BlackBerry AtHoc Desktop App

Installation and Administration Guide (for Microsoft Windows)

6.2.x.278

Contents

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*.

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.

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.

Request a new desktop app

To request a new desktop app, complete the following steps:

1. Go to the following URL:

   http://dsw-request.athocdevo.com/

   You must be connected directly to the BlackBerry AtHoc network or connected through a VPN to access the link.
2. In the **Contact Information** section, enter your full name and email address. You will receive an email when the new desktop app is available.
3. In the **Client Information** section, complete the following fields:
   - **Client Name**—Required. Enter the name of the organization. The client name appears in the list when running the installer manually. The client name is not an installation parameter.
   - **Client Edition**—Required. There are three generic editions: AtHocConsumer (for non-commercial, non-government use), AtHocCorp (for commercial customers), and AtHocGov (for military and government customers). Most requests should use one of these generic editions. Other editions have specific customizations such as the ability to choose from several organizations during installation.
   - **Client Version**—Required. Always choose the newest version unless there is a reason to choose an older one.
   - **Base URL**—Required.
   - **Provider ID**—Required.
4. In the **Client Information** section, select **Yes** or **No** for each of the following required options:
   - RunAfterInstall
   - Silent—Select **Yes** when using the `run.bat` file to install the desktop client.
   - MandateSSL
   - ValidateCert
   - UninstallOption
   - Audio

   Note: For more information about these options, see Run.bat.

   Note: There is only one option to select for the **VPS** field: Single. This means that only one organization appears in the organization list during installation when you run the installer manually.
5. In the **Additional customizations** section, select from the following options:

- **VPSList 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:"
- **Manual Selection**—The default is No. Select **Yes** to make a button appear on the organization dialog that allows the user to enter the base URL and organization ID during installation.
- **Schedule Reboot**—The default is No. Select **Yes** to configure the installer to schedule a reboot of the machine after installation.

6. Click **Submit**.

For more information about the desktop app installation options, see:

- Installation settings
- Run.bat
- Appendix A: Build settings

Installation methods

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

1. 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. 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. 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. 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.

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 uses ActiveX and works with Internet Explorer (IE) only.

Table 1: Summary of platform support

Desktop App	Internet Explorer	Windows	Server
6.2.x.270 and newer	9 and newer	10, 7	6.1.8.87 and newer. These versions support the "Collect Workstation Info" and "Sign on with LDAP attributes" options.

Desktop App	Internet Explorer	Windows	Server
6.2.x.269 and older	7 and newer	7, Vista, XP	6.1.8.84 and newer.

Installation artifacts

This section describes the artifacts (folders, files, and registry keys) 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 2: Installation artifact file folders

Folder name	Location	Contents	Example
AtHoc[edition]	In the 32-bit ProgramFiles folder	All client executable files	C:\Program Files (x86)\AtHocGov
AtHoc[edition]	In the CommonAppDataManufacturer folder	All other files included in the installer	C:\ProgramData\AtHocCorp

Files

The standard BlackBerry AtHoc desktop app installers contain the files described in the following table; custom installers can package more WAV files:

Table 3: Desktop client installer files

File	Description	Notes
AtHoc[edition].exe	The desktop application.	—
AtHoc[edition]GSHtmlCl.dll	File that uses Internet Explorer to create the alert pop-up.	—
AtHoc[edition]SystemInfo.dll	File that contains the code for the "Export System Information" button on the About dialog of the desktop app.	—
AtHoc[edition]TBr.dll	Legacy toolbar add-on for Internet Explorer.	—
.ico	—	Not used.

File	Description	Notes
999100.bmp	Deprecated AtHoc logo used in alerts. A new copy is downloaded at first GU.	Not used.
1.wav	Deprecated default audio file.	Not used.
Audio.xml	Deprecated default audio configuration file.	Not used.
Default.xml	Deprecated toolbar configuration file.	Not used.
Null.xml	Legacy file.	Not used.
Sync.xml	Deprecated toolbar synchronization file.	Not used.
systray-menu.xml	The default system tray configuration file. This file is used until the first GU downloads the organization-specified menu.	—
Blank.html	The default browser page to show in a browser pop-up window.	—

Registry keys

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

`HKLM\Software\SysWow6432Node\AtHoc[edition]`

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 "AtHoc[edition]" folder in the CommonAppDataManufacturerFolder. For example:

`C:\ProgramData\AtHoc[edition]`

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

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

The installation process creates several registry keys to register the ActiveX control that interacts with the user's machine to read and write the registry, play the audio file for an alert, and display the pop-up alert. These keys have names like `AtHoc[edition].LegacyFunctions` and `AtHoc[edition].Toolbar`.

Remove the toolbar from IE

If you are using the version .273 installer, perform the following steps to remove the toolbar from IE:

1. Look up the BrowserHelper (AtHoc[edition]BrowserHelper) for the edition and make a note of the GUID in the CLSID.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Browser Helper Objects` and delete key with the name that is the same as the GUID from Step 1.

3. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer \Extensions` and find the AtHoc Corp IE extension by selecting each item and looking at the name, and delete it {D2490E6A-1A5E-4997-A6F8-24ECB9D5FF93}.
4. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer \Toolbar` and delete the registry value DAF2720A-F5AA-4114-BC8A-B7F3E7F8EF85. This value is displayed as AtHoc IT Alerts in IE add-ons.

See Startup for information about files and registry settings that are created at startup.

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 User if none Exists" 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

