follows. For example, when an operator changes the desktop app settings in the management system, the desktop app receives a response at the next check update that indicates a get update is needed.

The desktop app then makes a GU request after the Check Update, and receives the settings as XML in the response.

First-time sign on traffic

During a first-time sign on or whenever settings get updated, the desktop app downloads settings. This includes downloading about 5079 bytes, depending on factors such as the number of items in the system tray menu.

Alert traffic

Alert downloads can include a .wav file. The alert is created from the HTML data received in Get Update (GU) response and then displayed on screen. An alert is about 23714 bytes. If the alert includes audio, the .wav file is downloaded separately and stored in ~/Library/Containers/com.athoc.adc.agent/Data/Documents/Servers/ Server/Audio (for Mac), or in ProgramData\AtHoc[edition]\wav (for Windows.)

Desktop app settings

This section describes settings used during installation to configure the desktop app, and settings that the desktop app uses during operation.

Installation settings (Windows)

Installation settings are passed to the MSI on the command line in the `run.bat` file. The MSI is compiled with at least one pair of default Provider ID and base URL values so that end users can manually install the desktop app. Multiple pairs of Provider ID and base URL values can be added to the MSI.

Run.bat

The `Run.bat` file is used to start the installer.

The following is a sample `Run.bat` file:

```
msiexec /qn /i BlackBerryAtHocNotifier_7.0.0.104.msi /l*vx
BlackBerryAtHocNotifier_7.0.0.104.log BASEURL=http://172.16.6.38/config/baseurl.asp
PID=2050329 RUNAFTERINSTALL=Y DESKBAR=N TOOLBAR=N SILENT=N VALIDATECERT=N
MANDATESSL=N UNINSTALLOPTION=Y
```

See the `msiexec` help for more information about the following part of the `Run.bat` command line:

```
msiexec /qn /i BlackBerryAtHocNotifier_7.0.0.104.msi /l*vx
BlackBerryAtHocNotifier_7.0.0.104.log
```

The `/qn` switch specifies quiet mode with no UI. This switch overrides the SILENT property. If you rely on the SILENT property passed in the command line and do not include the `/qn` switch, the installation dialog appears briefly while the Windows Installer processes the command line.

The `/i` switch indicates "Install."

`BlackBerryAtHocNotifier_7.0.0.104.msi` is the name of the installer associated with the switch.

The `/l*vx` switch specifies a verbose log.

`BlackBerryAtHocNotifier_7.0.0.104.log` is the name of the file where logging output is written.

The following table describes the other elements in the `run.bat` file.

Table 2: Run.bat file elements

Element	Description
BASEURL	The URL that the desktop app should connect to. **Required:** Yes **Format:** `http://<server_name_or_ip>/config/baseurl.asp`
PID	Provider ID. The organization that the desktop app should connect to. **Required:** Yes **Format:** Integer, for example 1234567.

Element	Description
RUNAFTERINSTALL	Specifies if the desktop app should start when the installer completes the installation. This element cannot be used to prevent the desktop app from starting when the machine starts. The desktop app is always added to the list of applications that start when the machine starts. **Required:** No **Values:** Y = Start after installation. N= Do not start after installation. **Default:** N
SILENT	Specifies if the MSI user interface (UI) should be displayed to the user. **Note:** If the SILENT value is set to Y, there is no UI. If SILENT is set to N, the BASEURL and PID parameters in the `run.bat` file are ignored. **Required:** No **Values:** Y = Do not show the UI. N = Show the UI. **Default:** N
MANDATESSL	Specifies if the URLs used for Sign On, Check Update, and Get Update must use the HTTPS protocol. **Required:** No **Values:** Y = URLs must use HTTPS. If they do not use HTTPS, the operation ends and logs the message "SSL required". N = URLs can use either HTTP or HTTPS. **Default:** N
VALIDATECERT	Specifies that the client certificate must not be expired, revoked, or otherwise invalid. Server certificates must not be expired, revoked, or otherwise invalid. **Required:** No **Values:** Y = Certificates are checked for validity. N = Certificates are not checked. **Note:** The server may require certificate validation. If a server requires certificate validation, an error is logged and the desktop app automatically attempts to open the certificate store and loop through the certificates, resending the request until it succeeds or until there are no more certificates. **Default:** N

Element	Description
UNINSTALLOPTION	Determines if a user can remove the desktop app using the Control Panel. **Required:** No **Values:** Y = Can be removed. N = cannot be removed. **Default:** N

Operating settings

Operating settings include settings returned by the server to the desktop app when the desktop app executes a Sign On (SO) or Check Update (CU), and default settings created during installation.

Desktop app settings updates

Settings that are stored by the desktop app in the user's registry key (Windows) or using Apple's UserDefaults mechanism (Mac) are associated with a version number. When an operator makes a change to one of these settings in the BlackBerry AtHoc management system, the version number associated with that setting is incremented. At the next CU, the server responds by sending the version of each set, and the desktop app determines that a Get Update (GU) is needed. The desktop app then executes a GU, receives the updated setting, applies it to the current runtime, and stores it in the registry along with the new version number (Windows), or using Apple's UserDefaults mechanism (Mac.)

Note: Changes to failover server URLs are not retrieved by the desktop app during CU, they are retrieved during SO.

Management system desktop app settings

You can manage settings for the desktop app in the BlackBerry AtHoc management console.

To update desktop app settings, complete the following steps:

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Desktop App**.
4. On the **Desktop App** window, select the options you want according to the guidelines below.