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 to disable removal of the 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 [EditionName].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 produc_guid here:

  ```
  HKLM\Software\Wow6432Node\AtHoc[edition]\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 the desktop app log, or the Start menu folder with the organization name.

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

For release 6.1.8.90 or earlier, the desktop app downloads a `config\baseurl.asp` file and receives a response that is about 1184 bytes. The desktop app then makes a sign-on request (99=SO) and receives a response that is about 232 bytes. The total sign-on traffic is about 1416 bytes.

For release 7.0.0.1 and later, the ASP code base is replaced with ASP.Net, but the download size is the same.

Check-update traffic

For release 6.1.8.91 or earlier, the desktop app makes a Check Update request (99=CU) and receives a response that is about 564 bytes.

For release 7.0.0.1 and later, the ASP code base is replaced with ASP.Net.

If check update 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. The desktop app saves the settings in an XML file in the user's `AppData\Local\AtHoc[edition]` folder. For example, `AppData\Local\AtHocGov`.

First-time sign on traffic

During a first-time sign on (that is, every time the desktop app starts up or when the session expires), the desktop app downloads all settings. This includes about nine files, for a total of about 5291 bytes, depending on factors such as the number of items in the system tray menu.

Alert traffic

Alert downloads can include a WAV or logo file. The alert is downloaded as an XML file with a name such as `DUA209999990.XML`. The alert file is stored in the user's `AppData\Local\AtHoc[edition]` folder. If the alert includes audio, the WAV file is downloaded separately and stored in the `ProgramData\AtHoc[edition]\wav` folder if not already present on the user's machine.

The following table shows the relationship between logo size and alert payload size.

Table 4: Image sizes and payload types

BlackBerry AtHoc release version	Image size (in bytes)	Alert payload size (in bytes)
6.1.8.87CP1	None	13,265
6.1.8.87CP1	3,225	30,318
6.1.8.87CP1	50,676	283,421[1]
7.0.0.1	None	12,702
7.0.0.1	3,225	15,010

BlackBerry AtHoc release version	Image size (in bytes)	Alert payload size (in bytes)
7.0.0.1	50,676	23,090

The above values are close approximations of the actual network traffic. The values are the size of the response text or files at the user's computer and do not consider compression or HTTPS.

[1] The discrepancy in number of bytes between a payload with no image and one with an image is due to the image appearing as a binary blob in four locations in the code that is downloaded. This is a known issue in the server code base for release 6.1.8.90 and earlier. Versions 7.0.0.1and later do not have this issue.

Desktop app settings

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

Build settings

The build environment on the server where the automated build occurs relies on two utilities and three configuration files.

The utilities are `build.exe` and `PackageDSWToMsi.exe`. Both utilities are Visual C# projects. The `BuildHelpers.sln` generates the `build.exe` utility. `BuildATSrcWxs.sln` generates the `PackageDSWToMsi.exe` utility.

The configuration files are `Options.xml`, `DSWMsiBuildInfo.xml`, and `install.ini`.

The `Options.xml` configuration file contains options that control MSI behavior.

The `DSWMsiBuildInfo.xml` configuration file contains the MSI product and package GUIDs and product information.

The `Install.ini` configuration file contains COM GUIDs that are used when compiling the DLLs.

See Appendix A: Build settings for details about these files.

Installation settings

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. See Options.xml schema for more information about adding Provider ID and base URL values 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 AtHocCorpDSW6.2.3.270.msi /l*vx AtHocCorpDSW6.2.3.270.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 AtHocCorpDSW6.2.3.270.msi /l*vx AtHocCorpDSW6.2.3.270.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.”

`AtHocCorpDSW6.2.3.270.msi` is the name of the installer associated with the switch.

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

`AtHocCorpDSW6.2.3.270.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 5: 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` **Written to:** `HKLM/SOFTWARE/Wow6432Node/AtHoc[edition]/BASEURL`
PID	Provider ID. The organization that the desktop app should connect to. **Required:** Yes **Format:** `http://<server_name_or_ip>/config/baseurl.asp` **Written to:** `HKLM/SOFTWARE/Wow6432Node/AtHoc[edition]/PROVIDER ID`
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 **Written to:** `HKLM/SOFTWARE/Wow6432Node/AtHoc[edition]/RunAfterInstall` There is no HKCU copy. **Added to:** `HKLM/SOFTWARE/Wow6432Node/Microsoft/Windows/CurrentVersion/Run`
DESKBAR	Specifies if the Deskbar (`AtHoc[editionName]Desk.exe`) should run. The Deskbar is a toolbar that appears on the Windows desktop. The feature in the BlackBerry AtHoc management system that creates Deskbar menu options has been removed, so the Deskbar no longer has any use. This element was removed from the installer in release 6.2.x.27x. **Required:** No **Values:** Y or N **Default:** N

Element	Description
TOOLBAR	Specifies whether or not the Toolbar (`AtHoc[editionName]TBr.dll`) should run. This is the toolbar that appears in Internet Explorer. The feature in the BlackBerry AtHoc management system that creates Toolbar menu options has been removed, so the Toolbar no longer has any use. This element was removed from the installer in release 6.2.x.27x. **Required:** No **Values:** Y = Enabled. The user is prompted to allow or disable the toolbar when IE starts. The toolbar appears in the Manage add-ons dialog. N = Disabled. **Default:** Y
SILENT	Specifies if the MSI user interface (UI) should be displayed to the user. **Required:** No **Values:** Y = Do not show the UI. N = Show the UI. 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. **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 **Written to:** `HKLM/SOFTWARE/Wow6432Node/AtHoc[edition]/MandateSSL` There is no HKCU copy.

Element	Description
VALIDATECERT	Specifies if a valid certificate is required. **Required:** No **Values:** Y = Certificates are checked for validity. Server certificates must not be expired, revoked, or otherwise invalid. N = Certificates are not checked. 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 **Written to:** `HKLM/SOFTWARE/Wow6432Node/AtHoc[edition]/ValidateCert` There is no HKCU copy.
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. The `<UninstallOption>no</UninstallOption>` node in the `options.xml` file has a default value of "Yes." The value in the `options.xml` file is overridden by the value in the `run.bat` file. **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. Most settings are stored in the registry, the rest are stored in XML files in the user's AppData folder. The settings described in this section are present in all 6.2.x.x versions of the desktop app.

Desktop app settings updates

Settings that are stored by the desktop app in the user's registry key (hkcu) 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.

Each key under `hkcu\AtHoc[edition]` includes a Version value except metaStore. Note that 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 the (Settings) icon.
3. In the Devices section, click **Desktop App**. The Desktop App window opens.
4. 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.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\PROVIDER\ ENABLERCLICKCLEARPOPUP`
- **Show uninstall option in control panel and Start menu**

  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.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\PROVIDER\NoUninstall`
- **Collect workstation information**

  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 6: Collect Workstation Information support

Version	Notes
6.2.x.270	Machine IP.
6.2.x.271+	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.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\PROVIDER\blockRequestIfLocked`
- **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, the email address entered in this field receives a copy of the log file.

This option is stored in:

`hkcu\software\AtHoc[edition]\PROVIDER\clientLog`

- **ActiveX Object Name**

  Enter the ActiveX object name for the desktop app. This is used when creating the JavaScript code that is sent by the server to the desktop app in response to requests and in alerts. For example, when the user selects the “Access Self Service” menu option, selects a response option, or clicks a button on an alert.

  The JavaScript code is generated dynamically and when it executes on the user’s machine it attempts to create an object using the value that appears in this field. For example, `AtHocCorpGStlbar.GShelper`. If the value does not match the desktop app edition, an error occurs. Depending on the feature accessed, the user may see “Error: Automation server can't create object” or “Validation Error.”

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.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\SYSTEM\systray-visibility`
- **Available Menu Items**

  Click the **Manage Menu Items** link 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. Changes to a menu item take effect immediately (without CU) because the GS request is processed server-side, and the resulting service URL is passed back to the desktop app.

The system tray menu is stored in the user's `AppData\Local\AtHoc[edition]` folder, in `SYSTRAY-MENU.XML`.

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:

- **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 2 minutes.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\system\KEEPER-INTERVAL`
- **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 (stored in `hkcu\software\AtHoc[edition]\SYSTEM\CONNECT-INTERVAL-WINDOW`). For more information, see the "User key" section in Registry settings.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\SYSTEM\CONNECT-INTERVAL`
- **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.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\SYSTEM\RECOVERY-INTERVAL`
- **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, the desktop app uses the value from the KEEPER-INTERVAL (the CU interval) as the random delay for sign-ons.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\SYSTEM\KEEPER-START`
- **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**

  This option provides a mechanism to expire desktop sessions that were created by the SYSTEM user. Sessions can be created by the SYSTEM user when desktop apps are deployed with SCCM and RUNAFTERINSTALL is set to "Y". Sessions can be created by the SYSTEM user when SCCM is used to update machines after the desktop app is installed.

  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.

  There is no registry value for this setting.
- **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 primary server allows desktop apps to connect.

  For more information, see Failover.

  This option is stored in:

  `hkcu\software\AtHoc[edition]\alternateBaseUrl1`
- **Reconnect Attempts Before Failover**

  This option specifies the number of attempts the desktop app performs before switching to the failover server.

Management system user authentication settings

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

To update user authentication settings, complete the following steps:

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

Enable 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 Enable 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 Windows usernames or domain names in SO and CU query strings.

  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.

  This option requires desktop app version 6.2.x.271 or later.
- **Smart Card**

  Select **Smart Card** from the Authentication Method list to enable smart card authentication. Select the number of client certificates to collect. The recommended value is 3.

  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.
- **Defer to Self Service**

  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 SmartCard, 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 External URL, the user is sent to a configured external URL for Single Sign On (SSO).
- **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 Enable 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.

To configure a desktop traffic URL, complete the following steps:

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

Registry settings

The AtHoc[edition] registry key in `HKLM/Software/Wow6432Node` (known as the “machine key”) is created during installation and contains the default connection settings and the configuration settings sent on the command line to the MSI.

The AtHoc[edition] registry key in `HKCU/Software` (known as the “user key”) is created by the desktop app when it starts and copies the default settings from the machine key to the user key. Values in the user key are updated when the desktop app connects to the server.

Note: The registry key location in HKCU should be under Wow6432Node because the desktop app is a 32-bit application.

The installer creates HKLM with the values specified in the installation script (SCCM or BAT file). If you run the MSI manually, it uses the values that the user chooses in the MSI dialogs. When the client starts, it always looks for HKCU first and use those values. If it does not find a key under HKCU, it looks for the key under HKLM and writes a copy from those values into HKCU. It does not matter if the values in HKLM do not match the values in HKCU.

Values in HKLM key are created during installation. Those values are the default values that are written to HKCU when the client starts. Once a user has signed on, all subsequent sign-ons by that user only read the HKCU values. If you have a machine that is fresh, you can change the values in HKLM only. If you have a machine that users have logged on to already, then you need to either delete their HKCU key or update it.

User key

The following are the keys found in the HKCU/Software user key:

- AtHoc[edition]
  - alternateBaseUrl1—See "Failover" in Management system desktop app settings.
  - Audio
  - BASEURL—Copied from `HKLM/Software/Wow6432Node/AtHoc[edition]/BASEURL`. This value is updated when redirected to a different system.
  - Extension
  - Installdate—Time stamp from when the installation happened. The format is: 20170811170307, which is 2017-08-11 17:03:07
  - ProgramsFolder—The user’s Start Menu folder for the AtHoc[edition] desktop app.

- LastBaseUrlIndex
- LdapAttributeValue—This value appears only when the desktop app attempts to save the value. The "LDAP attribute" is selected in **Settings** > **User Authentication** in the BlackBerry AtHoc management system. This value can be created manually in environments that do not use Active Directory. This value is compared with the user's Mapping Id.
- PROVIDER ID—Copied from `HKLM/Software/Wow6432Node/AtHoc[edition]/PROVIDER ID.`
- RegisterInIE—Not used.
- SendLogLink—Start Menu shortcut to send the desktop app log to. Contains the "C: \Program Files (x86)\AtHoc[edition]\AtHoc[edition].exe" log.
- serverType—ASP.
- TOKEN—Created and returned by the server at first SO.
- ToolbarLink—Legacy toolbar value. Not used by the desktop app.
- UID—Created and returned by the server at first SO.
- UninstallLink—Start Menu shortcut to uninstall the desktop app. Contains "C:\Windows \system32\msiexec.exe /x {product_guid}".
- UserPath—Path to the AtHoc[edition] folder in the user's AppData folder.

- ACTIONS—Not used.
- CLIENT—"Client version information." This key is not used by the desktop app.

  Note: The value for Version is always the same in the GU response returned by the server.
- Version—5.6.4.0.
- ENGINE—This key is not used by the desktop app.
- Internet Settings—This key does not appear unless changes are made on the Connection Settings tab of the desktop app's About dialog.
  - AuthPass—(REG_BINARY), hashed password.
  - AuthUser—(REG_SZ), username.
  - AutoDetectAddress—(REG_SZ), location of the automatic configuration script used when "Use automatic configuration script" is checked.
  - IsAuthEnable—(REG_DWORD), 1 = "I'm behind authentication proxy" is checked.
  - IsAuthPassSaved—(REG_DWORD), 1 = "Save authentication password" is checked.
  - IsAutoConfg—(REG_DWORD), 1 = "Use automatic configuration script" is checked.
  - IsAutoDetect—(REG_DWORD), 1 = "Automatically detect settings" is checked.
  - IsProxyEnable—(REG_DWORD),1 = "Use a proxy server" is checked.
  - ProxyServer—(REG_SZ), the proxy server URL and port.
- metaStore
  - data—Stores XML that indicates the user's status.
- PROVIDER
  - Application
  - AtHocAndLCSConnected
  - blockRequestIfLocked—See the "Stop checking for updates when Desktop is locked" section in Management system desktop app settings.
  - clientLog—See the "Email Address To Send Client Logs" section in Management system desktop app settings.
  - Connected—System tray icon to use when the desktop app is connected. Located in `C:\ProgramData \AtHoc[edition]\Ico`
  - Connecting—System tray icon to use when the desktop app is connecting. Located in `C:\ProgramData \AtHoc[edition]\Ico`
  - deskbar—Stores the value that was passed to the MSI for DESKBAR (the value for DESKBAR in `run.bat`).

- Disconnected—System tray icon to use when the desktop app is not connected. Located in `C:\ProgramData\AtHoc[edition]\Ico`
- enableNotifierAutoFocus—Supported by the client but not used. When set to "Y" this entry causes the pop-up to have focus. This entry enables compliance with Section 508 standards.
- enableRClick—Not used.
- ENABLERCLICKCLEARPOPUP—See the "Right-click to dismiss Desktop pop-up" section in Management system desktop app settings.
- FORCEDEXPOSETIME
- FORCEDEXPOSETYPE
- IEColor—Icon for use with unknown feature.
- IEGray—Icon for use with unknown feature.
- LOGO—Company logo to show in pop-up alerts. Located in `C:\ProgramData\AtHoc[edition]\Bmp`.
- NAVINDIRECT
- networkStatusBubbles
- NoUninstall—Y = uninstall is not allowed. N = uninstall is allowed. See the “Show uninstall option in control panel and Start menu” section in Management system desktop app settings.
- PROGRAMNAME
- PROVIDERLOGO
- PROVIDERURL
- PROVIDERNAME
- SendLog—Icon
- silent—Icon
- SUPPORT
- SYSTRAY_TOOLTIP
- toolbar
- TOOLBARNAME
- UnInstall—Icon for use during uninstallation.
- uninstallMessage
- UNINSTALLNAME
- Version

- SKIN—“Change IE toolbar skin.” This key is not used by the desktop app.

  Note: The values in this key are always the same in the GU response by the server.
- STYLESHEET—Service and button styles to use in Toolbar and menu visual configurations. this key is not used by the desktop app.

  Note: The value for Version is always the same in the GU response by the server.

  - Version=1
- SYSTEM

  - CONNECT-INTERVAL—See the "Reconnect Interval" section in Management system desktop app settings.
  - CONNECT-INTERVAL-WINDOW—Created when the client connects to an organization. Used when the client is unable to connect after first SO . This key adds a randomized wait interval to CONNECT-INTERVAL (the “Reconnect interval”) that the client uses before attempting to connect after the connection is lost. “Additional max delay time” is displayed in the client log when this key is in use.

    Note: The CONNECT-INTERVAL-WINDOW is calculated from the database value DSW_RECONNECT_WINDOW in PRV_EXTENDED_PARAMS_TAB. DSW_RECONNECT_WINDOW must be between 2 and 100. The calculated value for CONNECT-INTERVAL-WINDOW will be:

    valueInSeconds = (DSW_RECONNECT_WINDOW x Check Update interval) / 100

Note: The BlackBerry AtHoc server performs session maintenance and clears out stale desktop sessions. A session is considered stale if the desktop app has not performed a successful CU for a time that is equal to 1.5xCU + 30 seconds. For example, a CU of 1 minute means the session is stale if a CU has not occurred in the last 120 seconds. However, the session maintenance job runs every half hour, so the desktop app can have several failed CUs and then a successful one just before the session maintenance job runs and the session is not considered to be stale.

- GB-INTERVAL—Not used.
- KEEPER-INTERVAL—See the "Check Update Interval" section in Management system desktop app settings.
- KEEPER-START—See the "Start-up Delay" section in Management system desktop app settings.
- RECOVERY-INTERVAL—See the "Recovery Interval" section in Management system desktop app settings.
- systray-visibility—See the "Display System tray icon" section in Management system desktop app settings.
- Version
- SYSTRAY-MENU
  - Version
- TREE—This key is not used by the desktop app.

Operation

See Chapter 3 “Common Flows” in the *AtHoc Client Server Interface (CSI) Protocol - Technical Specification* for a description of the desktop app’s operations.

Client server interface

The BlackBerry AtHoc client server interface API (CSI) refers to the specification described in the *AtHoc Client Server Interface (CSI) Protocol - Technical Specification*.

CSI includes Sign On (SO), Check Update (CU), Get Update (GU), and Get Service (GS).

The desktop app uses Microsoft’s WinInet API to communicate with the BlackBerry AtHoc server. The desktop app assembles a query string according to the CSI specification for the particular operation (SO, CU, GU, or GS) and appends it to the Base URL and passes that in the WinInet InternetConnect API call.

Startup

When the desktop app starts for the first time, it performs the following actions:

1. Look for the AtHoc[edition] user key under HKCU.
   a. If the key does not exist, it is created using values from the machine key which was created during installation:

      `HKLM\Software\SysWow6432Node\AtHoc[edition]`.

   b. If the key is present, it reads several values to prepare for communication with the server: alternateBaseUrlIndex, BASEURL or alternateBaseUrl(n), PROVIDER ID, TOKEN, and UID.
2. Create Start menu shortcuts for the generic desktop app edition (AtHoc[edition] Desktop).
3. Attempt to connect to the server and request baseurl.asp passing two parameters on the query string: organization ID and a random string created from a new GUID.
4. If SO is successful, create a new Start menu folder with the name of the organization, delete the contents of the generic client Start menu, and create new shortcuts in the new folder.

   Note: Any shortcuts that are added to the “AtHoc[edition] Desktop” shortcut folder are moved to the organization-named shortcut folder when the desktop app restarts.
5. Create data files. Data files are updated during operation. For example, when an alert is received or when a GU occurs. Data files are replaced each time the desktop app starts. Data files are stored in the user folder:

   `C:\Users\<user>\AppData\Local\AtHoc[edition]`

   Note: Each time the client starts it deletes the files in `C:\Users\[profile name]\AppData\Local \AtHoc[edition]` and downloads new copies.

Windows Start menu

The installer for the desktop app does not add anything to the Start menu. The desktop app creates a Start menu folder when it starts up. The default name is taken from the edition. For example, the AtHocGov client creates an “AtHocGov Desktop” generic Start menu folder. Each time the desktop app starts, it looks for the generic Start menu folder and creates it if it does not exist.

When the desktop app connects to an organization, it creates a custom Start menu folder with the organization name, attempts to move the shortcuts in the generic Start menu folder to the custom Start menu folder, and attempts to delete the generic Start menu folder. Selections in the Desktop App page in Settings affect the presence of some shortcuts. For more information, see Management system desktop app settings.

When the desktop app is stopped and restarted, in addition to the initial steps of creating the generic Start menu folder, the Start menu folder with the organization name is deleted and then re-created. Note that shortcuts created manually in the custom Start menu folder are deleted in this process.

After the desktop app connects, if the same shortcut is added to both of the Start menu folders, it will not be deleted in the above sequence (the Start menu folder with the organization name is not deleted and recreated at start up).

Internet connection

When the desktop app starts for the first time, there is no registry key 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 to wait before attempting to connect again. Once the desktop app connects to an organization, the user key is created along with values that are used to determine the wait interval to use when it is unable to connect.

During subsequent CU intervals when the desktop app is unable to connect, it will wait an interval of time and try to connect again. The wait interval is determined by the following formula:

```
wait interval = CONNECT-INTERVAL + (CONNECT-INTERVAL-WINDOW x (rand()/RAND_MAX+1))
```

where rand() is between 0 and RAND_MAX, and RAND_MAX is guaranteed to be at least 32767. (RAND_MAX is an integer constant.) The Interval is in seconds.

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`. The SO query string has the following format:

```
http[s]://<server_path>/csi/session/action.asp?
99=SO&00=<UserId>&02=<Token>&03=<PID>&...
```

The following are query string parameters:

- 00—User ID.
  - A negative VPS ID (for example, -2050329) indicates that this is a first time sign on.
  - A positive value is for a User ID, and indicates that this is not a first time sign on.
- 02—Token, generated by the server. The first time sign on value is 0.
- 05—Windows username.
- 06—Domain name.

For more information on query string parameters, see Appendix B: Desktop client URL parameters.

To prevent transmission of the machine IP, enable the **Collect Workstation Info** option in the BlackBerry AtHoc management console, at **Settings** > **Desktop App**.

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**.

Unresolved desktop users in organization 1

Desktop users are stored in organization 1 under the following conditions:

- PID=1 in the `run.bat` file was used to install the client. The customer uses the redirector to move users to the correct organization and baseurl based on machine name.
- The PID in the `run.bat` file that was used to install the client is not found in the system.
- A client performs a first time SO on the primary system (the system that the client connects to during first-time start up and has redirection enabled) and is redirected to a secondary system. A user is created in organization 1 on the primary system and redirection is logged in that end-users's properties. This allows an operator to determine which users have connected, and where they have been redirected to.

Check update

Check Update (CU) is a periodic call to Blackberry AtHoc to get a list of sections and dynamic update (DUA) version. The CU query string has the following format:

```
http[s]://<server_path>/csi/session/action.asp?99=CU&00=<UserId>&01=
<SessionId>&02=<obsolete>&03=<AppVersion>&04=2&05=0&...
```

When CU determines that an update is pending, it initiates a Get Update (GU). That results in the client writing a list of section versions to the log.

The following is a sample from a log:

```
CU-|ENGINE,0|SKIN,1|TREE,1|CLIENT,5.6.4.0|STYLESHEET,1|ACTIONS,1| 209999990,0,|
SYSTEM,551307491|PROVIDER,551307491|SYSTRAY-MENU,549731261|
```

In the above sample, the format is "|SECTION-NAME,version|", showing the names and versions of sections that correspond to the registry keys under the desktop app's user key. For example, the version for PROVIDER is 551307491, which you can see in the user's registry: `HKCU\Software\AtHocCorp\PROVIDER\Version`.

If the CU is successful, the client shows the connected icon ()in the system tray. If the CU is not successful the client shows the disconnected icon () in the system tray.

Detect and retrieve a desktop alert

When the DUA version has changed, indicating that a desktop alert has been published to the user, the desktop app logs the following information:

```
…CInternetInterface::DownloadURL  Downloading http[s]://<server_path>/csi/session/
action.asp?99=CU&...
…CInternetInterface::DownloadURL  Http status code: 200
…CBackChannel::CheckDUVersion     New Version
…CBackChannel::GetDuaUpdate       File - 209999990.
```

After the DUA version changes, there is a Get Update, and information that indicates the file that contains the content is logged. For example:

```
…CBackChannel::SetPopup      File: c:\ProgramData\AtHoc[edition]\Htm\AT8746227.htm
```

Get update

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

The following are GU parameters:

- 00—User ID.
- 01—Session ID.
- 02—The item to download. Each GU downloads one item.

Downloaded payloads are stored as XML files in the following location:

`C:\Users\[username]\AppData\Local\AtHoc[edition`

Alerts

A downloaded alert is stored in DUA209999990.XML. The XML is parsed for alert code (HTML and Javascript), and is put in a new file that is stored in:

`C:\ProgramData\AtHoc[edition]\Htm\`.

The naming convention for the alert file is `AT1234567899.htm`. These files are deleted by the client when the alert is ended.

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. Get Service (GS) is also known as "SPS mode (non-direct)", because the service is accessed through `<AtHoc_Server_Home>/sps web app`.

In contrast, Direct-log mode (DL) is where the desktop app sends the URL request using the WinInet API and not through the browser.

Example get service URL

The following is a sample GS URL:

```
https://alerts4d.athoc.com/sps/get.asp?99=GS&00=9999999&01=
1210261388&02=530&03=&04=&05=530&06=&07=&08=&09=ff2&
```

For testing access to Self Service, an end user can paste the GS URL in the address bar of Internet Explorer (IE) 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

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 cause is either an invalid ActiveX Object name in the management system (**Settings** > **Desktop App**), or a browser setting that is blocking use of the ActiveX object.

Confirm the following browser settings:

- Run ActiveX controls and plug-ins (should be Enable).

- Script ActiveX controls marked as safe for scripting (should be Enable).

Redirection to validation error

When accessing Self Service, the desktop app downloads `wwwroot\sps\get.asp`. This page has the following JavaScript code that creates an ActiveX object:

```
utility = new ActiveXObject("AtHoc[edition]GStlbar.GShelper");
```

For example:

```
utility = new ActiveXObject("AtHocGovGStlbar.GShelper");
```

After creating the object, the code tries to use it to retrieve the user ID. If retrieving the user ID fails, a redirection to the validation error page occurs. The following is an excerpt of the code in `get.asp`:

```
try {
         clientUid = utility.GetUID();
         finalURL = finalURL.replace("00=[uid]", "00=" + clientUid);
}
catch(e)
{
         finalURL = "<%=baseURL%>/sps/valderror.asp";
}
```

Failover

Desktop apps starting with 6.2.x.18 have the ability to 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.

Table 7: Failover support in BlackBerry AtHoc server

Server version	Notes
6.1.8.76	Failover URLs appear on the Desktop Software tab.
7.4	Failover URLs appear in **Settings** > **Desktop App**.

Table 8: Failover support in the desktop app

Desktop app version	Notes
6.2.x.263	(2010) More robust failover support.
6.2.x.269	(2014) Fixed issues in failover URL handling.
6.2.x.272	(2016) Fixed issue with invalid user token on failover and failback.

Desktop app version	Notes
6.2.x.278	(2018) 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.

The desktop app stores the failover URL in the registry value “alternateBaseUrl1.”

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. The desktop app then increments the LastBaseUrlIndex registry value. If this value is not present, the desktop app creates the string value and sets it to 1. The desktop app then attempts to connect using the next alternateBaseUrl(n), where n is the value in LastBaseUrlIndex in `hkcu\software\AtHoc[edition]\`.

After the desktop app is connected to the failover server, if that server stops responding, the desktop app resets LastBaseUrlIndex to 0 and attempts to connect using the original Base URL value.

Caveats to consider when configuring Failover URLs

For desktop app versions 6.2.x.268 and lower, the secondary server must have the same number of Failover URLs, otherwise the desktop app clears the registry values for any alternateBaseUrl(n) that does not exist in Failover Servers. However, the desktop app increments the LastBaseUrlIndex during fail back. This causes the desktop app to attempt to use the empty alternateBaseUrl(n) value. Subsequent CUs fail, and LastBaseUrlIndex is incremented. The fix is to delete LastBaseUrlIndex or set it to 0.

For desktop app versions 6.2.x.271 and lower, 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.

Table 9: Redirector support in BlackBerry AtHoc server

Server version	Notes
6.1.8.84 CP9	The following functionality was modified as per customer inputs: • User attributes for tracking redirection were added. • "does not contain" was added to the list of operators. • A text field where a name exemption can be added to exempt particular users from redirection was added. • Use of Mapping API during SO is not functional in 84 CP9, where the Mapping API source code was modified to get redirection rules from the RDR_FIND_RULE stored procedure.
6.1.8.85 R3SP4 CP1	• HotFix IWS-17717_Redirector_Fix(6.1.8.85_R3SP4CP1) contains the code merge from 6.1.8.84 CP9, which came out after 6.1.8.85 R3SP4 CP1. • Use of the Mapping API during SO is broken in 85 R3SP4 CP1, where the Mapping API source code was modified to get redirection rules from the RDR_FIND_RULE stored procedure.
6.1.8.87 CP1	• Use of Mapping API during SO was restored. • User attributes for redirection are not updated correctly in both the From VPS and To VPS when redirection occurs after first time sign on.

The Redirector Agent was overhauled in 6.1.8.84 CP9. The system task and the Redirector Agent are removed if they are present.

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 10: User attributes sent by the desktop app

Client property	Description
Machine IP	IPv4 address of the machine. (Desktop app versions from 6.2.x.270 may not pass the IP address of the machine.)
Machine Name	Computer name.

Client property	Description
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.

To enable redirection for the desktop app, complete the following steps:

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 the (**Settings**) icon.
4. In the System Setup section, click **System Settings**. The System Settings page opens.
5. Click **Edit**.
6. In the Redirection Settings section, select the **Enable Client Redirection** check box.

Add redirection rules

To add redirection rules for the desktop app, complete the following steps:

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 the (**Settings**) icon.
4. In the System Setup section, click **System Settings**. The System Settings page opens.
5. Click **Edit**.
6. In the Redirection Settings section, click **Redirection Rules**. The Redirector Rules screen opens.
7. Click **Add New Rule**. The Add new redirect rule dialog opens.
8. 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**.
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. (Optional) Select the **Skip Url Reachable test** check box, if you are sure that you have entered a valid redirection URL.
15. Click the (check mark) icon. 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
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

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

To add system tray menu items to the desktop app, complete the following steps:

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. In the navigation bar, click the (Settings) icon.
3. In the Devices section, click **Desktop App**. The Desktop App window opens.
4. In the System Tray Menu section, select the **Display System Tray** check box.
5. Click **Manage Menu Items**. The Desktop App Menu Items window opens.
6. Click **Add Menu Item**. The Add Menu Item window opens.
7. 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. (Optional) Add a separator to the Menu Configuration XML.

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

The default functions include the following items:

Option	Code
Check for New Alerts	8009
Dismiss All Popups	8022
Access Self Service	521
Update My Info	530
Update My Device Info	531
About	8005

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 in order for the change to take effect.

Addition or removal of a menu item is picked up by desktop app clients at the next check update. Changes to a menu item take effect immediately (without CU) because the GS request is processed server-side, and the resulting service URL is sent back to the desktop app.

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. Five predefined values allow you to use user-specific data. The Static value allows you to hard-code a name-value pair.

Authentication

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

Mapping API

The following table lists Mapping API support in the BlackBerry AtHoc server:

Table 11: Mapping API support in the BlackBerry AtHoc server

Server version	Notes
6.1.8.84 CP8	Processed during SO.
6.1.8.84 CP9	Broken (not processed during SO.)
6.1.8.85 R3SP1	In DesktopSignOn.
6.1.8.85 R3SP4 CP1	Restored (processed during SO.)

Mapping API was provided as a way to support unforeseen authentication requirements. Mapping API is a reference to a COM function that is called by name during sign on (in legacy VB COM code, “CallByName” is used). CallByName takes an object and procedure name, so the “API” is a string that contains the class name and procedure name in this format:

```
className::procedureName.
```

The above formatted value is stored in DSW_SIGNON_MAPPING_API column of the PRV_EXTENDED_PARAMS_TAB table. CallByName creates an instance of the object with name className, and calls the function procedureName. All of the desktop app parameters are sent to the function and may be returned with updated values.

Legacy Visual Basic code uses the Mapping API as follows:

```
comClassName = Mid(className, 1, InStr(className, "::") - 1)
comInterface = Mid(className, InStr(className, "::") + 2)
Set comClass = CreateObject(comClassName)
output = CallByName(comClass, comInterface, VbMethod, nProviderId, sDomainName, sDomainUserName, sClientCerts)
```

The one known use of Mapping API uses a WSC component written in vbscript. The custom WSC component interface is:

```
<component>
      <?component error="true" debug="false" ?>
```

```
      <registration
              progid="AtHocRedirector.wsc"
…
      <public>
              <method name="ClientMachineLookup"/>
      </public>
     <script language="VBScript">
<![CDATA[
       Public Function ClientMachineLookup(lUserId, lProviderId, sToken, sClientIP,
sMachineName, sDomainUserName, sDomainName, sClientCerts)
…
```

Finally the function makes a database call to look up redirector information that applies to the user. The function parameters are populated from results of the database query:

```
SELECT PROVIDER_ID, OPERATOR, CRITERION, REDIRECT_TO_VPS FROM RDR_RULE_TAB WITH
(NOLOCK) WHERE ATTRIBUTE_NAME = 'Machine Name' AND OPERATOR = 'starts with' AND
charIndex(criterion, ?) = 1
```

Add a parameter to replace “?” with clientMachineName.

Use LDAP attribute

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

Desktop app version 6.2.x.271 and BlackBerry AtHoc server version 6.1.8.87 CP1 support the use of LDAP attributes for authentication.

Organization configuration

LDAP authentication is based on the end user's Username. When using the mail attribute, the end user's Username attribute must contain the end user's email address from Active Directory.

To configure your organization to use the LDAP attribute for authentication, complete the following steps:

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. In the navigation bar, click the (Settings) icon.
3. In the Users section, click **User Authentication**. The User Authentication screen opens.
4. 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. Next to Create New User if an Account is not Found, select the **Enable** check box.
8. Click **Save**.

Migrate existing users to LDAP attributes

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 the previous task.
- Save the changes.

- Update the end Username for each user. For example, when using the LDAP mail attribute, set the Username 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 client to query Active Directory, users must have at least read-only permission to their Active Directory. The client sends the value of the attribute to the server. The server performs a user search where the Username in each user record is compared to the attribute value. If a match is found, the client 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 Username 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 Username has not been set correctly.

If the desktop app cannot query Active Directory, it waits until it can. The desktop app caches the designated attribute in the registry, in the string value LdapAttributeValue under HKC\Software\AtHoc[edition], 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.

When the desktop app restarts, it downloads baseurl.asp which contains the initial instructions for sign on. When LDAP authentication is enabled, the instructions include a userLookupMode node with type="LDAP" and the name of the attribute to use. For example:

<userLookupMode type="LDAP">mail</ UserLookupMode>

The desktop app then creates a new "LdapAttributeValue" string value in the registry under HKCU\Software \AtHoc[Edition].

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. The LAST_KEEP_ALIVE time stamp in the session record is updated at each CU and is used to determine inactivity. When the desktop app stops polling the server, the LAST_KEEP_ALIVE time stamp is not updated and the Desktop Sessions Maintenance session maintenance job determines that the session is stale and deletes the record.

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. This job executes the CLEANUP_USER_SESSIONS stored procedure.

For more information, see Appendix C: Database server.

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.

   The formula for determining whether or not a session is stale is:

   LKA + 1.5xCU + 30 < Now

   where LKA is the value in the LAST_KEEP_ALIVE column in the session table.

   Values are in seconds.
2. When the desktop app logon time is less than the current time minus SSN_FORCE_CLEANUP_INTERVAL in the ngaddata.prv_provider_tab. 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.

The above formulas are used in the CLEANUP_USER_SESSIONS stored procedure.

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.

section describes how the desktop session becomes stale due to the user shutting down or locking the machine, but what happens when the application server stops accepting requests? For example, when the AtHoc Desktop 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. The formula states that 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.

Change the provider or base URL

Sometimes a desktop app is connected to the wrong server (BASEURL registry value) or to the wrong organization (PROVIDER_ID registry value). The PROVIDER_ID and BASEURL are stored and retrieved by the desktop app in the user key `HKCU/Software/AtHoc[edition]`. Installed values are stored in the machine key `HKLM/Software/Wow6432Node/AtHoc[edition]`.

To make the desktop app connect with the correct BASEURL or PROVIDER_ID, you can update these values in the user key and restart the desktop app. However, if the desktop app has already connected to the wrong server or organization, it also has values stored for the User ID (UID registry value) and TOKEN, and attempts to use those when connecting.

If the desktop app refuses to connect after changing BASEURL or PROVIDER_ID, try making the same change in the machine key and then delete the user key and restart the desktop app. The app then reads the machine key and connects to the correct server and organization.

Changes made to the user key are not picked up by other users who log on to the machine. If there are other users who may use the machine, it is better to make changes to the machine key, delete the user key, and then restart the desktop app. Any users who have already been on the machine also need to delete their user key.

Troubleshoot desktop app issues

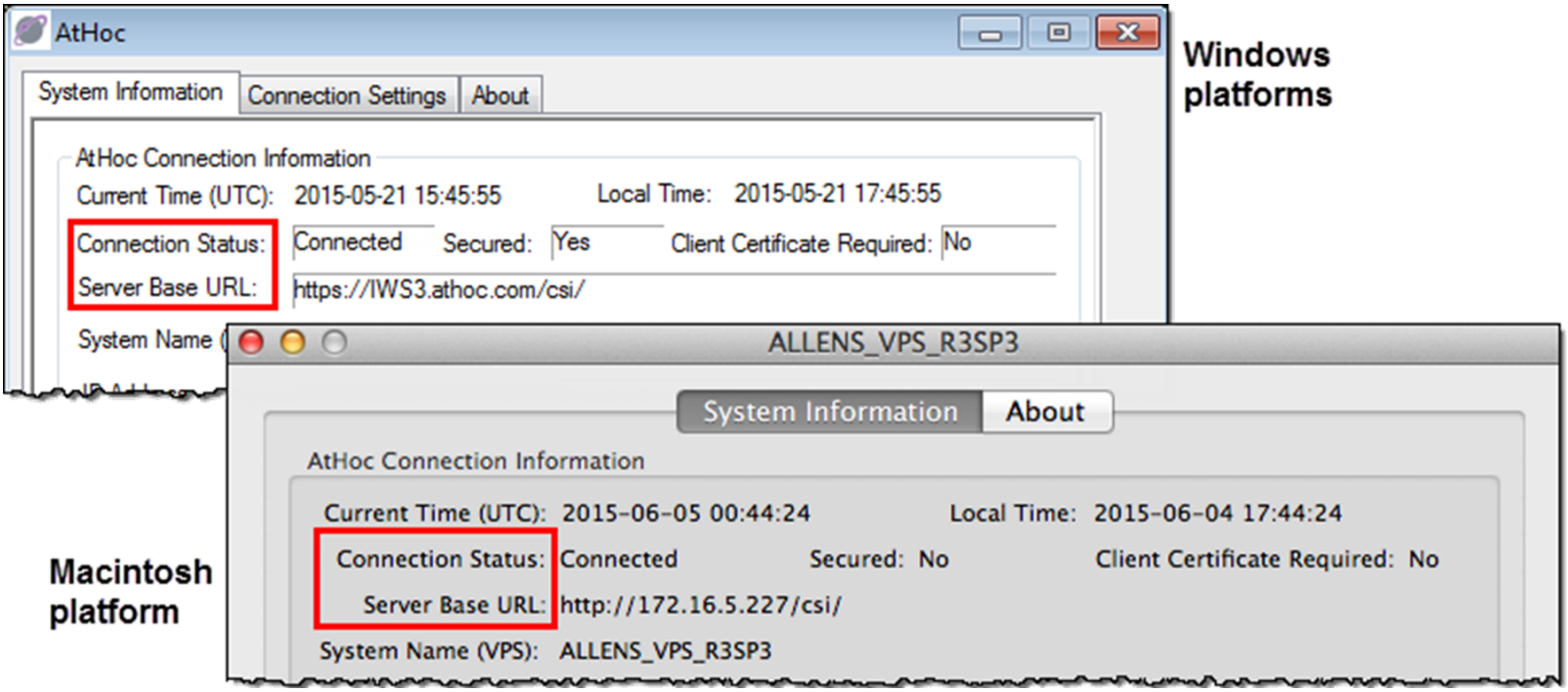
This section describes issues you may encounter after installing the BlackBerry AtHoc desktop app on users' desktops. In most cases, the solutions provided in this chapter resolve these problems. If they do not, contact BlackBerry AtHoc Technical Support at athocsupport@blackberry.com.

Access Desktop App details

Before contacting BlackBerry AtHoc 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.

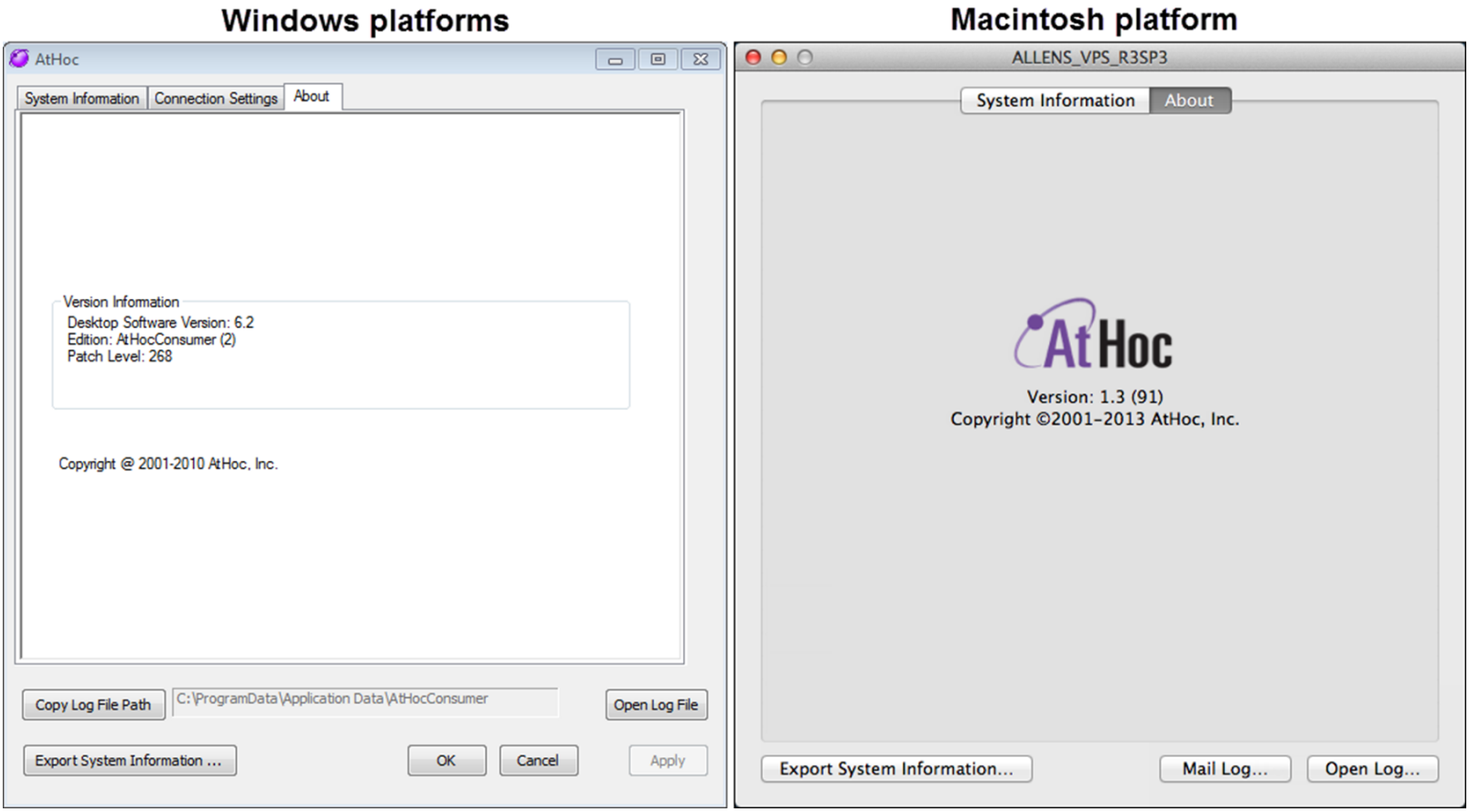
Right-click on the  (Globe) icon and select **About** from the menu that appears to access the application details screens.

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 to which you are connected.



The **Connection Settings** tab, which appears only on Windows platforms, provides options for automatic configuration and use of a proxy server. Because these settings are not used for most installations, it is unlikely you will need to review this information.

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.



Installation issues

Installation Fails with a 1603 error (MSI log)

This occurs when the UninstallOldVersions custom action is allowed to run on a system that has had a previous client installed, and the action finds remnants of that old client. This is fixed in desktop app version 6.2.x.269 and later.

There are two levels of functionality, one is always disabled, the other you need to edit the `options.xml` schema and set DeepCleaning to NO. You should always set DeepCleaning to NO to completely remove the UninstallOldVersions custom action from the MSI.

Read the desktop app log

To view the desktop app log, 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
Message	ProviderId: 2050329

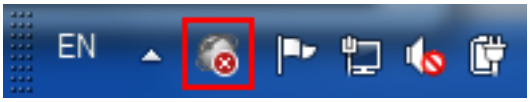
Note: Column headers do not appear in the desktop app log file.

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:

```
...Downloading http://(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:

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

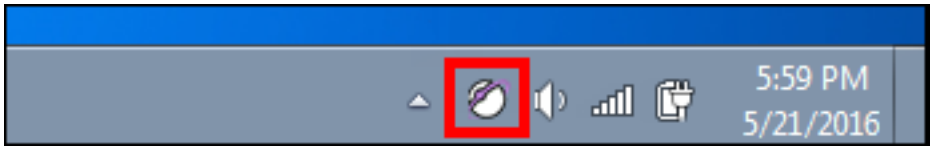
Gray globe - user account is disabled

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  (Globe) icon appears on your screen, indicating that you are connected to the BlackBerry AtHoc server and are ready to receive alerts.

Windows Platforms



Macintosh Platform

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".

Windows Platforms

Macintosh Platform

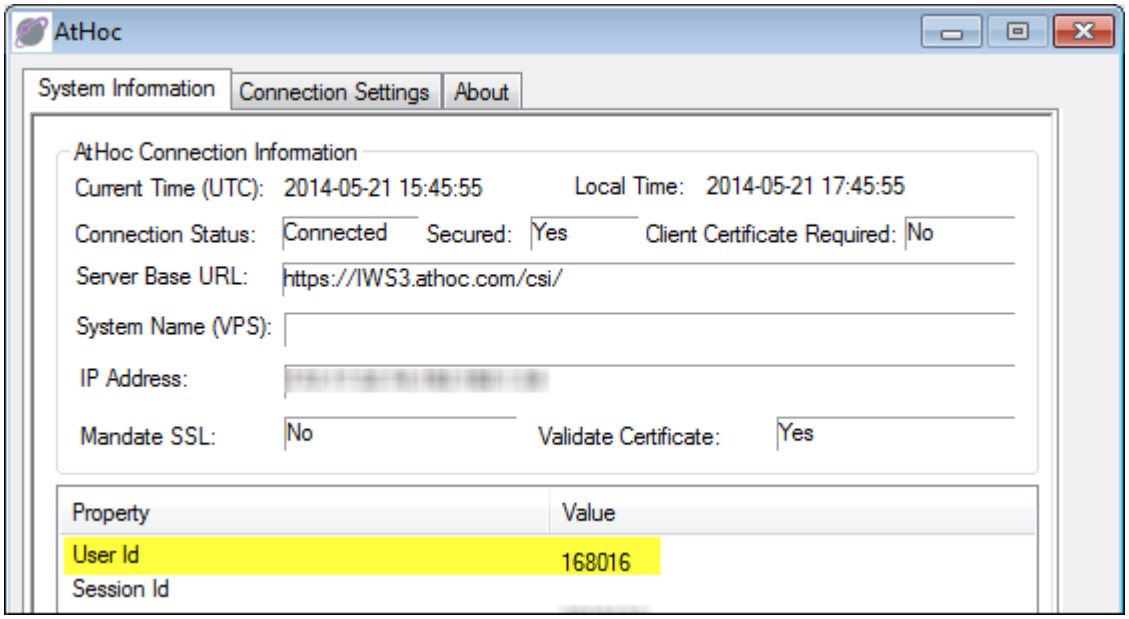
When the Desktop App is disconnected, the app cannot receive alerts.

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 right-clicking the  (Globe) icon 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 outlined in Desktop app does not connect.

Desktop app does not connect

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

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

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

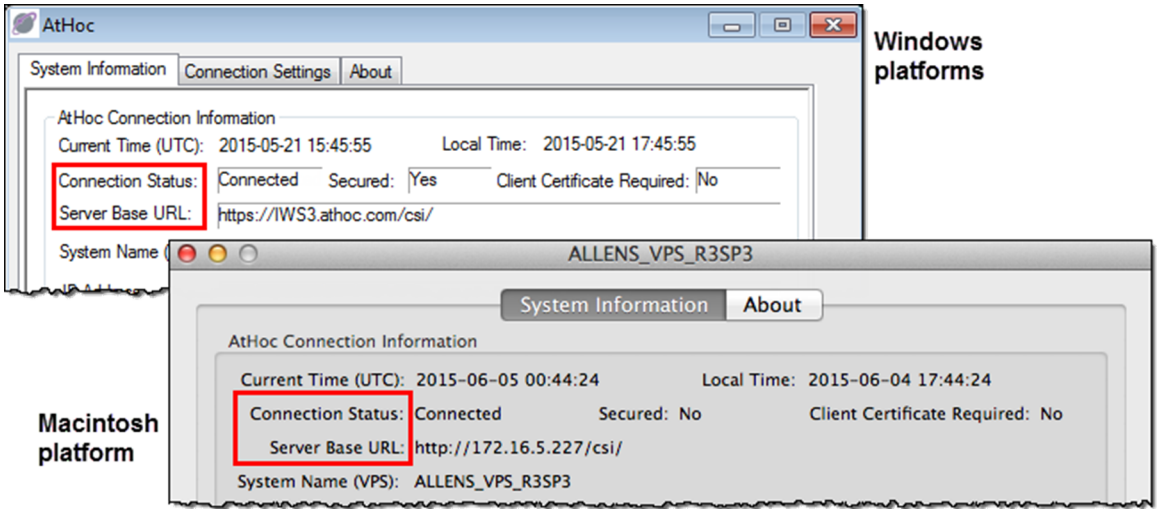
The app might not connect to the BlackBerry AtHoc server due to a number of reasons related to the network configuration. To resolve the problem, do the following:

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

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

1. Right-click the (Globe) icon.
2. In the menu that appears, click **About**.
3. On the About screen that appears, 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.
- 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.
- An intermediate certificate issued by the organization prevents the desktop client from connecting. Remove the intermediate certificate to resolved 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 underpowered 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 underpowered and CPU use is not high, check for a bad disk on the database server.
- All users see gray globe() icons.

  Make sure the “ActiveX Object name” is correct for the organization in **Settings** > **Desktop App**.

  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

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

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

Automation server can't create object error

This error may be followed by a “Server Error 404 – File or directory not found” error and is caused by disabling “Run ActiveX controls and plug-ins” in Internet Settings (for the zone that applies).

The reason this occurs is because the JavaScript returned from the GS call tries to access the desktop app:

```
utility = new ActiveXObject("AtHocCorpGStlbar.GShelper");
```

Validation error

A validation error can be caused by a wrong ActiveX Object name in the management system (in **Settings** > **Desktop App**).

A validation error can be caused by the user’s browser settings blocking ActiveX. See Validation error for details.

Appendix A: Build settings

The following sections describe the `Options.xml` and `DSWMsiBuildInfo.xml` schema, and the `Install.ini` file.

Options.xml schema

MSI behavior is controlled by the values in the `options.xml` schema.