General

The following options are available in the General section:

- **Right-click to dismiss Desktop pop-up**

  Enable this option to allow end users to dismiss the desktop pop-up with a right-click.
- **Show uninstall option in control panel and Start menu (Windows)**

  Enable this option to show the Uninstall button in the toolbar of the "Uninstall or change a program" dialog in Programs and Features when the AtHoc[edition] application is selected from the list of applications.
- **Collect workstation information (Windows)**

  Enable this option to allow the desktop app to send the machine IP address, machine name, username, and domain to the BlackBerry AtHoc server. Disable this option to reduce the amount of user information that is transferred over the network. When this option is disabled, IP targeting does not work.

The following table shows support for Collect Workstation Information in the desktop app:

Table 3: Collect Workstation Information support

Version	Notes
7.0	Machine IP and machine name. The value is retrieved in a call to baseURL.asp.

- **Stop checking for updates when Desktop is locked**

  This option is useful in environments where users do not turn off their machines. When this option is not enabled, desktop apps continue to poll the server at the CU interval when end users are away. Server resources are used for no purpose, and the "Desktop User(s) OnLine" count and graph on the management system home page show artificially high values.

- **Email Address To Send Client Logs**

  Enter an email address to send the desktop app log to. When the user selects the "Send <organization name> Log" in the Start menu for the desktop app (Windows), or when the user selects **Mail Log** in the About screen of the desktop app (Mac), the email address entered in this field receives a copy of the log file.

Audio

The following options are available in the Audio section:

- **Speaker Options**

  This option specifies how the desktop app works with built-in speakers. Select "Consider end user system settings" to prevent the desktop app from overriding the end users' local system speaker settings. Select "Always turn on speaker" to override local speaker settings. When this option is selected, the Desktop Volume Threshold slider control appears.

- **Desktop Volume Threshold**

  This option specifies the volume level that the desktop app sets the audio to.

  Note: The operating system does not provide a way for the desktop app to distinguish between headphones and speakers. When end users are wearing headphones that are plugged into the machine's audio jack, an incoming alert may sound extremely loud.

System tray menu

The following options are available in the System Tray Menu section:

- **Display System tray icon**

  The system tray icon (🌐) is the purple globe icon that appears in the system tray when the desktop app is running. Enable this option to show the icon.

- **Available Menu Items**

  Click **Manage Menu Items** to open the Desktop App Menu Items window. From this screen, you can add or edit a desktop tray menu item. When you add a menu item, note the ID that is displayed.

- **Menu Configuration**

  The XML in the Menu Configuration field creates the exact representation of the desktop menu items that are seen by an end user. Menu items have this format:

  <Item Id="8009" Type="Link"/>

where Id is the service ID. You can see the list of services in the Desktop App Menu manager. There are two item types: Separator and Link. Separators add a line in the menu that is used to separate groups of items.

Addition or removal of a menu item is picked up by desktop apps at the next Check Update.

See System tray menu for more information about System Tray menu items.

Client server communications

The following options are available in the Client Server Communications section.

Note: For BlackBerry AtHoc release 7.4 and later releases, you must have system administrator permissions to configure client server communications.

- **System Setup URL**

  This is the URL to the server where BlackBerry AtHoc is installed.
- **Check Update Interval**

  The Check Update Interval (CU) determines how frequently the desktop app polls the server for updates, including alerts. A lower value causes end users to receive desktop pop-up alerts sooner. A higher value causes users to receive desktop pop-up alerts later. The recommended value is 3 minutes.
- **Reconnect Interval**

  The Reconnect Interval specifies the interval the desktop app waits before attempting to contact the server again when the connection is lost. When a CU fails due to a lost connection, either a timeout or no Internet connection is available, the desktop app uses the Reconnect Interval setting to determine the number of CU intervals to wait before attempting to connect again. The minimum value is 1. The maximum value is 10. The default value is 2.

  This option is used in conjunction with CONNECT-INTERVAL-WINDOW.
- **Recovery Interval**

  The Recovery Interval specifies the number of CU intervals the desktop app waits before attempting to contact the server again when the server responds to a SO or CU with an error.

  The minimum value is 1. The maximum value is 10. The default value is 2.
- **Start-up Delay**

  The Start-up Delay option is a fractional value between 0 and 1 inclusive that is used to determine the amount of delay before the desktop app first attempts to sign on. A value of 0 specifies no delay and a value of 1 specifies to wait one full Check Update interval. A value of .5 specifies a delay of 50% of the check update interval.

  This setting enables you to stagger desktop app sign-ons where users arrive or return to work at the same time and reduce server load caused by many simultaneous sign-ons.

  Note: If there is no KEEPER-START value in the registry (Windows) or in the UserDefaults (Mac), the desktop app uses the value from the KEEPER-INTERVAL (the CU interval) as the random delay for sign-ons.
- **Communication Session Expires After**

  This option determines when the desktop app session is reset on the server (and the record deleted from the session table). The default value is 86400 seconds (24 hours). When the desktop app session expires, the desktop app performs a sign on at the next CU.
- **Override Default Communication Session Expiration Time After**

  By expiring desktop sessions after an interval of inactivity, this option provides a mechanism to get desktop apps to perform a sign on in environments where users do not turn off their computer. Because redirection occurs during sign on, this option can be used to get desktop apps to redirect in environments where users do not turn off their computer.

- **Group-based Check Update Interval**

  This option allows the system to override the check update interval for specific groups and give different users different check update intervals depending on the XML configuration. Select the Enable check box to view and edit the XML. Specify the value in seconds.

Failover

The following options are available in the Failover section:

- **Failover Server URL**

  Specify the URL to a server for the desktop app to connect to when the primary server is unavailable. You can specify one failover server URL. You must have a failover server that has a copy of the primary database with the same values. The desktop app updates the failover server URL only during SO. The failover server URL value on the failover server should be changed to the primary URL for the primary server before the failover server allows desktop apps to connect.