The following are guidelines for creating or updating the `options.xml`schema:

1. BaseUrlVpsList element—This element is always updated for a new edition or repackage.
   a. One or more Element nodes must be present. This information is used when running the MSI manually, not when running from a script.
   b. Each element adds another record to the list of providers on the Select Your System dialog.
2. UpgradeCodes element—This element provides a way to upgrade an existing installation of the desktop app. Do not add this element unless the installation should allow end users to uninstall their existing client before installing the new client. The installer prompts the user and shows their existing clients in a list, and the user must select the client to uninstall.
3. Editions element—Do not add this element unless you must set DeepCleaning to Yes, and you need the same client edition to be searched and removed during install. This should never be the case, there are other ways to uninstall the client and DeepCleaning causes the MSI to return a failure code.
4. ProductName, SystemName, ServerProductName nodes— Do not change these elements.
5. EditionName—This element is always updated for a new edition but never for a repackage. This element contains the name of the edition.
6. ConnectionInstructions—Do not include this element unless requested otherwise.
7. ManualSelection—Enable this element only when requested. This element allows the end user to manually enter the base URL and provider ID.
8. DeepCleaning—You can enable the DeepCleaning element. However this element was disabled in desktop app release 6.2.269 and later, so DeepCleaning does not occur.
9. UninstallOption—This element should default to “no” for government and military customers, but should be set to “yes” for other customers unless requested otherwise.
10. ScheduleReboot—Do not include this element unless requested otherwise.
11. BaseUrlVpsListHeaderText—Do not include this element unless requested otherwise.
12. AcceptableEditions—This list should not include any editions that the customer does not have. Since it is used by DeepCleaning and that has been disabled, the list is irrelevant most of the time.

Sample schema

```
<?xml version="1.0" encoding="utf-8"?>
<Options>
  <BaseUrlVpsList>
     <Element baseUrl="https://alerts4d.athoc.com/config/baseurl.asp"
providerId="1" label="AtHoc Support" />
   </BaseUrlVpsList>
  <UpgradeCodes>
       <UpgradeGUID>272DCAF9-7916-4388-B143-D605407CA7AA</UpgradeGUID>
```

```
  </UpgradeCodes>
    <Editions>
        <EditionName>AtHocGov</EditionName>
    </Editions>
    <ProductName>AtHoc Desktop Notifier</ProductName>
    <SystemName>Network-Centric Mass Notification</SystemName>
    <EditionName>AtHocGov</EditionName>
    <ServerProductName>AtHoc IWSAlerts</ServerProductName>
    <ConnectionInstructions>Please select your system from the list below:</
ConnectionInstructions>
    <ManualSelection>yes</ManualSelection>
    <DeepCleaning>no</DeepCleaning>
    <UninstallOption>no</UninstallOption>
    <BaseUrlVpsListHeaderText>Select Your System </BaseUrlVpsListHeaderText>
    <AcceptableEditions>
      <EditionName>AtHocGov</EditionName>
    </AcceptableEditions>
   </Options>
```

Options.xml schema elements

The following sections describe the elements found in the `Options.xml` schema file.

BaseUrlVpsList

This element creates the list of organizations that appear in the System selection window of the MSI.

Example

```
 <Element baseUrl="https://alerts4d.athoc.com/config/baseurl.asp"
providerId="1111111" label="Organization Name" />
```

Attributes

baseUrl—The full Base URL of the server where the Provider is: “http[s]://[server_name]/config/baseurl.asp.”

providerId—The number of the organization.

label—The value that appears in the MSI window.

UpgradeCodes

Optional. The UpgradeCodes element is used when upgrading an existing installation of the desktop app.

UpgradeGUID

The UpgradeGUID (or UpgradeCode) of the installed client to upgrade.

Editions

Note the difference between this node and EditionName (described below under SystemName.)

Deprecated. See the EditionName element.

EditionName

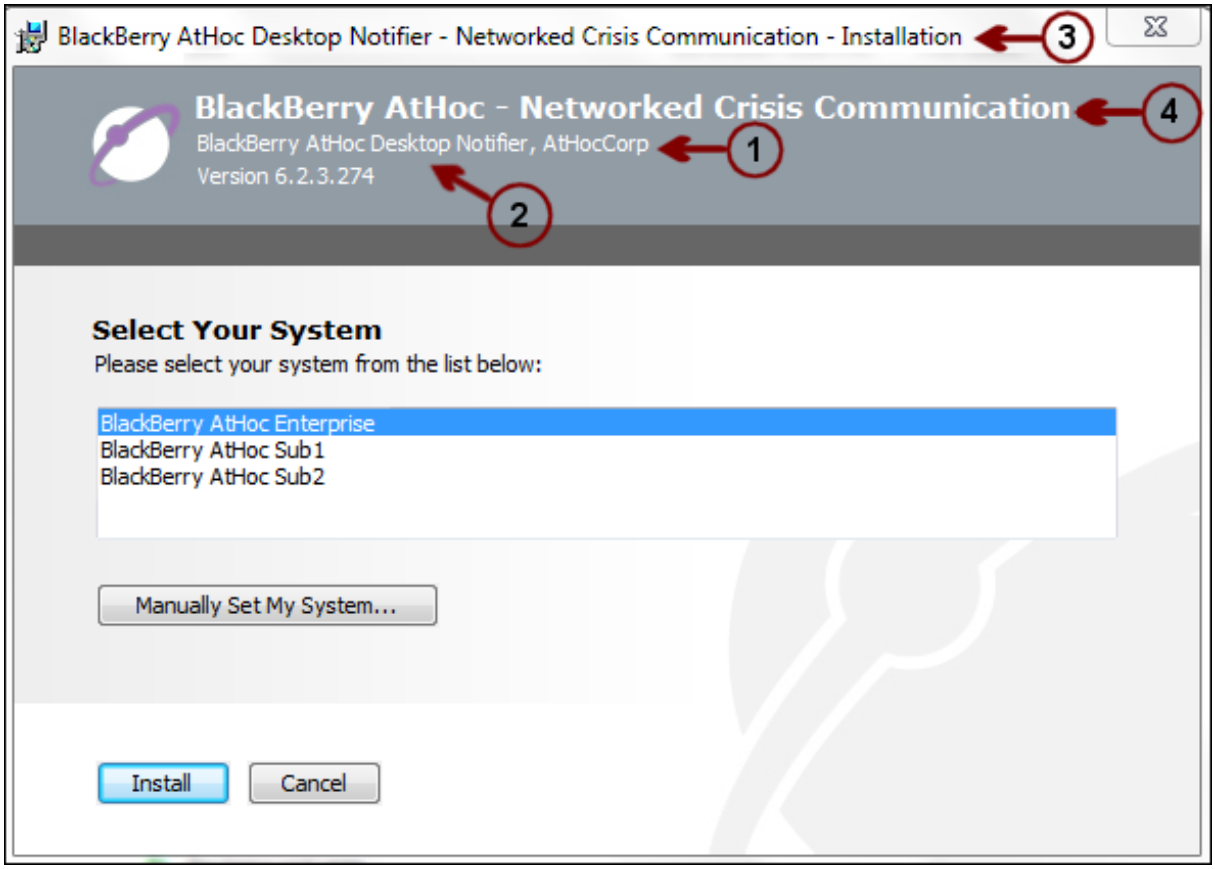
This element is a child of the Editions element. Each EditionName element will be searched for and uninstalled if present.

ProductName

This element is displayed in the MSI window. This element is number 2 in the following image.

SystemName

This element is displayed in the MSI window. This element is numbers 3 and 4 in the following image.



EditionName

The application name of the desktop app. For example, AtHocGov. This element is item 1 in the image above.

ServerProductName

This element is displayed in the MSI window. This element is always displayed as “AtHoc IWSAlerts."

ManualSelection

This element provides the user interface that allows the user to input the Base URL and Provider ID. Valid values are " yes" or "no." These values are case insensitive. The default is "no."

DeepCleaning

This element determines whether or not deep cleaning of existing client installations is performed.

Valid values are "no" and "NO." These values are case sensitive. Any value other than “NO” or “no” will enable Deep Cleaning.

There are two custom actions involved in Deep Cleaning, both perform identical operations to search for remnants of existing clients:

- DetectOldVersions—Runs before UninstallOldVersions, and returns 3 (abort) if remnants of previous installations are found.
- UninstallOldVersions—Runs after DetectOldVersions. This element attempts to uninstall and clean up all remnants of existing clients listed under AcceptableEditions.

Note: DetectOldVersions causes the MSI to show a 1603 result code and log an installation failure even though the client functions normally. For this reason, the DeepCleaning element has been disabled in the installer.

UninstallOption

Optional. This element provides a way to specify whether or not users can uninstall the client from the standard Windows UI. Valid values are "yes" and "no." These values are case insensitive. The default is "yes."

Note: This value is overridden by the UNINSTALLOPTION value in the `run.bat`file.