  For more information, see Failover.
- **Reconnect Attempts Before Failover**

  This option specifies the number of attempts the desktop app performs before switching to the failover server. The minimum value is 1. The maximum value is 10. The default value is 2.

Management system user authentication settings

You can manage user authentication settings for the desktop app in the BlackBerry AtHoc management console.

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. In the navigation bar, click ⚙.
3. In the Users section, click **User Authentication**.
4. Select the options you want according to the guidelines below.
5. Click **Save**.

Enabled authentication methods

Select the check boxes to enable the following authentication methods for the desktop app:

- LDAP Attribute
- Smart Card
- Username and Password
- Windows Authentication (select either Username or Domain and Username)

Assign authentication methods to applications

In the User Authentication section, the items available in the Authentication Method list are determined by the options selected in the Enabled Authentication Methods section.

- **LDAP Attribute**

  Select **LDAP attribute** from the Authentication Method list and provide an Attribute. The desktop app queries this attribute directly from the signed-in user's directory profile and sends it to the server.

  This option enables the desktop app to authenticate with an Active Directory attribute that the administrator chooses. This option allows the desktop app to operate while sending less user information to the server. When this option is selected, the desktop app does not send usernames or domain names (Windows) or domain name (Mac) in SO and CU query strings.

Select **Create new user if an account is not found** to configure the desktop app to create a user at SO if the user does not already exist.

- **Smart Card**

  Select **Smart Card** from the **Authentication Method** list to enable smart card authentication.

  - From the **Number of Certificates** list, select the number of client certificates to collect. The recommended value is 3.
  - Optionally, in the **Regular Expression** field, enter a regular expression in the following format: `UID=(? <edipi>\d{8,10})`. Contact BlackBerry AtHoc customer support to configure this field.
  - Optionally, in the **Client Regular Expression** field, enter a client regular expression in the following format: `.*?(^)(?:(?!\s-[A||E||S]).)*`. This format extracts information from the client certificate subject name to find the identical certificates for authentication. The regular expression provided in the UI is a sample expression that may not be suitable for your environment. You can build you own regular expression or contact BlackBerry AtHoc customer support to configure this field.
  - Optionally, select **Create new user if an account is not found** to configure the desktop app to create a user at SO if the user does not already exist.

- **Defer to Self Service**

  Note: This option is not supported on the Mac desktop app.

  Select **Defer to Self Service** from the **Authentication Method** list to configure the desktop app to use the user authentication method selected for Self Service. When this method is selected, end users will see a login window. When the user clicks Log In, they are redirected to Self Service to complete the sign in process. This process depends on the authentication method selected by the administrator.

  If the Self Service authentication method is set to Username and Password, the users sees a registration window and must provide their first name, last name, username, password, confirm their password, and fill in a captcha. The user has the option to register as a new user or to sign in with their existing user credentials.

  If the Self Service authentication method is set to Smart Card, the user sees a certificate selection screen and must pick a certificate. They may also be required to enter a PIN.

  If the Self Service authentication type is set to Windows Authentication, the user sees a Windows credentials screen and must provide their username and password.

  If the Self Service authentication method is set to Single Sign-On, the user is sent to the SSO URL.

- **Windows Authentication**

  Select **Windows Authentication** from the **Authentication Method** list to configure the desktop app to use only the user's Windows username or Windows username and domain. The Windows username is passed in parameter 05 during SO. See Appendix B: Desktop client URL parameters for more information about SO parameters.

  Select the **Create new user if an account is not found** check box to configure the desktop app to create a user at SO if the user does not already exist. New users are created with their Windows username as their username. If the Domain and Username option is selected in the Enabled Authentication Methods section, the user is created with "DOMAIN\username" as Username, Mapping ID, First Name, Last Name, and Display Name.

Management system desktop traffic URL

The desktop traffic URL is the Web address for the desktop app. If no desktop traffic URL is configured, desktop traffic uses the System URL. The desktop traffic URL value is returned when the desktop app requests the `baseurl.asp` before sign on.

The desktop traffic URL provides a way to configure the desktop app use a different URL than the System URL. Set up a desktop traffic URL when you need to distinguish desktop traffic from traffic from the BlackBerry AtHoc management system or from Self Service.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Change to the **System Setup (3)** organization .
3. In the navigation bar, click .
4. In the **System Setup** section, click **System Settings**.
5. On the **System Settings** page, click **Edit**.
6. In the **System Setup Parameters** section, enter the URL in the **Desktop Traffic URL** field.
7. Click **Save**.

Management system end users manager

In the BlackBerry AtHoc management system in the end users manager, the following states describe the desktop app attribute:

- **Active**: The user has connected to the desktop app within the last 30 to 60 days.
- **Inactive**: The user has not connected to the desktop app for at least 30 to 60 days.
- **Not Available**: The use has never connected to the desktop app on the current organization.

Operation

Startup

Internet connection

When the desktop app starts for the first time, there is no registry key (Windows) or data stored in UserDefaults (Mac) for the user, no check update (CU), reconnect interval, or failover settings. If the desktop app is unable to connect to the server during a first-time start up, it uses a hard-coded value of 30 minutes (Windows) or 10 minutes (Mac) to wait before attempting to connect again.

Failover at startup (Windows)

The desktop app can shut down while attempting to connect to a failover server. When the desktop app starts up later, it reads LastBaseUrlIndex. Because the value LastBaseUrlIndex will not be 0, the desktop app uses the alternate base Url for that index and attempts to connect. It is likely that the failover server will not be running, and the desktop app cannot connect. The solution is to change LastBaseUrlIndex to 0 and restart the client. An alternative is to stop the client, delete the user key, then restart the client.

Sign on

Sign on (SO) occurs each time the desktop app starts. SO is preceded by a call to `baseurl.asp`, which returns XML that includes the Base URL that the client should use for sign on. This Base URL may be different than the Base URL specified during installation. SO operations are logged by the desktop app, and can be found by searching the desktop app log for 99=SO.

For Mac, if the SO is successful, is displayed in the system tray. If the SO is not successful, is displayed.

User creation

When the desktop app connects for the first time, the server attempts to find an existing user based on the selected authentication method and the query string parameters passed by the desktop app. If a user is not found, a new user is created. You can disable user creation in the BlackBerry AtHoc management console, at **Settings > User Authentication**.

Check update

Check Update (CU) is a periodic call to BlackBerry AtHoc to get a list of sections.

When CU determines that an update is pending, it initiates a Get Update (GU).

If the CU is successful, the client shows in the system tray. If the CU is not successful the client shows in the system tray.

Get update

Get Update (GU) means to get a new version for a configuration section or for a dynamic update (DUA).

Alerts

Windows

A downloaded alert is stored in: `C:\ProgramData\BlackBerryAtHocNotifier\Htm\`

Note: If a user has more than one BlackBerry AtHoc desktop app running, they may miss an alert. End users may have the BlackBerry AtHoc desktop app installed on more than one computer, but only one desktop app at a time per user can check for updates. When a desktop app retrieves an alert for the user, the server considers the alert sent and does not allow another desktop app to retrieve that alert for the same user.

Get service

Services are actions initiated by the user from the system tray that can trigger desktop app actions (system services), open a browser window, navigate to a specific URL, and launch local applications.

Services are configured in the Desktop App menu in the BlackBerry AtHoc management system.

For testing access to Self Service, an end user can paste the GS URL in the address bar of a browser and try to bring up Self Service. However, since 00 is the user ID and 01 is the session ID, the URL is specific to the user and to the session. Self Service should launch for the end user provided that the session has not expired. The same URL does not open Self Service for another user.

Validation error (Mac)

When a user gets a Validation Error page while using any of the Self Service menu options available in the desktop app (or any other service menu option that goes through wwwroot/sps), the may be a browser setting that is blocking use of the Safari extension. Verify that the AtHoc ADC Extension is enabled in the Extensions tab in Safari preferences.

Failover

Both Windows and Mac desktop apps can fail over from one BlackBerry AtHoc server (the primary) to a secondary server. When the primary server becomes unresponsive and CUs fail, desktop apps that have a failover URL will fail over; that is, they will swap the Base URL with the failover URL. The desktop client attempts to contact the current server the number of times configured in the "Reconnect Attempts Before Failover" setting before trying the failover server.

There can be only one failover URL. You can configure the failover server URL in the BlackBerry AtHoc management system at **Settings** > **Desktop App**. The desktop app picks up the failover URL at SO but not at CU.

Failover occurs automatically. If the desktop app is unable to connect at CU, it will keep trying until it exceeds the value in "Reconnect Attempts Before Failover" in the Failover section of the Desktop App settings.

After the desktop app is connected to the failover server, if that server stops responding, the desktop app attempts to connect using the original Base URL value.

Caveats to consider when configuring Failover URLs

The user token (and possibly the userid) may be invalid when failing over or failing back. Users should be present in the failover system because it should be a recent copy of production. However, the user token or session ID may not be current which causes the server to reject the SO.

Redirection

Redirection is a way to change the server or provider ID that the desktop app connects to.

How client redirection works

Redirection occurs during the Sign On process but prior to Sign On. The desktop app sends several properties to the server when attempting to sign on. These properties, which correspond to User Attributes, are compared to the values set in the redirection rules. When there is a match, redirection instructions in the rule are processed.

When redirection is ignored for a client, an informational record is written to the diagnostic log.

Table 4: User attributes sent by the desktop app

Client property	Description
Machine IP	IPv4 address of the machine. (Windows desktop app versions from 7.0 may not pass the IP address of the machine.)
Machine Name	Computer name.
OS User Name	User's machine login name.
OS Domain Name	Domain name which the machine is logged in to.

Redirection can be to a different organization in the system, or to a different system and organization.

Note: The Desktop Software Authentication mode must be the same in both organizations.

Note: The Collect Workstation Info option in **Settings** > **Desktop App** > **General** must be enabled in the desktop app gateway of the source organization.

Note: The Create New User if an Account is Not Found option in **Settings** > **User Authentication** > **Assign Authentication Methods to Applications** must be enabled in the target organization.

Redirection during first time sign on

For redirection across systems, redirection is logged in the end user's properties on organization 1. A user is created in organization 1.

For redirection in the same system, redirection is logged in the user's properties in the new organization. A user is not created in organization 1.

Redirection after first time sign on

For redirection across systems, redirection is logged in the end user's properties in the "from" organization.

For redirection in the same system, redirection is logged in the end user's properties in both the "from" and the "to" organizations.

Enable redirection

Redirection is disabled by default. You must have system administrator permissions to configure redirection.

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click .
4. In the **System Setup** section, click **System Settings**.
5. On the **System Settings** page, click **Edit**.
6. In the **Redirection Settings** section, select **Enable Client Redirection**.

Add redirection rules

You must have system administrator permissions to configure redirection rules.