ScheduleReboot

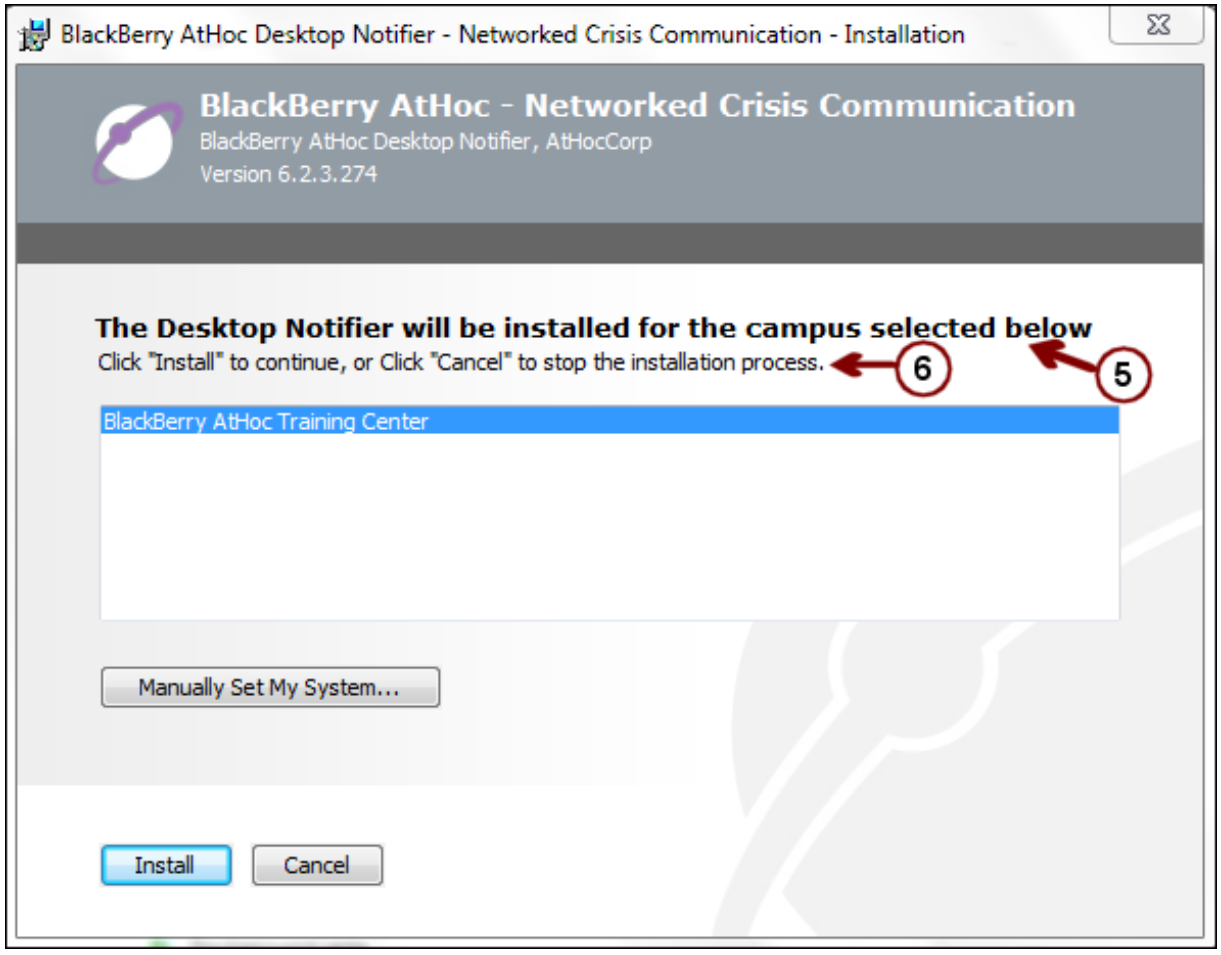
Optional. This element provides a mechanism to cause the machine to reboot after installing the client. Valid values are "yes" and "no." These values are case insensitive. The default value is "no."

BaseUrlVpsListHeaderText

Optional. Default: none. The text to display above the list of organizations instead of the default “Select Your System.” This element is item 5 in the MSI image below.

ConnectionInstructions

This element provides a way to modify the text. This element is item 6 in the image below.



AcceptableEditions

This element provides a list of AtHoc Desktop Client names that the code will look for and attempt to uninstall if Deep Cleaning is enabled. The code performs Deep Cleaning on each edition in this list.

If this node is empty, then a default list of edition names in `CallUninstaller.cpp` is used to perform the uninstallalation and deep cleaning operations (acceptableEditionNameSet).

Note: PackageDSWtoMsi fails if this node is not present.

EditionName

(Subnode of AcceptableEditions.) This element specifies the names of different editions of the BlackBerry AtHoc desktop app. There are no spaces in the names.

DSWMsiBuildInfo.xml schema

This file is used by the desktop app build environment. The ProductGUID, PackageGUID, and UpgradeGUID values are MSI Product Id, Package Id, and UpgradeCode values and must adhere to Windows Installer guidelines.

Sample schema

The following is a sample `DSWMsiBuildInfo.xml` schema file:

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<AtHocDSWMsiBuildInfo>
<Version>6.2.4.275</Version>
<ProductName>AtHocGov</ProductName>
<ProductGUID>E465530B-9773-4806-8A22-FC667DD4C314</ProductGUID>
<PackageGUID>E67ACBBE-A775-4B80-B12C-CAC7AA1C12A9</PackageGUID>
<UpgradeGUID>272DCAF9-7916-4388-B143-D605407CA7AA</UpgradeGUID>
</AtHocDSWMsiBuildInfo>
```

DSWMsiBuildInfo.xml schema elements

The following sections describe the elements found in the `DSWMsiBuildInfo.xml` schema file.

AtHocDSWMsiBuildInfo

This element is the parent node.

Version

This element is the client version. The version convention is: 6.2.x.y

Where x is: 0, 2, 3, 4, and so on.

0 = “AtHoc Internal client”

2 = “Consumer client”

3 = “Corp client” for commercial customers.

4 = “Gov client” for military and government customers.

ProductName

Provided in the Professional Services request.

ProductGUID

This must be different for every edition but can be reused when repackaging.

PackageGUID

This must be different for every edition but can be reused when repackaging.

UpgradeGUID

The MSI UpgradeCode. Microsoft recommends that authors of installation packages use a new UpgradeCode for the first version of a product. Subsequent builds (a newer version of the product, or the same version of the product in a different language) should use the same UpgradeCode as the first version of the product.

Install.ini

The `Install.ini` file contains the COM GUIDs for the client. They must be different for every edition, but can be reused when repackaging.

Sample

The following is a sample `Install.ini` file:

```
#define CLSID_LIBRARY F51ED1F1-E890-48B6-8C41-1A7740418F08
#define CLSID_HELPER 0B4890E7-1F62-47FB-B0DF-0923547FE151
```

```
#define CLSID_HELPER_STR "{0B4890E7-1F62-47FB-B0DF-0923547FE151}"
#define CLSID_BHO 7BD7BEA4-3526-4189-B3E2-BA75CA7F7EBF
#define CLSID_BHO_STR "{7BD7BEA4-3526-4189-B3E2-BA75CA7F7EBF}"
#define CLSID_TOOLBAR 5423FA90-121E-4D4F-B5E3-E054046C0A3D
#define CLSID_TOOLBAR_STR "{5423FA90-121E-4D4F-B5E3-E054046C0A3D}"
#define CLSID_OPENER E5B88953-FC2D-4A83-83AF-6EAC0A6E3DC5
#define CLSID_OPENER_STR "{E5B88953-FC2D-4A83-83AF-6EAC0A6E3DC5}"
#define CLSID_LEGACY 619831F1-54AC-45D4-A8B2-84C856218013
#define CLSID_LEGACY_STR "{619831F1-54AC-45D4-A8B2-84C856218013}"
#define GUID_IEBUTTON 39BDC338-853D-4B62-8BD6-1C0C647DEB64
#define GUID_IEBUTTON_STR "{39BDC338-853D-4B62-8BD6-1C0C647DEB64}"
#define AT_OWNER L "AtHocGov"
 #define AT_OWNER_A "AtHocGov"
 #define AT_OWNER_ACK            L "AtHocGov"
 #define AT_OWNER_ACK_A          "AtHocGov"
```

Appendix B: Desktop client URL parameters

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

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

Table 12: Desktop client URL parameters

Parameter	Sign on	Check update	Get update	Get service	Direct log
99	SO	CU	GU	GS	DL
00	Userid	Userid	Userid	Userid	Userid
01	—	Session id	Session id	Session id	Session id
02	Token	Toolbar status: (Obsolete)	Section	Service id	DUA id
03	Pid	Client version	—	Search box topic	DUA version
04	Sign on attempt number	Explorer windows count (Obsolete)	—	URL/file (current location, before navigation)	DUA state
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	—	—	Operating system (not supported	—
08	Client metastore (was platform)	Registered platforms (for example IE, Deskbar)	—	FF1 (from service definition)	—
09	Client IP	Client IPs	—	FF1 (from service definition)	—

Parameter	Sign on	Check update	Get update	Get service	Direct log
10	—	—	—	FFN (from service definition)	—
11	—	—	—	Title of current HTML page (if any)	—
12	—	—	—	Target URL / file (for navigation)	—
15	Logon user name	—	—	—	—
98	Client certificate	—	—	—	—
SendMsg	—	Messages specified by front-channel methods SychronizeWithDelay () and SynchronizeLater()	—	—	—

Appendix C: Database server

6.1.8.88 and lower

- Session table: [ngkadata].[dbo].[SSN_SESSION_TAB]
- CLEANUP_USER_SESSIONS stored procedure in ngkadata

6.1.8.89

- (moved and renamed) Session table: [ngaddata].[dbo].[SSN_SESSION_DiskBased_TAB]
- CSI Configuration Cache table: [ngkadata].[dbo].[CSI_CONFIG_CACHE_TAB]
- CLEANUP_USER_SESSIONS stored procedure in ngaddata

7.0.0.2

- (moved) Session table: [ngkadata].[dbo].SSN_SESSION_DiskBased_TAB
- CSI Configuration Cache table: [ngkadata].[dbo].[CSI_CONFIG_CACHE_TAB]
- CLEANUP_USER_SESSIONS stored procedure in ngaddata

Appendix D: Application server

- wwwroot\config
- wwwroot\csi
- wwwroot\sps

6.1.8.85 R3SP4 CP1 and lower

- GU calls use csiXML.WSC.

6.1.8.87 CP1 to 6.1.8.90

- GU calls use Usr.CsiUser.

7.0.0.2

- baseurl.asp in wwwroot\config was removed. Calls are routed to AtHoc.Config.MvcApplication.
- action.asp in wwwroot\csi was removed. Calls are routed to AtHoc.CSI.MvcApplication.

BlackBerry AtHoc customer 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 Portal:

https://support.athoc.com/customer-support-portal.html

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

Legal notices

Trademarks

Patents

BlackBerry Solution License Agreement

Contact Information

BlackBerry AtHoc

311 Fairchild Drive

Mountain View, CA 94043

Tel: 1-650-685-3000

Email: athocsupport@blackberry.com

Web: http://www.athoc.com