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click .
4. In the **System Setup** section, click **System Settings**.
5. On the **System Settings** page, click **Edit**.
6. In the **Redirection Settings** section, click **Redirection Rules**.
7. On the **Redirector Rules** screen, click **Add New Rule**.
8. On the **Add new redirect rule** dialog, in the **VPS** list, select an organization.
9. In the **Attribute Name** list, select one of the following values: **Machine IP**, **Machine Name**, **OS Domain Name**, or **OS User Name**.
10. In the **Operator** list, select one of the following options: **contains**, **starts with**, or **does not contain**.

   Note: Only one rule with the **does not contain** option is allowed per organization. You can use multiple comma-separated criteria in a single record.
11. In the **Criterion** field, add a valid criterion based on the selection you made in the Attribute Name list.
12. In the **Redirect To URL** field, enter a valid URL for redirection.
13. In the **Redirect To VPS ID** field, enter an organization ID.
14. Optionally, select the **Skip Url Reachable test** check box, if you are sure that you have entered a valid redirection URL.
15. Click .

The new redirection rule is added to the Redirection Rules screen.

Exempt redirection

At the top of the Redirector Rules window there is an "Exempt redirection for users with username containing" field. Use this field to ignore certain users when processing redirection rules. Text entered in the field is right-compared with the OS User Name passed by the desktop app. If the text in the field is found in the middle of OS User Name, that is not a match. The text in the field must appear at the right end of OS User Name for there to be a match. The character matching is not case sensitive. Comma-separated values are allowed.

When redirection is ignored for a desktop app, an informational record is written to the diagnostic log.

Examples:

OS user name	Exempt text	Redirection
JSMITH.ADMIN	admin	No

OS user name	Exempt text	Redirection
JOHN.SMITH	admin	Yes (Assuming a redirection rule applies to this user.)
JSMITH.ADMIN.USER	admin	Yes (Assuming a redirection rule applies to this user.)
JSMITH.ADMIN2	admin,admin1,admin2,admin3	No

Note: Exempt text can be a .csv list.

System tray menu

For new desktop app deployments, the BlackBerry AtHoc Management System menu item in the desktop app system tray menu is no longer included by default. Enterprise administrators and organization administrators can add the BlackBerry AtHoc Management System menu item in the System Tray Menu XML. If the menu item is added, all operators connected to the desktop app will start to see the menu item after the next get update (GU) call. For existing desktop app deployments, the BlackBerry AtHoc Management System menu item will be removed from the desktop system tray menu when:

- An enterprise administrator or organization administrator makes any update to the system tray menu XML.
- The desktop app gateway is saved.
- The desktop app completes a GU call to retrieve new System Tray Menu XML for the organization.

Only users with operator permissions will see the BlackBerry AtHoc Management System menu item.

Operators can configure the items that appear in the Desktop App system tray menu.

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Desktop App**.
4. On the **Desktop App** window, in the **System Tray Menu** section, select **Display System Tray Icon**.
5. Click **Manage Menu Items**.
6. On the **Desktop App Menu Items** window, click **Add Menu Item**.
7. On the **Add Menu Item** window, enter a name and URL for the new menu item.
8. Click **Save**. Take note of the ID of the new menu item.
9. Add the new menu item to the Menu Configuration XML in the **Menu Configuration** field.

   Menu items have this format: <Item Id="8009" Type="Link"/>
10. Optionally, add a separator to the Menu Configuration XML.

   Separators have this format: <Item Type="Separator" />
11. Optionally, cut and paste the code for each additional function to add or move menu items and separators.
12. Click **Save**.

The following menu items are available:

Option	Included by default	Code
Check for New Alerts	Yes	8009
Dismiss All Popups	Yes	8022
Access Self Service	Yes	521
Update My Info	Yes	530
Update My Device Info	Yes	531
About	Yes	8005
BlackBerry AtHoc Management System	No	532
Connection Options...	No	8008
Deskbar always on top	No	8013

The following is a sample Menu Configuration XML:

```
<SystrayLayout>
  <Item Id="8009" Type="Link" />
  <Item Id="8022" Type="Link" />
  <Item Type="Separator" />
  <Item Id="521" Type="Link" />
  <Item Id="530" Type="Link" />
  <Item Id="531" Type="Link" />
  <Item Type="Separator" />
  <Item Id="8005" Type="Link" />
</SystrayLayout>
```

There are global menu items and items that are private to a specific organization. Global menu items are defined in one of the setup providers, for example organization 3 and organization 1. Private menu items are defined in the working organization.

A global change to one of the existing menu options such as 521 "Access Self Service" can be made in organization 1. A change to the global setting (for example the query string) affects server-side processing, so there is no need for desktop app clients to do a check update for the change to take effect.

Addition or removal of a menu item is picked up by desktop app clients at the next get update.

When a public menu item is deleted without changing the system tray menu XML, users will see a server error when accessing the menu option.

Add a custom URL

Custom URLs can contain query string parameters. The Static value allows you to hard-code a name-value pair.

Authentication

Authentication options are accessed in the BlackBerry AtHoc management system at **Settings** > **User Authentication**.

Use LDAP attribute

You can use LDAP attributes to provide authentication without Windows usernames and domain names being sent outside of the domain.

Organization configuration

You can configure your organization to use the LDAP attribute for authentication.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** screen, in the **Enabled Authentication Methods** section, select the **Enable** check box next to LDAP Attribute.
5. In the **Assign Authentication Methods to Applications** section, select **LDAP Attribute** from the Authentication Method list in the Desktop app section.
6. In the **Attribute** field, enter the Active Directory attribute to use for authentication. For example, mail.
7. Optionally, next to **Create New User if an Account is not Found**, select **Enable**.
8. Click **Save**.

Migrate existing users to LDAP attributes

LDAP Authentication is based on the end user's Mapping ID. When migrating existing users to LDAP authentication, and the mail attribute is used, the end user's Mapping Id attribute must contain the end user's email address from Active Directory. To migrate existing users to use LDAP attributes, complete the following tasks:

- Configure the LDAP Attribute option in the BlackBerry AtHoc management system and enter the attribute, as described in Organization configuration.
- Update the end Mapping ID for each user. For example, when using the LDAP mail attribute, set the Mapping ID to the value of the user's email address in Active Directory.
- Restart the desktop app.

When the desktop app starts, it receives instructions from the server about the LDAP attribute to use. The desktop app then queries Active Directory for the value of that attribute for the local user. In order for the desktop app to query Active Directory, users must have at least read-only permission to their Active Directory. The desktop app sends the value of the attribute to the server. The server performs a user search where the Mapping ID in each user record is compared to the attribute value. If a match is found, the desktop app is connected to the user record in the system and the user can then receive alerts that are targeted to them.

If the LDAP attribute values have not been synchronized to the Mapping ID field, or if the value is not matched to an existing user in the BlackBerry AtHoc system, a new user is created. Starting with BlackBerry AtHoc server version 7.0.0.1 there is a "Create new user if an account is not found" option that is not selected by default. This is to prevent desktop apps from creating a user, and to prevent the desktop app from creating duplicate users when a user's Mapping ID has not been set correctly. Select this option to enable the desktop app to create users.

If the desktop app cannot query Active Directory, it waits until it can (Windows), or it tries to connect using the Windows domain and username authentication method (Mac). The desktop app caches the designated attribute in the registry (Windows) or in UserDefaults (Mac), and uses the cached copy if access to Active Directory fails.

Desktop app configuration

When the authentication mode is changed in the User Authentication settings, you must stop and then restart the desktop app to apply the new settings.

If the user does not have read access to Active Directory, the registry value can be updated manually or with a Group Policy Object (GPO). Each user has a different value, for example email address, so the GPO must take that into consideration.

The client session

A desktop app session, also known as a client session, is created at Sign On (SO), when a session record is created in the database. The desktop app is not continuously connected to the server. The desktop app connects temporarily at SO and when it polls the server at the check update (CU) interval.

When the user shuts down the machine (or locks it and the "Stop checking for updates when Desktop is locked" option is selected in the Desktop App page in Settings in the BlackBerry AtHoc management system), the user's session becomes stale because the desktop app stops polling the server and is not able to do a CU. The Desktop Sessions Maintenance job runs every 30 minutes to clean up stale sessions.

Stale sessions

There are three ways that the desktop app session becomes stale:

1. A CU has not been performed for an interval of 1.5 times the CU interval plus 30 seconds.
2. When the desktop app logon has run for longer than the value set for Communication Sessions Expires After in the Desktop App gateway. The default is 86400 seconds.
3. When the desktop app is inactive for longer than the value in "Override Default Communication Session Expiration Time After" option in **Settings** > **Desktop App**, when the value is not zero.

Home page chart

Data for the home page chart comes from the session table. The session table is used to store data about active desktop app sessions. The home page chart has a 30 minute granularity, which is due to the 30-minute interval between runs of the "Desktop Sessions Maintenance" system task that cleans up stale desktop sessions. See The client session and Stale sessions for an explanation of how the desktop session becomes stale.

When the AtHoc Desktop Integrated Pool is recycled, desktop apps are unable to perform a CU until the recycle completes. If a desktop app attempts a CU when the application pool is recycled and is unable to connect, and if the desktop session maintenance system task runs immediately after that, only one CU was missed. A session becomes stale when a CU has not occurred for 1.5 times the CU interval plus 30 seconds, so the desktop app may be able to do a CU before the session is deemed stale. You will not see that any of these events occurred by looking at the home page chart.

Desktop apps continue to try to connect when the application server is unable to process requests. For example, when IIS is stopped or when the server is swamped by too many requests. In this situation, stale sessions are cleaned up (that is, the records are deleted) when "Desktop Sessions Maintenance" runs.

Troubleshoot desktop app issues

This section describes issues you may encounter after installing the BlackBerry AtHoc desktop app on users' desktops. In most cases, the solutions provided in this chapter resolve these problems. If they do not, contact BlackBerry AtHoc customer support at athocsupport@blackberry.com.

Access Desktop App details

Before contacting BlackBerry AtHoc customer support for help with problems you are having with the AtHoc Desktop App, you should open the application details screens for the particular version of the application that you are running. The information contained on these screens is useful for the Support team as they work to diagnose and fix the problem you are encountering.

Click and select **About** from the menu that appears to access the application details screens.

The **System Information** tab shows if the app is currently connected to a BlackBerry AtHoc server and the server URL. The **Connection Status** field displays Connected if you have a connection and the **Server Base URL** field displays the URL of the server you are connected to.

The **About** tab displays the version of the Desktop App that is installed on your machine. If the Support team requests that you send them your system details, you can export that information by clicking the **Export System Information** button on the screen. You can also open your log file or copy and mail your log file path by clicking the corresponding button on the screen.

Read the desktop app log

Windows

- Click the globe icon in the System Tray and then select **About** > **Open Log File**.
- The log is stored in `C:\ProgramData\AtHoc[edition name]`. The log accumulates to 1 MB, then is overwritten.

Log Format

The following is an example log entry:

```
Date Time User Thread Subroutine Message
2015-01-15 00:44:31 [NT AUTHORITY\SYSTEM] 000012B0 CBackChannel::Initialize
 ProviderId: 2050329
```

Column name	Value
Date	2015-01-15
Time	00:44:31
User ([Domain name\User name])	[NT AUTHORITY\SYSTEM]
Thread ID	000012B0
Subroutine	CBackChannel::Initialize

Column name	Value
Message	ProviderId: 2050329

Note: Column headers do not appear in the desktop app log file.

Mac

- Click the globe icon in the System Tray and then select **About** > **Open Log**.
- The log is captured for the last 6 hours.

Log Format

Note: Column headers do not appear in the desktop app log file.

The following is an example log entry:

```
Date        Time                    Hostname  Process        PID      Message
2020-08-28            14:50:10.831389+0530  localhost AtHoc ADC Agent[41161]:
 AtHoc ADC: Starting up
```

Column name	Value
Date	2020-08-28
Time	14:50:10.831389+0530
Hostname	localhost
Process	AtHoc ADC Agent
PID	41161
Message	AtHoc ADC: Starting up

Connection issues

The following sections detail connection-related issues and how to troubleshoot them.

Gray globe - desktop app not connected

A "gray globe" icon with a red circle that has a white "x" inside indicates that the client is not connected:

The client will not appear connected until it successfully completes Sign On. There will be log entries near the point of Sign On that can point to the issue. To find where Sign On takes place, search the log for the Sign On action which is "99=SO" in the URL:

```
...https://(server)/csi/session/action.asp?99=SO&00=-2050329.1&....
```

If you do not find this entry, search the log for the entry where it downloads `baseurl.asp`. This entry occurs just before Sign On:

```
...https://(server)/config/baseurl.asp?PID=2050329....
```

Gray globe - user account is disabled (Windows)

A "gray globe" icon with a yellow circle that has a white "x" inside indicates that the user account is disabled in the BlackBerry AtHoc system: .

Check your ability to receive alerts

After the desktop app launches successfully, the appears on your screen, indicating that you are connected to the BlackBerry AtHoc server and are ready to receive alerts.
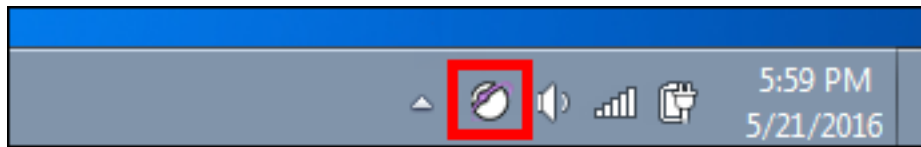
If the desktop app has been installed but it is disconnected from the BlackBerry AtHoc server, the icon is grayed-out with a red circle with a white "x".

When the desktop app is disconnected, the app cannot receive alerts.

Windows: If your account has been disabled, the icon appears in gray with a yellow circle () and you cannot receive alerts.

Desktop app is not receiving alerts

If you do not receive any alerts after installing the desktop app, check the following:

• Was your User ID targeted? To find out if it was, contact the Operator who created the alert and ask them to confirm that your User ID was part of the target group. You can find your User ID by clicking and selecting **About** from the menu that appears. Your User ID is listed at the top of the Value column on the System Information tab.

• Is your BlackBerry AtHoc desktop app connected to a server? Is it the correct server?
• Was your account enabled in the BlackBerry AtHoc system? If the desktop app icon appears in gray with a yellow circle (), your account is not enabled.

To view the server settings, follow the steps in Desktop app does not connect.

Desktop app does not connect

The (Globe - connected) icon displays when it is connected to the BlackBerry AtHoc server.

The (Globe - disconnected) icon displays when the desktop app is disconnected.

Windows: The (Globe - disabled) icon displays when the user account is disabled in the BlackBerry AtHoc system.

The app might not connect to the BlackBerry AtHoc server due to the network configuration. To resolve the problem, do the following:

- Ensure the app workstation is connected to the network.
- Verify that proxy and firewall settings are not blocking access in your browser and the Connection Settings for the app.

To verify that your app is connected to the correct server, complete the following steps:

1. Click .
2. In the menu that appears, click **About**.
3. On the **About** screen, click the **System Information** tab if it is not already open.

   The **Connection Status** should be Connected and the **Server Base URL** should point to the BlackBerry AtHoc server. If the base URL is wrong, the usual fix is to uninstall the app and then install it, inputting the correct set of input parameters, which includes the base URL for the server.

WinInet errors and warnings

Warning require client certificate 12044.

This error occurs when using HTTPS and "VALIDATECERT=N" in the `run.bat` file , but SSL is set to "Require SSL" for the wwwroot\csi web application.

If using HTTPS, you may see an entry that indicates the SSL configuration of IIS:

`"Validate cert 84C80300" or "IGNORE cert 84C83300"`

For more information, see Certificate issues.

ERROR Could not send request due to: 12xxx

This is a standard WinInet error. This error occurs for reasons indicated by the description of the particular error. Here are some common errors:

- 12002, "The request has timed out."

  Look into server performance issues such as high CPU usage and a large number of sign on attempts.
- 12007, "Internet name not resolved."

  This error can indicate a DNS issue.
- 12029, "Cannot connect."

  This error has several possible causes:

  - A proxy is required but the "Use a proxy server" check box (in **Internet Explorer** > **Internet Options** > **Connections tab, LAN Settings**) is not selected.
  - A rule to have client traffic bypass the proxy is not configured when a proxy server is used.
  - A recent change for firewall settings on the server.
- 12031, "Connection reset."

  This error message may be displayed if the desktop app was pointed to the failover server to allow upgrade of the production server and the failover server was set to the production server, causing a circular loop.
- 12157, "Security channel error."

HTTP status codes

The following are standard HTTP status codes:

`Http status code with certificate: [status code]`: The "with certificate" indicates the HTTPS branch.

`Http status code: [status code]`: Indicates the HTTP branch that does not handle certificates.

Status Codes

- 403, "forbidden": Usually indicates a certificate issue.
- 407, "Proxy authentication required": Indicates the need to enable the use of a proxy.
- 500, server error: Look in the diagnostic log or Windows logs, or enable logging in IIS.

Certificate issues

If you are experiencing client certificate issues, check the following items:

- If there is a Tumbleweed client on the server, make sure it is running.
- Windows: Check if there are too many certificates in the user's store. There is a limit to the number of certificates that can be tried before a timeout. The number is about 150 certificates.
- Windows: An intermediate certificate issued by the organization prevents the desktop client from connecting. Remove the intermediate certificate to resolve the problem.
- If your desktop client does not authenticate, it may be due to nonstandard formatting in your CAC certificate. Contact BlackBerry AtHoc customer support and request that an organization-specific regular expression be configured for your system.

Sign on and check update issues

Gray Globes

-
  Many, but not all, users see gray globe ( ) icons.

  This occurs when the server is under powered or trying to support too many desktop app users. Other symptoms include high CPU use in the desktop application pool worker processes, or timeouts in the IIS log for SO and CU.

  When the server is not under powered and CPU use is not high, check for a bad disk on the database server.

-
  All users see gray globe ( ) icons.

  Check to see if there is a Tumbleweed or Axway client that checks the certificate revocation list. If there is a Tumbleweed or Axway client, make sure they are running.

  Check if there needs to be a proxy exclusion for the desktop app client.

High CPU use by application pool worker processes

High CPU use by application pool worker processes may be caused by one of the following conditions:

- An under-powered application server: With a single application server with 4 CPUs and 4 GB RAM, the desktop application pool worker processes use about 50% each. In this case, two worker processes use 100% of the available CPU.
- Symantec Endpoint Protection Service is scanning the database files.

Self Service issues

The following topics describe Self Service issues and how to troubleshoot them.

Multiple prompts for certificate (Windows)

The following are some known scenarios for multiple prompts for certificates:

1. Users see multiple prompts to pick a certificate when attempting to bring up Self Service from the desktop app menu.

   This may be due to the CTL (certificate trust list) putting too many certificates in the certificate store causing the certificate validation to time out. The solution is to remove any certs that are not needed.

   For more information, see http://support.microsoft.com/kb/931125.
2. Users see a prompt to pick a certificate every few minutes.

   In the IIS console under CSI web application, the "Client certificates" option in SSL Settings feature is not set to "Ignore."
3. Users are prompted to select a certificate several times when trying to access Self-Service from the "Access Self-Service" menu in the desktop app menu.

   This does not happen when using the Self-Service URL.

Server error 404 - File or directory not found (Windows)

This error may be preceded by an "Automation server can't create object" error. The URL looks like: https:// alerts4.athoc.com/3125901.

Prompts to enable extension (Mac)

Users see prompts to enable an extension when attempting to start Self Service from the desktop app menu. The prompts appear when the Mac desktop app extension is not enabled in Safari. To resolve this issue, in Safari, go to preferences and enable the AtHoc ADC Extension on the Extensions tab.

Appendix B: Desktop client URL parameters

This excerpt of a URL from a client log is an example of a "sign on":

```
https://<server>/csi/session/action.asp?99=SO&00=-2050329.1&02=0&03=2050329...
```

Table 5: Desktop client URL parameters

Parameter	Sign on	Check update	Get update	Get service
99	SO	CU	GU	GS
00	Userid	Userid	Userid	Userid
01	—	Session id	Session id	Session id
02	Token	Toolbar status: (Obsolete)	Section	Service id
03	Pid	Client version	—	Search box topic
04	Sign on attempt number	Explorer windows count (Obsolete)	—	URL/file (current location, before navigation)
05	Windows username (or domain user name)	BHO registry status (Obsolete)	—	AID (alternate service ID, from the service definition)
06	Windows domain (domain name)	Operating system	—	Launching application (what browser/deskbar)
07	Machine name	Mac: Safari version	—	Operating system (not supported
08	Client metastore (was platform)	Registered platforms (Windows: for example IE, Deskbar)	—	FF1 (from service definition)
09	Client IP	Client IPs	—	FF1 (from service definition)
10	LDAP attribute value	—	—	FFN (from service definition)
11	—	—	—	Title of current HTML page (if any)

Parameter	Sign on	Check update	Get update	Get service
12	—	—	—	Target URL / file (for navigation)
15	Logon user name	—	—	—
98	Client certificate	—	—	—

BlackBerry AtHoc Customer Support Portal

BlackBerry AtHoc customers can obtain more information about BlackBerry AtHoc products or get answers to questions about their BlackBerry AtHoc systems through the Customer Support Portal:

https://www.blackberry.com/us/en/support/enterpriseapps/athoc

The BlackBerry AtHoc Customer Support Portal also provides support via computer-based training, operator checklists, best practice resources, reference manuals, and user guides.

Documentation feedback

The BlackBerry AtHoc documentation team strives to provide accurate, useful, and up-to-date technical documentation. If you have any feedback or comments about BlackBerry AtHoc documentation, email athocdocfeedback@blackberry.com. Please include the name and version number of the document in your email.

To view additional BlackBerry AtHoc documentation, visit https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc. To view the BlackBerry AtHoc Quick Action Guides, see https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc/Quick-action-guides/latest.

For more information about BlackBerry AtHoc products or if you need answers to questions about your BlackBerry AtHoc system, visit the Customer Support Portal at https://www.blackberry.com/us/en/support/enterpriseapps/athoc.

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada