BlackBerry AtHoc

BlackBerry AtHoc Networked Crisis Communication

Installation and Configuration Guide

Version 7.3, October 2017

Trademarks

Patents

BlackBerry Solution License Agreement

Contact Information

BlackBerry AtHoc

2988 Campus Drive, Suite 100

San Mateo, CA 94403

Tel: 1-650-685-3000

Email: support@athoc.com

Web: http://www.athoc.com

Contents

Changes to this document

Release	Section	Update
Release 7.3	Support for products, processes, procedures, and protocols	Added the OEM Cloud Delivery Service (East) and the OEM Cloud Delivery Service (West) to the list of available delivery gateways.
	Notification Delivery Service support	New topic.
	Virtualized Environments	Topic removed.
	Database server	Topic moved to the *BlackBerry AtHoc Capacity Planning Guidelines*. Updated supported Windows Server versions,and SQL server versions.
	Clustered database configuration	Configuration task moved to Database server installation section.
	Installation requirements	• Updated supported Windows Server versions. • Removed note about issue with HTTP activation when upgrading .NET on a 2008 Server. • Removed .Net Framework v. 3.5.1 and ImageMagick from requirements table. • Updated the steps to set the server locale to US English.
	Discontinued support for Windows 2008 and SQL 2008	New topic added to Installation and Upgrade chapters.
	Obtain a certificate from a Certificate Authority (CA)	Changed "2008 Server" to "IIS 7 and newer."
	Network and Platform configuration requirements	Topic moved to *BlackBerry AtHoc Capacity Planning Guidelines*
	Supported upgrade paths	Updated upgrade path releases.
	Set the SSL client certificate	Updated the list of Application and virtual directories.
	Apply FIPS patch for Windows 2008 R2	Removed topic.
	Enable delivery gateways	Removed topic.
	Configure TempDb	Removed topic.
	Import the geographic data with BCP (post upgrade)	Removed topic.
	Update alert templates with locations	New topic added.
	Uninstall ImageMagick	New topic added.
	IIS post-installation checklist	Updated application pool configuration tables.

Release	Section	Update
Release 7.0.0.2	Set Anti-Virus File Exclusions	Added the IIS Temporary Compressed Files folder to the list of items that should be excluded from anti-virus real-time scanning.
	Application Server > Installation Requirements	Added Dynamic Content Compression to the list of components that must be pre-installed.
	Contact BlackBerry AtHoc Technical Support	Updated the Contact number and the website links of BlackBerry AtHoc Technical Support.
	Configure New Access Card Formats for Operator Auto-Login	Removed "Make Database Changes" from the high-level steps to configure operator authentication using CAC or PIV cards.
	Advanced Server Configuration	Removed a key from the <Server=Server Name> parameter.
	Virtualized Environments	Updated the guidelines for provisioning virtual machines (VMs).

Release	Section	Update
Release 7.0.0.1	BlackBerry AtHoc Icons and Rebranding	Changed the BlackBerry AtHoc desktop icon for the desktop app. Transition from AtHoc to BlackBerry AtHoc naming and logos.
	Application Servers and Common System Resources	Removed reference of shared files. Replaced "AtHoc Processor/ Services" with "IWS Services" and "AtHoc service account" with "IWS Services application pool accounts". Modified the steps in "Login Requirement" topic.
	Support for Products, Processes, Procedures, and Protocols	Corrected "Delivery Medium" to "Delivery Gateway". Removed all the instances of SMTP.
	AtHoc Server Requirements	Removed the instance of "SQL Server Express". Updated the SQL versions from "SQL 2013 to SP3" and "2014 to SP2" and Windows Server to "Windows 2012 R2 (64 bit)". Added a new topic head "Configure IWS Application Server for Windows Authentication (optional)"
	Install BlackBerry AtHoc	Correction: Replaced the welcome screen with the new screen. Replaced the Test connection screen shot with the new "appdaemon" screenshot, screenshot of step 4 and 5 in "Database Server Installation" and screenshot of step 4 in "Application Server Installation". Rewrote the step to select database server. Removed the step- "Locate the license ZIP file". Modified the steps in "Database Server Installation" and "Application Server Installation".
	Upgrade Preparation	Correction: Updated the "Support Upgrade Paths" table and the steps in "Application Server Upgrade and Database Server Upgrade". Replaced the wizard welcome screen with the new screen to match the release number in the "Application Server Upgrade" and "Database Server Upgrade" section. Removed: The "Release Specific preparation steps for Database server and Application server" and "Ensure Section Titles are Unique for all Custom Tabs in Self Service", "Backup Config Files section", and "Clean up Mobile Device Extensions"
	Install a MIR3 Certificate	Updated the steps for installing the certificate. Removed all instances of AtHocProcessor.
	Update AtHoc Management System Security Policy	Updated the steps and the screen shots.
	Generate a Machine Key for Each Application Server	Removed the "Configuration File Settings" section. Changed the topic title to "Enable FIPS on Each Application Server"
	Set Up the IWS Services Account	Updated the application pool names list and deleted step 3. Changed the topic title to "Archive and MAS Export Service Account Requirements".
	Multiple	Changed prerequisite ".Net Framework v.4.5.1" to ".Net Framework v.4.6.1".
	Enable Delivery Gateways	Updated the steps describing how to enable gateway. Removed "Clean Up the OPM Gateway" and "Email Configuration" sections.

Release	Section	Update
	Configure Role-Based Permissions for the AtHoc Mobile App	Removed "When Using the AtHoc Mobile App. Version 2.3 and Earlier" section.
Release 6.1.8.90 Patch	Migrate the CAP Listener Agent	Updated section to "Migrate the CAP Feed Poller".
	Migrate the IEM Agent	Updated section to "Migrate the CAP Event Processor".
Release 6.1.8.90	Throttling Self Service	New topic.
	Migrate the CAP Listener Agent	New topic.
	Migrate the IEM Agent	New topic.
Release 6.1.8.89	Configure AtHoc Database Operations to Use Windows Authentication	Fixed incorrect code in Step 3 by removing commas between arguments.
	AtHoc Database Requirements: Database Server	Updated the SQL versions from 2008 and 2012 to 2012 and 2014 SP2.
	AtHoc Application Server: Installation Requirements	Added Important note about how to avoid a potential issue with HTTP Activation when upgrading .Net on a 2008 Server.
	AtHoc Application Server: Installation Requirements	Added prerequisite for Application Server: HTTP Activation feature, which is found under .NET Framework 3.5.1 Features.
	AtHoc Application Server: Installation Requirements	Changed prerequisite ".Net Framework v.4.5.1" to ".Net Framework v.4.6".
	AtHoc Application Server: Installation Requirements	Added prerequisite for ImageMagick-7.0.2-6-Q16-x64-dll.exe 3 and ImageMagick-7.0.2-6-Q16-x86-dll.exe.
	Overall document	Added new cover page and new legal text; fixed numbering and formatting problems throughout document.

Release	Section	Update
Release 6.1.8.88	Upgrade Preparation>Application Server Preparation	Added instructions for backing up the XML files for any duplicated devices.
	Post Installation/Upgrade Configuration	Added instructions for restoring the XML files for any duplicated devices.
	Post Installation/Upgrade Configuration: IIS Post Installation Checklist	Added 2 new nodes for specifying a custom email template.
	Post Installation/Upgrade Configuration: Update the White List	New topic.
	Post Installation/Upgrade Configuration: Set the SSL Client Certificate	Added folders for various releases.
Release 6.1.8.87	AtHoc Server Requirements: Application Server Installation Requirements	Added BCP utility requirement for importing geolocation data pack. Removed the Microsoft SQL Server System CLR (x86) 2008 type.
	AtHoc Server Requirements: Application Server Installation Requirements	Added BCP utility requirement for importing geo-location data pack. Removed the Microsoft SQL Server System CLR (x86) 2008 type.
	Post Installation: Import Geolocation Data Pack	Added optional, manual import steps.
	Post Installation: Enable Delivery Gateways	Added upgrade requirement for Mass Devices—all must be manually enabled after an upgrade.
	Post Installation: Migrate to an Enterprise	Changed the section title from "Setup an Enterprise". Updated screen captures and descriptions to include more detail about migrating to an Enterprise.
	Advanced Server Configuration: Duplicate Organizations Across Systems	Added new section to describe the Organization Duplicator tool, used to duplicate an organization from one system to another.
Release 6.1.8.86 R3	Upgrade: AtHoc: Upgrade Preparation	Added a section discussing unique section names (custom attributes) for Self Service custom tabs. This is a required preupgrade step.
	Upgrade: AtHoc: Upgrade Preparation	Updated path for upgrade.

Release	Section	Update
Release 6.1.8.86 R2	Global: AtHoc Processor	Changed references from AtHocProcessor to AtHoc Services.
	AtHoc Server Requirements	Updated the "Required File System Permissions" table, first row, last column, changed to "Y".
	AtHoc Server Requirements: Application Server	For "Installation Requirements," updated version number for ASP.NET MVC to "4.0".
	AtHoc Server Requirements: AtHoc Service Account	Updated configuration steps for the application pool identities.
	Upgrade: AtHoc: Upgrade Preparation	Updated path for upgrade.
	Upgrade AtHoc: Pre-Upgrade Preparation > Backup Critical Data	Added section discussing geo-location attributes.
	Post-Installation/Upgrade Configuration: IIS Post Installation Checklist	Removed references to Windows Server 2003 and IIS 6.
	Post-Installation/Upgrade Configuration: Set the SSL Client Certificate	Updated instructions and the table. *Read closely for changes.*
	Post Installation Checklist: Application Pools	Table update, new table for AtHoc Services Application Pools.
	Advanced Server Configuration	Moved subsection called "Start the AtHoc Services and Execute IIREST" to the beginning of the chapter.

Release	Section	Update
Release 6.1.8.85 R3, SP4	Post Installation: Install a MIR3 Certificate	Added detailed steps for installing the certificate.
	Post Installation: Enable Delivery Gateways	Added a requirement that you *must* re-enable the AtHoc Mobile Notifier Gateway after upgrading.
	Post Installation: Configure Role-Based Permissions for the AtHoc Notifier Mobile App	Added detailed steps for configuring access to advanced features (anything except Alerts) for AtHoc Notifier v2.4 or later of the mobile application. For those mobile customers using 2.3 or earlier, there are required steps for access to Maps and other advanced features.
	Post Installation: Configure Auto Login	Added work flow for adding new types of access cards.
	Post Installation: Enable Inbound Event manager for IPAWS	Added *required* step for IPAWS implementations.
	Post-Installation: IIS Checklist	Added the note "After upgrading to 6.1.8.86, you must manually start IIS."
	Multiple	Added Windows Server 2012 support.
	Multiple	Added SQL Server 2012 support.
	Appendix A	Added Troubleshooting Appendix.
Release 6.1.8.85 R3, SP1	All	Restored section numbers.
	Chapter 3, Installation Requirements	.Net 3.5 End of Life. Removed this release as an installation requirement.
Release 6.1.8.85 R3	AtHoc Account Requirements	Correction: Changed "Users role" to "Users group" in the second paragraph.
	Installation Requirements	Correction: Removed last row in the table that described SQL Server 2008 R2. Added a row for Microsoft SQL Server System CLR Types.
	Migrate a Pre-Installed Server	Rewrote "Configure AtHoc Database Operations to use Windows Authentication" for clarity.
	Backing up Critical Data	Added critical information for backing up databases and alert and tracking information.
	Supported Upgrade Paths	Updated for current release.
	Configure Client Certificates on the Application Server	New section describes how to configure client certification.
	Set the SSL Client Certificate	Updates to the SSL settings table.
	Server Proxy Configuration	Correction: Added Windows Server 2008 steps.
	Migrate the PSS Polling Agent Configuration File	New section describes how to migrate the configuration file from the application server to the database.

Release	Section	Update
	IIS Post-Installation Checklist	Added information about adding or verifying mime types in II6.
Release 6.1.8.85 R2 CP2	AtHoc Account Requirements	Corrected "ApplicationPoolIdentity" account name.
	Required Group Policies	Corrected GPO name from "Group Policy Operations", to "Group Policy Object."
	Required Group Policies	Corrected the value of "Replace a process level token" in the first table under Required Group Policies.
	Back Up CONFIG Files	Added a section about backing up .CONFIG files before upgrading AtHoc.
	Set Anti-Virus File Exclusions	Added a section about setting anti-virus file exclusions.
	Enable Delivery Gateways	Updated steps for enabling gateways.

Chapter 1: Getting started

BlackBerry AtHoc Networked Crisis Communication is a commercial off-the-shelf (COTS) solution that turns an existing IP network into a comprehensive emergency mass notification system. It is an easily customizable system, which is why military, government, and commercial organizations use BlackBerry AtHoc to provide physical security, force protection, and personnel accountability for their workforce.

BlackBerry AtHoc customers are able to effectively leverage notifications to ensure that critical information reaches the right audiences in a timely manner.

This guide describes the configuration options for the BlackBerry AtHoc product, specifies the installation requirements, and details the installation procedure. This information is provided in the following chapters:

- System Components and Configuration
- BlackBerry AtHoc Server Requirements
- Install BlackBerry AtHoc
- Upgrade BlackBerry AtHoc
- Post Installation / Upgrade Configuration
- Advanced Server Configuration
- Verify BlackBerry AtHoc is Operational

The following topics are covered in this chapter:

System overview

BlackBerry AtHoc Networked Crisis Communication is a flexible, commercial software solution for enterprise-class, subscription-based mass communication. BlackBerry AtHoc system consists of the following basic elements that are illustrated in Figure 1, BlackBerry AtHoc System Elements.

- AtHoc Server
- Operators (Administrators and Publishers)
- AtHoc Desktop App

AtHoc server

The AtHoc Server supplies these capabilities:

- Provides central application functionality, a Web-based user interface for user subscription, delivery preferences, and system administration.
- Enables message routing to targeted users through its delivery engine depending on user-delivery settings and preferences. The Store-and-Forward capability saves alerts for desktop

delivery when a user is offline and delivers them once a user's presence is detected, provided the alert is still alive.

- Schedules recurring alerts for the purposes of performing tests or issuing repeated reminder messages.
- Enables target alerts across multiple systems through cross-systems setup. Alert cascading is also available.
- Provides response tracking, reporting, and archiving features. Extensive audit reports detail operator actions within the system and can help pinpoint the sources of security violations. Real-time aggregated alert delivery and response summary reports are available in a graphical view (bar, graph, or pie charts).
- Stores alerts history for each user automatically.
- Includes APIs and integration modules to alert delivery and dissemination systems such as Telephony Alerting Systems (TAS), SMS aggregators, and wide area speaker array (Giant Voice) systems.
- Includes integration modules with external user directories such as LDAP or Active Directory for user synchronization and import, and end-user authentication.
- Enables windows authentication for BlackBerry AtHoc by adding a new Logon in SQL Server for the domain account and makes the new Logon the owner of all AtHoc databases.
- Includes APIs for integration with external systems and an Agent Platform that enables monitoring of external information sources and generating alerts according to subscription rules.

Operators (administrators and publishers)

Operators serve the following functions in BlackBerry AtHoc:

- Operators are users who can manage the BlackBerry AtHoc system, initiate alerts to be disseminated, and track and report alert publishing information.
- Operators can have multiple roles depending on their assigned tasks and responsibilities. For example, they can be publishers or administrators.
- Operators use a rich Web-based interface to perform management and administration activities as defined by their privileges and permissions.

AtHoc Desktop App

The AtHoc Desktop App serves the following functions in the BlackBerry AtHoc system:

- The AtHoc Desktop App appears as a small purple globe in the end user's system tray.
- When new alert content is published, AtHoc Desktop App displays an audio/visual notification as a desktop popup.
- The end-user can dismiss the desktop popup, choose a response option (when sent), and click a link to obtain additional information about the emergency condition.
- Additional delivery devices include: Web delivery, e-mail, mobile devices, phones, pagers,

TTY/TDD devices, SMS, Giant voice, LMR, and instant messaging (IM).

- The AtHoc Desktop App can be installed on a Windows or an Apple client.

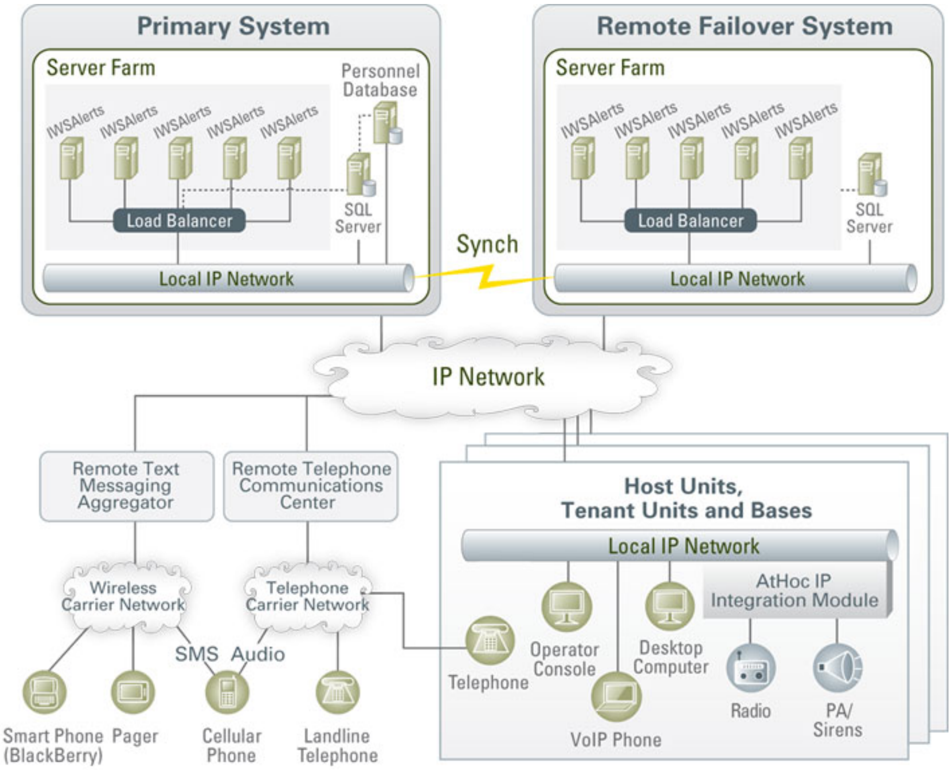


Figure 1: BlackBerry AtHoc System Elements

Note: The available BlackBerry AtHoc features and functionality depend on the licensed BlackBerry AtHoc edition. If you have questions, contact your BlackBerry AtHoc Account Manager.

How to use this guide

Read the overview of BlackBerry AtHoc components and configuration in the following sections of Chapter 2, "System Components and Configuration": *Main Modules*, *AtHoc Physical Configuration*, and *Support for Products, Processes, Procedures, and Protocols*.

Ensure your database and application servers conform to the platform requirements specified in the *BlackBerry AtHoc Capacity Planning Guidelines*.

- For a new installation, follow the instructions in Chapter 5, "Install AtHoc" and Chapter 7, "Post-Installation/Upgrade Configuration."
- For upgrading an existing installation, follow the instructions in Chapter 6, "Upgrade AtHoc" and Chapter 7, "Post-Installation/Upgrade Configuration."

To obtain information on advanced topics including migrating a pre-installed server, configuring IIS processor affinity, increasing the maximum file upload size, and other topics, see Chapter 8, "Advanced Server Configuration."

Contact BlackBerry AtHoc technical support

If you encounter any problems or have questions regarding the BlackBerry AtHoc software, contact BlackBerry AtHoc Technical Support using any of the following methods:

- **Web Site Form:** https://support.athoc.com/customer-support-portal/-login.html
- **Telephone:** (888) GO-ATHOC (462-8462)
- **Email:** athocsupport@blackberry.com

Tip: The Web-based support form is the primary method for contacting BlackBerry AtHoc technical support.

Chapter 2: System components and configuration

This chapter describes the BlackBerry AtHoc components and common configurations.

The following topics are covered in this chapter:

Main modules

The BlackBerry AtHoc platform is composed of two types of server components:

- *Database Server*—Based on Microsoft SQL Server 2012 or Microsoft SQL Server 2014 SP2.
- *Application Server (one or more servers)*—Acts as a Web-based application server that provides all user-related interactions. The application server also runs the IWS Services, which are responsible for scheduling events, providing notification delivery, and running background batch processes used for integration with external applications and content sources.

The database and application servers interact with the AtHoc Desktop App, Web browsers, and various delivery gateways such Telephony and SMS (text messaging). (See the figure below, *Interaction of the Database and Application Servers with Other Components*.) Additionally, the servers provide integration points with enterprise application suites such as LDAP, Active Directory, HR, and corporate portals.

In cases where redundancy is needed, a BlackBerry AtHoc failover solution can be implemented so that if the primary BlackBerry AtHoc platform becomes unreachable, notification capabilities are automatically transferred to a secondary platform.

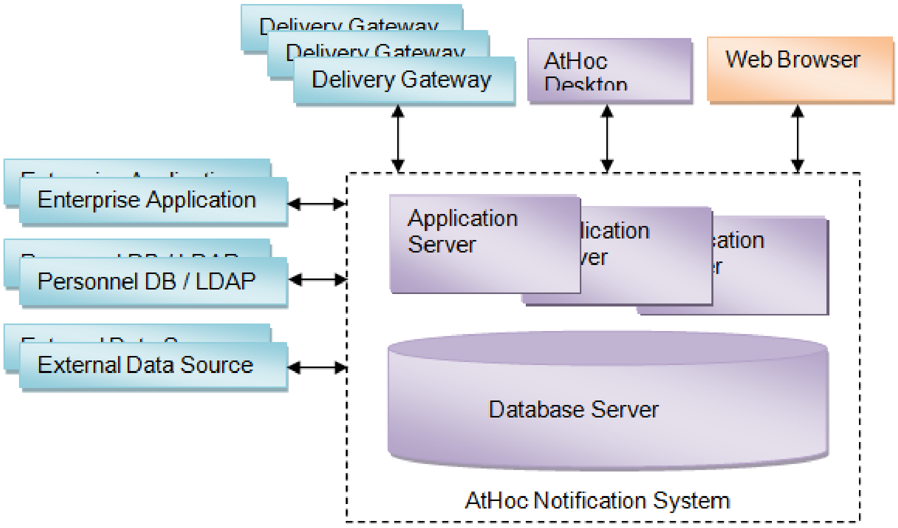


Figure 1: Interaction of the Database and Application Servers with Other Components

BlackBerry AtHoc physical configuration

Although all server components can be installed on the same machine, BlackBerry AtHoc recommends installing each server on different machines. More specifically, the database server is located on one machine, and each application server is installed on another machine.

Database server

The database server can be installed in a clustered database configuration, providing hot failover between the database machines.

Application servers

It is easy and safe to add and remove machines to and from the Web Farm without affecting the end-user experience.

The Web Farm provides HTTP/HTTPS service to the Web browsers and the AtHoc Desktop App.

IWS Services is a website that runs web applications under IIS. The services schedule jobs (such as processing alerts and importing users), poll PSS, and track and report alert responses. Each application runs in its own application pool and the load can be configured on each application server, based on the anticipated load.

Additional high availability can be achieved by installing a fail-over site in an active-passive configuration to support continuous operation in cases of a primary site failure.

Application servers and common system resources

The application servers use common system resources that include the following:

- *Database Server*—Application servers must be able to connect to the database server. The connection string is stored in the registry of each application server.
- *MSMQ (Microsoft Message Queuing)*—BlackBerry AtHoc uses MSMQ for queuing jobs and events. MSMQ is configured on each application server.

The following graphic illustrates the BlackBerry AtHoc physical configuration in a typical redundant setup for a single site.

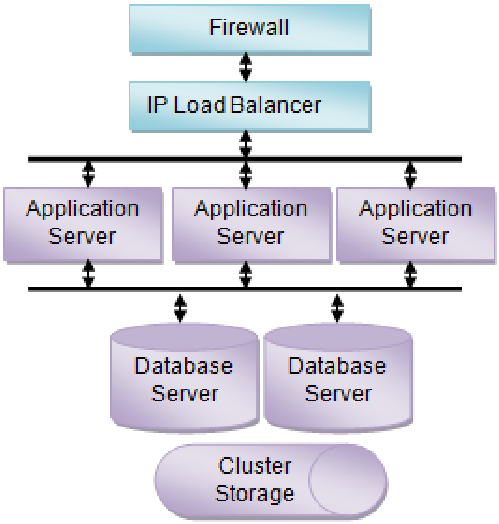


Figure 1: BlackBerry AtHoc Physical Configuration in a Redundant Setup (Single Site)

Support for products, processes, procedures, and protocols

Several third-party components are used to support the BlackBerry AtHoc implementation that includes:

- Backups
- System maintenance and operation monitoring
- Connectivity
- Delivery gateways

Backups

Backups refer to the following:

- Database backup products and processes
- Application server backup products and processes

System maintenance and operation monitoring

System operation monitoring systems include examples such as the following:

- OpenView
- Tivoli

Connectivity

Connectivity refers to the following:

- *Local connectivity*—Providing connectivity between the local machines on which BlackBerry AtHoc is installed. Specifically, it is connectivity between the application server (or servers) and the database machine (or machines).
- *Serving HTTP or HTTPS*—The application servers provide HTTP or HTTPS service to Web browsers and the AtHoc Desktop App. For HTTPS configuration, a Web PKI certificate must be installed on the Web servers.
- *Accessing external HTTP or HTTPS sources*—For integration with external applications and data sources by the application server IWS Services. This connectivity can be configured through a proxy (an authenticating proxy is not supported). If an external telephony calling service is used, Web connectivity from the application servers to the calling service must be established.
- *A firewall*—To protect the BlackBerry AtHoc platform.

Delivery gateway

- AtHoc Cloud Delivery Service East and AtHoc Cloud Delivery Service West are available out of the box and can deliver alerts through Telephony, SMS, and Email.
- OEM Cloud Delivery Service (East) and OEM Cloud Delivery Service (West) are available out of the box and can deliver alerts through Email.

Notification Delivery Service support

BlackBerry AtHoc release 7.3 is compatible with Notification Delivery Service (NDS) version 2.8.5 or higher.

Chapter 3: BlackBerry AtHoc account requirements

You can use a non-system account for the AtHoc application pool identities.

Required group policies

The following account policies are their values are the defaults on Windows Server before any changes due to Security Technical Implementation Guide (STIG) or Group Policy Object (GPO). Any service account that is used to replace the AtHoc application pool identities or IIS_IUSRS must be a User or Group member of the policies as shown in the table.

Policy	Values
Adjust memory quotas for a process	AtHoc application pools
Create global objects	Service
Generate security audits	AtHoc application pools
Impersonate a client after authentication	IIS_IUSRS Service
Log on as a service	AtHoc application pools Service
Replace a process level token	AtHoc application pools

Chapter 4: Install BlackBerry AtHoc

This chapter describes the steps to perform a new installation of BlackBerry AtHoc.

The following topics are covered in this chapter:

Discontinued support for Windows 2008 and SQL Server 2008

Support for Windows 2008 and SQL 2008 was removed. You cannot install or upgrade BlackBerry AtHoc until you upgrade Windows and SQL to one of the following supported versions:

- Windows 2012R2 (64 bit)
- Windows 2016
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014 (without MEMOPT)
- Microsoft SQL Server 2012

Installation requirements

See the *BlackBerry AtHoc Capacity Planning Guidelines* for the hardware and software requirements for installing and upgrading BlackBerry AtHoc.

The following components must be pre-installed:

- Valid certificate if using SSL.
- The Windows components listed in the following table:

Component	Notes
Web Server (IIS) Role	—
Message Queuing Feature	Also called MSMQ.

Component	Notes
.Net Framework v. 4.7	For Windows Server 2012R2 (64 bit), you need to install the HTTP Activation feature under both .NET Framework 3.5 Features and .NET Framework 4.5 Features. Note that although the .Net Framework version is 4.7, the feature shows as .NET Framework 4.5 Features in Windows Server 2012.
DotNetCore.1.0.4_1.1.1-WindowsHosting	—
ASP.NET 2.0 AJAX Extensions 1.0	—
ASP.NET MVC 4.0	—
SQL Server BCP Utility	Command-line utility used to import geographic shape data into the NGGEO database. Used during database upgrade only. **Note:** If BCP is not available, the installation will continue but NGGEO will be empty, and you will need to run the data import manually. See Post Installation/Upgrade Configuration chapter for details.
Required Microsoft SQL Server System CLR Type: • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 (without MEMOPT) • Microsoft SQL Server 2016	Required if the Application Server is not the same machine as the Database Server.

- The Web Server Role Services listed in the table below.

  Note: While adding role services, allow the installation of supporting Role Services when prompted.

Role service	Notes
Static Content	—
Default Document	—
HTTP Errors	—
ASP.NET	—
.NET Extensibility	—
ASP	—
ISAPI Extensions	—
ISAPI Filters	—

Role service	Notes
HTTP Logging	Optional. Useful if there is a need to troubleshoot.
Request Monitor	—
Tracing	Optional. Useful if there is a need to troubleshoot.
Basic Authentication	—
Windows Authentication	For a domain that has “logon as a service” rights.
Request Filtering	—
Static Content Compression	—
Dynamic Content Compression	—
IIS Management Console	—
IIS Management Scripts and Tools	—

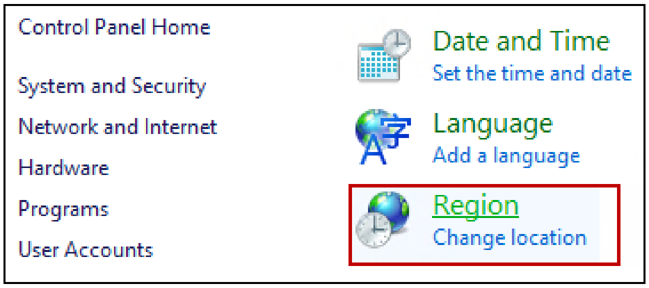
- Installation permissions: The logon account for installing AtHoc should have the following permissions:
  - Copy files and folders.
  - Register DLLs and .NET Assemblies.
  - Write registry keys.
  - Configure IIS (Internet Information Services).

Server locale must be US English

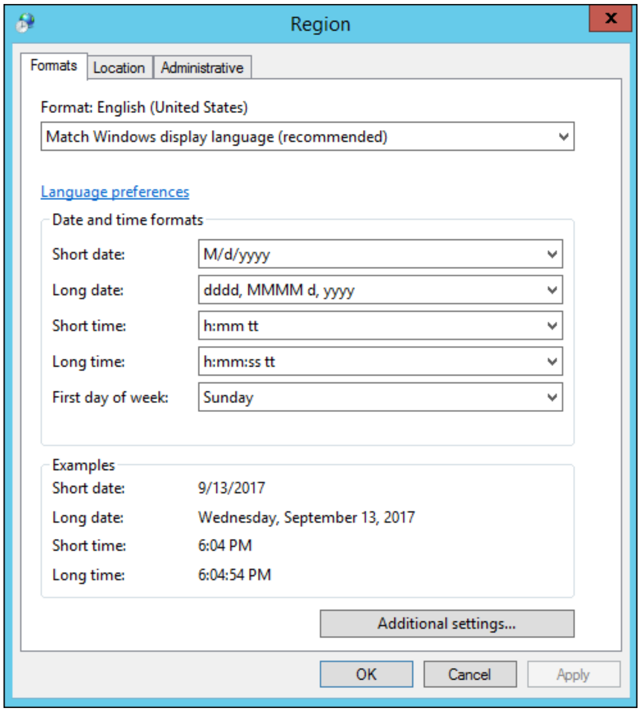
If you switch the locale of the server’s operating system to anything other than US English, errors appear in the event log when you publish an alert and receive tracking information.

To set the locale to US English (Windows 2012 Server or Windows 2016 Server), complete the following steps:

1. Go to the Control Panel and click the **Clock, Language, and Region** link.
2. In the list that appears, click the **Region** link.



3. On the Formats tab, in the Format drop–down list, select **English (United States)**.



Format: English (United States)

Match Windows display language (recommended)

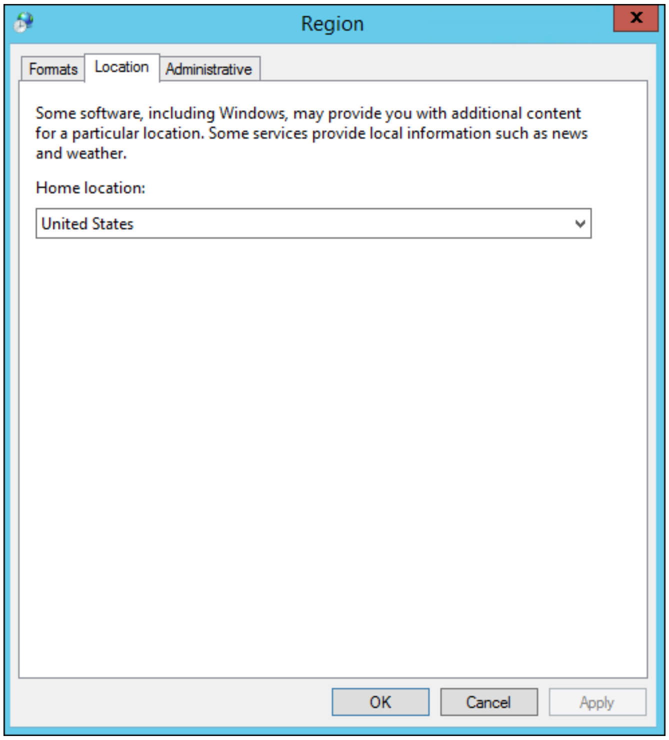
Date and time formats

Short date:	M/d/yyyy
Long date:	dddd, MMMM d, yyyy
Short time:	h:mm tt
Long time:	h:mm:ss tt
First day of week:	Sunday

Examples

Short date:	9/13/2017
Long date:	Wednesday, September 13, 2017
Short time:	6:04 PM
Long time:	6:04:54 PM

4. On the Location tab, in the Home location list, select **United States**.

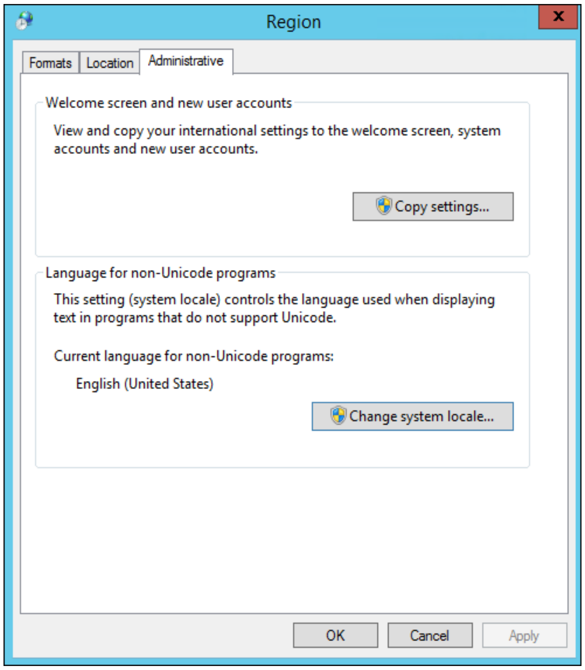


Some software, including Windows, may provide you with additional content for a particular location. Some services provide local information such as news and weather.

Home location:

United States

5. In the Administrative tab, click the **Change system locale** button and select English (United States).



Region

Welcome screen and new user accounts

View and copy your international settings to the welcome screen, system accounts and new user accounts.

Language for non-Unicode programs

This setting (system locale) controls the language used when displaying text in programs that do not support Unicode.

Current language for non-Unicode programs:

English (United States)

6. Reboot the system after you make the system locale change (required).

Configure HTTPS/SSL

It is recommended that an HTTPS / SSL certificate be set up on all application servers before installing AtHoc.

To create a certificate request, complete the following steps:

1. Open the **Internet Services Manager**.
2. Go to the **Properties** for the web site under consideration.
3. Click the **Directory Security** tab.
4. Click the **Server Certificate** button.
5. Follow the wizard to create a new certificate.
6. At the end of the process, provide a file name for storing the certificate request.
7. Send the file to the appropriate certificate authority.

   Note: It is very important that you specify a proper Common Name while requesting the certificate. The Common Name must be the hostname that will be used by your users to access the BlackBerry AtHoc system.

For example, if your users will use `https://alerts.company.com`, you must use **alerts.company.com** as the Common Name. Moreover, in a Web Farm configuration, the Common Name must be the name of the virtual Web Farm.

Obtain a certificate from a Certificate Authority (CA)

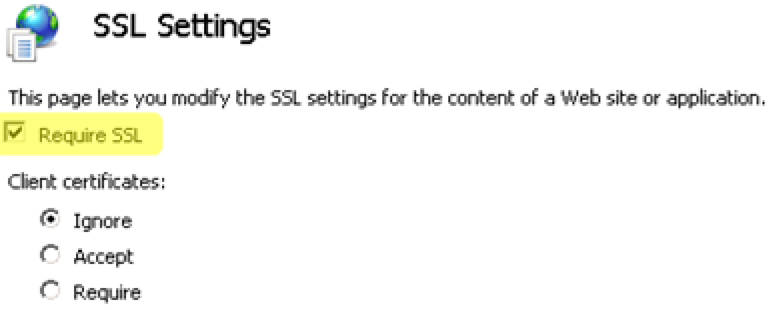
There are commercial Certificate Authorities such as VeriSign or Thawte that can provide a certificate that is recognized by common browsers. In large organizations, there is usually an organizational certificate authority that can provide the required certificate.

To install the certificate (IIS 7 and newer), complete the following steps:

1. Open the **Internet Services Manager**.
2. Select the web site.
3. Click **Bindings** in the right-hand menu.
4. Click **Add**.
5. On the Add Site Binding dialog, select https from the Type drop–down, make changes to **IP Address and Port** if required, and select the SSL certificate.
6. Click **OK**.
7. Select the http binding on the Site Bindings screen and click **Remove**.
8. Accept the prompt and close the Site Bindings screen.

To require SSL Communication (if desired) (IIS 7 and newer), complete the following steps:

1. Open the **Internet Services Manager**.
2. Select **SSL Settings** for the Web site under consideration.
3. Click **Apply**.



SSL Settings

This page lets you modify the SSL settings for the content of a Web site or application.

☑ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require

Database server configuration

The following sections describe elements of the configuration.

Database administration tools

The SQL Server Management Studio and the SQL Server Configuration Manager should be installed. These are options in the SQL Server installer.

SQL server settings

Follow these steps for any edition of SQL Server:

1. Ensure that TCP/IP protocol is enabled. This setting is available in the SQL Server Configuration Manager.
2. Enable the database instance to accept both local and remote connections. This setting is available in the properties for the SQL Server instance, on the Connections page.
3. The SQL Server Browser service is required if you have installed a database instance and the TCP port is dynamic. Enable the SQL Server Browser by turning on the service in Service

Manager. Ensure that the SQL Server Browser service is started in Windows Services manager and that it has the same Startup type as the SQL Server (MSSQLSERVER) service.

4. New database installation and some IWS operations such as Archiving requires that the SQL Server service account have permission to write the file system. Ensure the SQL Server service account has permission to write the file system, or change it to Local System account. The sever account is found in the Windows Service manager, on the Log on tab of the Properties dialog for the SQL Server service. In some installations, access to the database file system using a SQL account is not allowed due to security considerations.
5. Enable SQL server updates by MSI. To ensure that the MSI can reconfigure the system during installation (to prevent an “Ad hoc update to system catalogs is not supported” error), run the following SQL under DB Master before a new install or upgrade:

   ```
   sp_configure 'allow updates', 0;
   ```

   ```
   reconfigure;
   ```
6. The AtHoc Installer (MSI) creates AtHoc databases and sets up user account to access those databases. If a database restore is performed manually and the user accounts are missing, they can be created by running the SQL stored procedure `ATH_CREATE_USERS`. It may be necessary to grant the database user permission to some stored procedures as well. Contact BlackBerry AtHoc Support for information about using this stored procedure.

Login requirements

- An **SA or DBA** login to the database with a machine or domain account is required. Local Administrators and Domain Administrators are not automatically added to the SQL Server **sysadmin** Group.

Configure application server for Windows authentication (optional)

1. Add a new Logon SQL Server for the domain account and make the new logon the owner of all AtHoc databases.
2. Modify all AtHoc application pools and the IUSR logon account to use the new logon.
3. Change the OleDbConnectionString. Change “User Id=ngad;Password=@THOC123;” to “Integrated Security=SSPI;”.

TempDB (system) database configuration

- Ensure that there are four data files. Each file should have an initial size of 1GB and a maximum size set to Unrestricted.
- Ensure that there is one log file. The log file should have an initial size of 512 MB and a maximum size set to 2 GB.
- Set Update Statistics: True in Database properties.
- At least 8 GB must be available on the storage array to allow for the TempDB to grow as needed by SQL Server.

The number of Data files and log files is the same regardless of the number of CPU’s.

Windows Server Firewall exclusion rule

If the Windows Server firewall is turned on, create a firewall inbound exclusion rule or turn off the firewall by completing the following steps:

1. Open **Server Manager**.
2. Select **Windows Firewall with Advanced Security** under Configuration.
3. Click **Inbound Rules** in the working area.
4. Click **New Rule**.
5. Select **Port** for the rule type.
6. Enter the port number (default is 1433 unless using an instance; find the port using Configuration Manager).
7. Select **Allow Connection**.
8. Apply to all.
9. Provide a name like “SQL Server Connection” and click **Finish**.

Clustered database configuration

The BlackBerry AtHoc database server can be installed in a single database configuration or in a clustered failover configuration. The database can be installed in a shared environment where the database serves other applications as well.

Clustered database support provides higher availability in case a database server crashes, with automatic failover to the other database machine, and then failback when the primary database machine is back online. BlackBerry AtHoc considers the database server as a single database resource. For exact database configuration and setup in a clustered environment, see the relevant Windows Server 2016, or 2012 R2 (64 bit) clustering support, and the database configuration and setup for failover (it is specific to the database release).

Installing BlackBerry AtHoc on a clustered database server configuration is different from a regular installation. Consult with the BlackBerry AtHoc Professional Services team if a clustered database environment is used.

For detailed configuration steps, see Install BlackBerry AtHoc on a clustered database.

Database server installation

During a new installation, run the AtHoc Installer (MSI) on the database server. The MSI supports both SQL Server authentication and Windows authentication connections to SQL Server. A windows authentication connection requires the users machine or domain login to have a login in SQL Server, and that login must be a sysadmin.

The database server must be installed first when installing separate application and database servers. When installing both application and database servers on the same machine (a “combo install”), they can be installed at the same time.

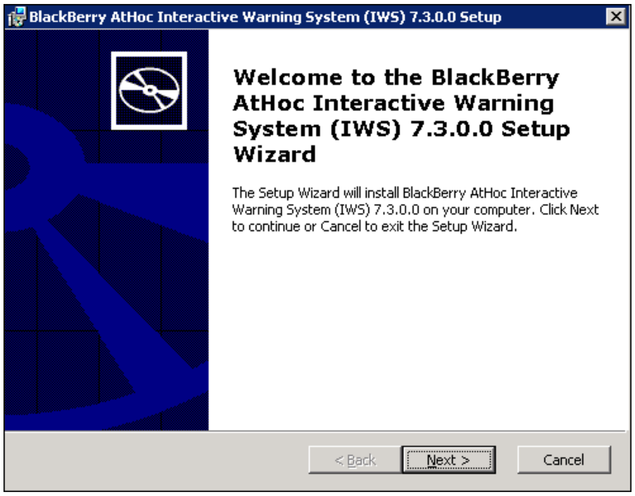
To install the BlackBerry AtHoc database server, complete the following steps:

1. Start the installation by opening an elevated command prompt, navigate to the folder with the .BAT file, then type the .BAT file name and press Enter to run it. The .BAT file name follows

the naming convention "AtHocIWS_AirForce_7.0.x.x_build.bat.

Tip: The .BAT file distributed with the MSI generates a log file of the installer actions. The log file, `ATHOC_yyyy_mm_dd_hh_mm_AM|PM.log`, is created in the root of the C: directory.

2. To open an elevated command prompt, locate cmd.exe in the program search, then right-click on cmd.exe and choose Run as Administrator. If the User Account Control window appears, click Yes to run the Windows Command Prompt as Administrator.
3. On the Welcome screen, click **Next**.

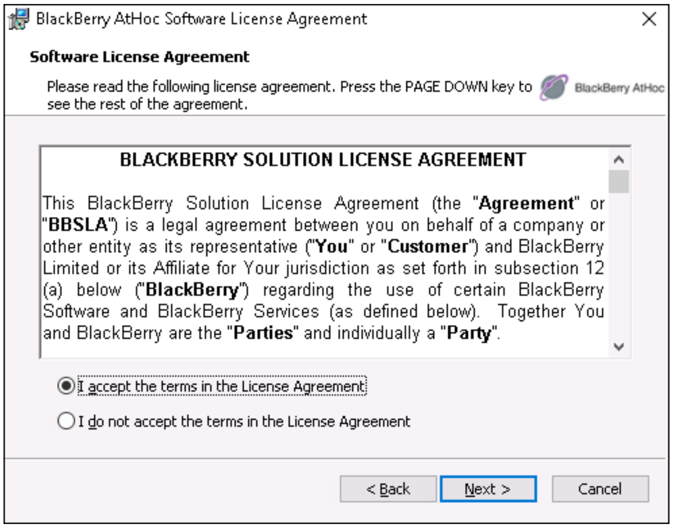


BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 Setup

Welcome to the BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 Setup Wizard

The Setup Wizard will install BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Accept the Software License Agreement, then click **Next**.



BlackBerry AtHoc Software License Agreement

Software License Agreement

Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.

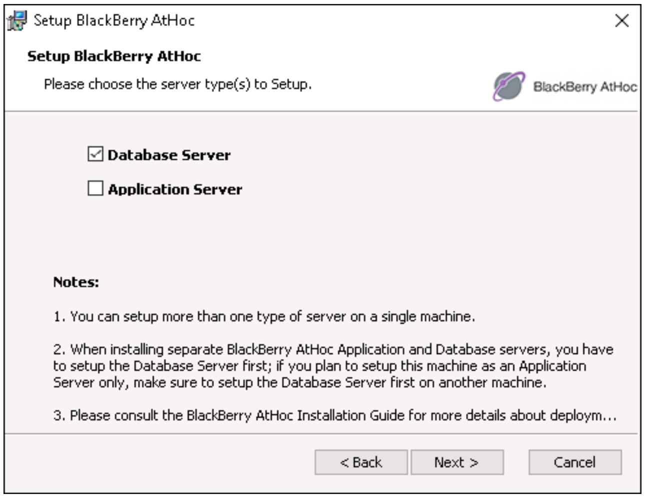
BLACKBERRY SOLUTION LICENSE AGREEMENT

This BlackBerry Solution License Agreement (the "**Agreement**" or "**BBSLA**") is a legal agreement between you on behalf of a company or other entity as its representative ("**You**" or "**Customer**") and BlackBerry Limited or its Affiliate for Your jurisdiction as set forth in subsection 12 (a) below ("**BlackBerry**") regarding the use of certain BlackBerry Software and BlackBerry Services (as defined below). Together You and BlackBerry are the "**Parties**" and individually a "**Party**".

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

5. Choose the **Database Server** check box, then click **Next**.



Setup BlackBerry AtHoc

Setup BlackBerry AtHoc

Please choose the server type(s) to Setup.

☑ **Database Server**

□ **Application Server**

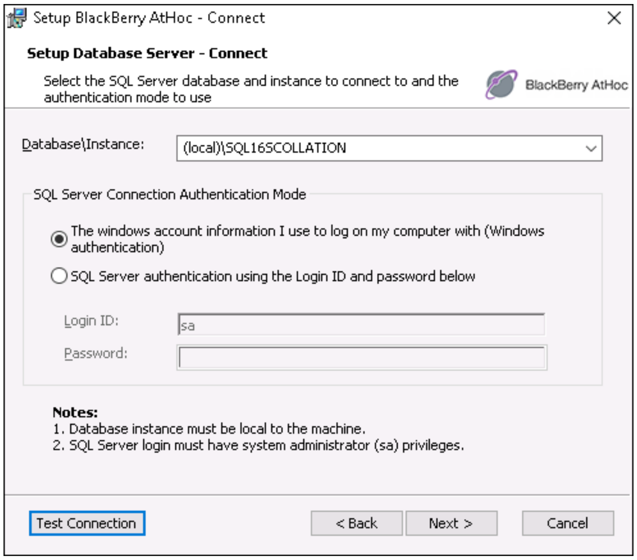
Notes:

1. You can setup more than one type of server on a single machine.

2. When installing separate BlackBerry AtHoc Application and Database servers, you have to setup the Database Server first; if you plan to setup this machine as an Application Server only, make sure to setup the Database Server first on another machine.

3. Please consult the BlackBerry AtHoc Installation Guide for more details about deploym...

6. Enter the machine name of the database server and the instance name, if any, then select the Authentication Mode and provide the credentials if required.



Setup BlackBerry AtHoc - Connect

Setup Database Server - Connect

Select the SQL Server database and instance to connect to and the authentication mode to use

Database\Instance: (local)\SQL16SCOLLATION

SQL Server Connection Authentication Mode

● The windows account information I use to log on my computer with (Windows authentication)

○ SQL Server authentication using the Login ID and password below

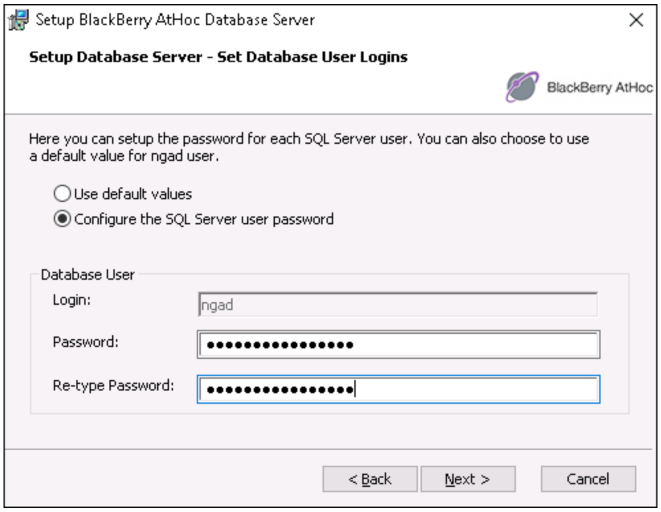
Login ID: sa

Password:

Notes:

1. Database instance must be local to the machine.
2. SQL Server login must have system administrator (sa) privileges.

7. Set up the password for the ngad database user by supplying your own values or using the defaults. Click **Next**.



Setup BlackBerry AtHoc Database Server

Setup Database Server - Set Database User Logins

Here you can setup the password for each SQL Server user. You can also choose to use a default value for ngad user.

○ Use default values
● Configure the SQL Server user password

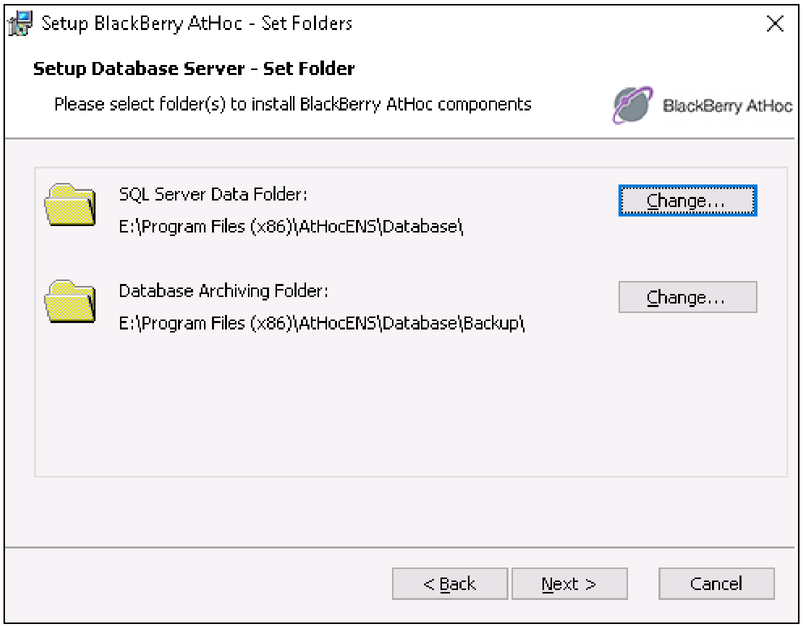
Database User

Login: ngad

Password: ••••••••••••••••

Re-type Password: ••••••••••••••••

8. Specify the folders to install the BlackBerry AtHoc components by clicking the associated **Change** button to specify the SQL Server data folder and the Database archiving folder that you want. Or click **Next** to accept the default locations for both folders.



Setup BlackBerry AtHoc - Set Folders

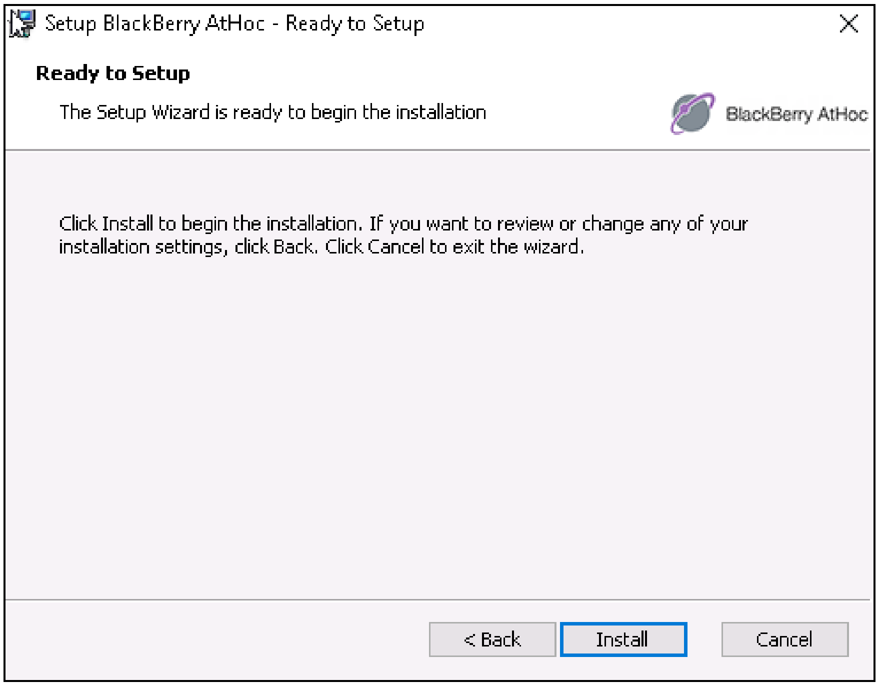
Setup Database Server - Set Folder

Please select folder(s) to install BlackBerry AtHoc components

SQL Server Data Folder:
E:\Program Files (x86)\AtHocENS\Database\

Database Archiving Folder:
E:\Program Files (x86)\AtHocENS\Database\Backup\

9. Click **Install** to begin the installation or click **Back** to change the installation settings.

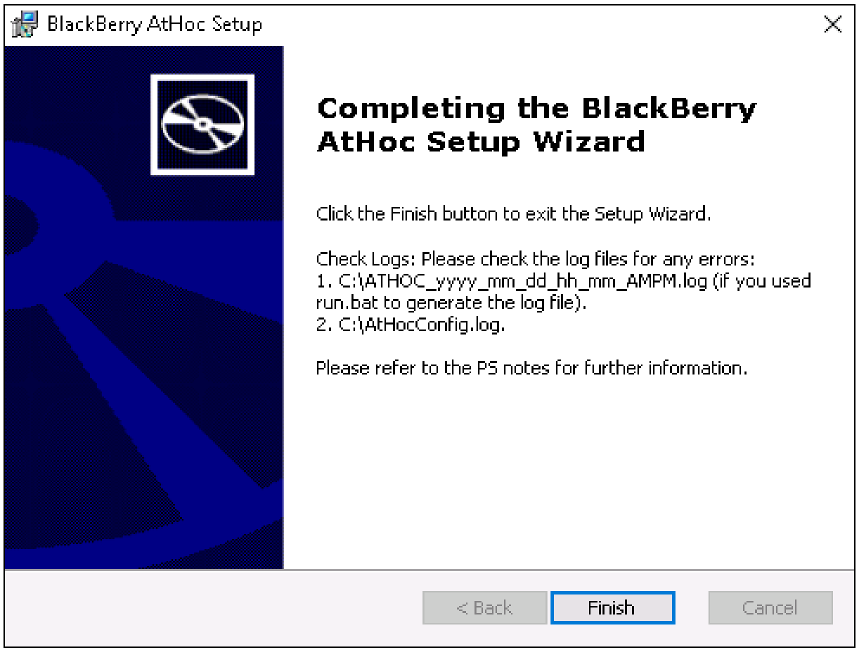


Ready to Setup

The Setup Wizard is ready to begin the installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

10. View the onscreen progress bar to gauge the status of the installation.
11. When the installation completes, click **Finish** to exit the Setup Wizard.



Completing the BlackBerry AtHoc Setup Wizard

Click the Finish button to exit the Setup Wizard.

Check Logs: Please check the log files for any errors:
1. C:\ATHOC_yyyy_mm_dd_hh_mm_AMPM.log (if you used run.bat to generate the log file).
2. C:\AtHocConfig.log.

Please refer to the PS notes for further information.

12. Continue with the installation of the application server or servers, as described in the next section.

Install BlackBerry AtHoc on a clustered database

To install on a clustered database or 64-bit SQL Server platform, complete the following steps:

Note: Contact BlackBerry AtHoc Technical Support to obtain the SQL scripts required for this procedure.

1. Set up a staging database server running SQL Server.
2. Proceed with the installation of the database server on the staging database server, as described in the "Database Server Installation" section of this guide.
3. After the database server installation is complete, back up the four new AtHoc databases on the staging Server, and then move the backups from the staging server to the production database server.
4. Restore the four databases on the production database server using the Enterprise Manager or by running the stored procedure `dbo.RestoreATPUB` from the master database.
5. Recreate AtHoc database users by running the stored procedure `dbo.ATH_CREATE_USERS` from the master database.
6. Continue with the installation of the application server, as described in the "Application server installation" section of this guide.

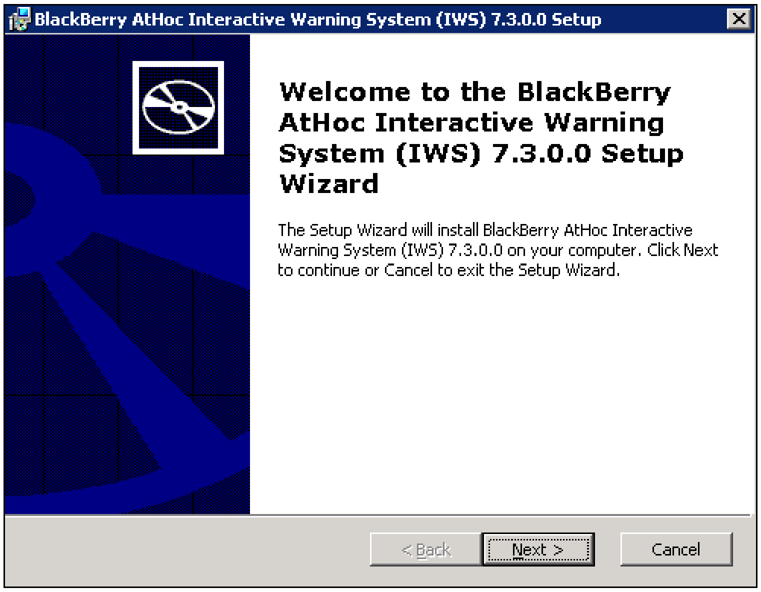
Application server installation

For a new application server install, the application server and database server must be installed on separate machines. The AtHoc installer (MSI) creates a trusted connection to the database, which uses the current users domain account. The account must have a login in SQL Server, and that login must be a sysadmin.

To install the application server, complete the following steps:

1. Start the installation by opening an elevated command prompt, navigate to the folder with the .BAT file, then type the .BAT file name and press Enter to run it. The .BAT file name follows the naming convention "AtHocIWS_AirForce_7.0.x.x_build.bat.

   Tip: The .BAT file distributed with the MSI generates a log file of the installer actions. The log file, `ATHOC_yyyy_mm_dd_hh_mm_AM|PM.log`, is created in the root of C:.
2. To open an elevated command prompt, locate cmd.exe in the program search, then right-click on cmd.exe and choose Run as Administrator. If the User Account Control window appears, click Yes to run the Windows Command Prompt as Administrator.
3. On the Welcome screen, click **Next**.

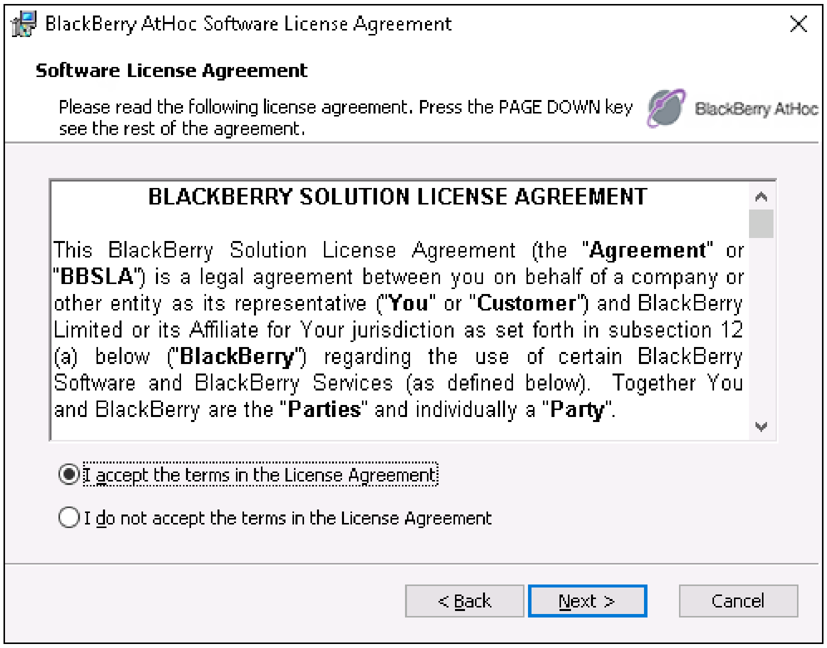


BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 Setup

Welcome to the BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 Setup Wizard

The Setup Wizard will install BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Accept the Software License Agreement, then click **Next**.



BlackBerry AtHoc Software License Agreement

Software License Agreement

Please read the following license agreement. Press the PAGE DOWN key see the rest of the agreement.

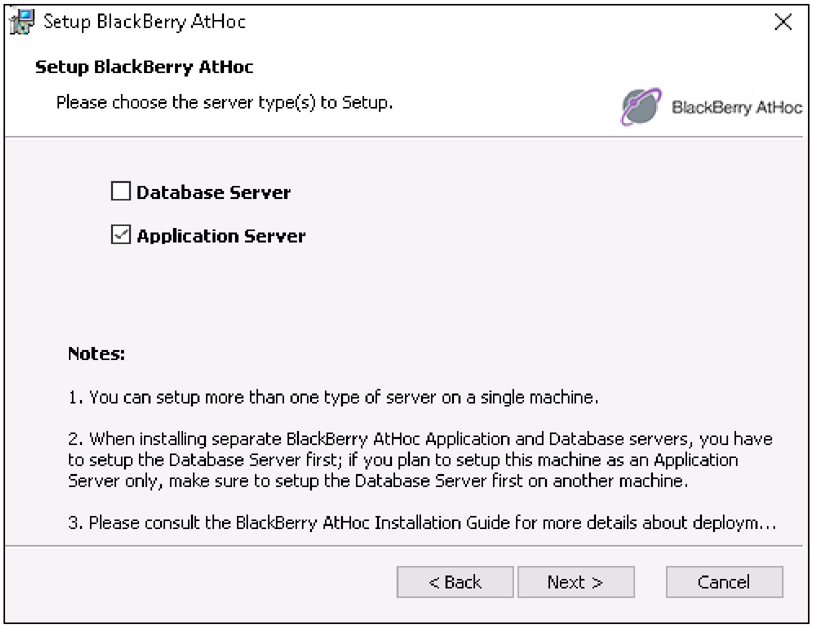
BLACKBERRY SOLUTION LICENSE AGREEMENT

This BlackBerry Solution License Agreement (the "**Agreement**" or "**BBSLA**") is a legal agreement between you on behalf of a company or other entity as its representative ("**You**" or "**Customer**") and BlackBerry Limited or its Affiliate for Your jurisdiction as set forth in subsection 12 (a) below ("**BlackBerry**") regarding the use of certain BlackBerry Software and BlackBerry Services (as defined below). Together You and BlackBerry are the "**Parties**" and individually a "**Party**".

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

5. Choose the **Application Server** check box, then click **Next**.



Setup BlackBerry AtHoc

Setup BlackBerry AtHoc

Please choose the server type(s) to Setup.

☐ **Database Server**

☑ **Application Server**

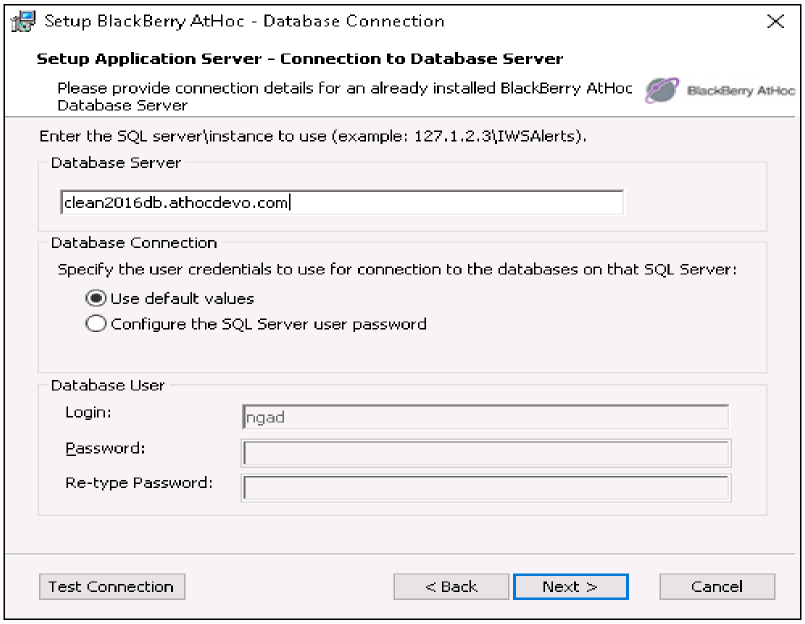
Notes:

1. You can setup more than one type of server on a single machine.

2. When installing separate BlackBerry AtHoc Application and Database servers, you have to setup the Database Server first; if you plan to setup this machine as an Application Server only, make sure to setup the Database Server first on another machine.

3. Please consult the BlackBerry AtHoc Installation Guide for more details about deploym...

6. If using a named instance, manually enter the server name or IP and instance name.
7. Click **Test Connection**. The AtHoc Test Connection script tests the connection through the `ngad` account and the SQL databases and it tests a trusted connection that does not include the user ID and password.



Setup BlackBerry AtHoc - Database Connection

Setup Application Server - Connection to Database Server

Please provide connection details for an already installed BlackBerry AtHoc Database Server

Enter the SQL server\instance to use (example: 127.1.2.3\IWSAlerts).

Database Server: clean2016db.athocdevo.com

Database Connection

Specify the user credentials to use for connection to the databases on that SQL Server:

● Use default values

○ Configure the SQL Server user password

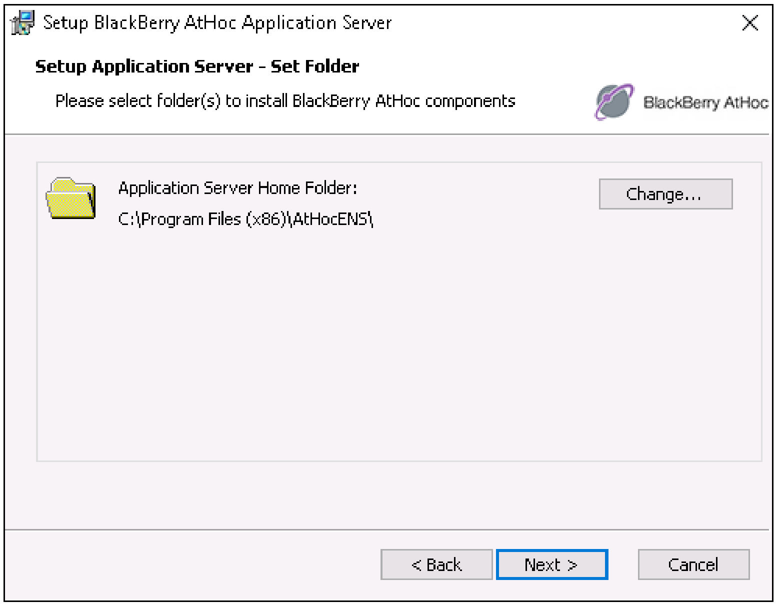
Database User

Login: ngad

Password:

Re-type Password:

8. Specify the application server home folder to install the BlackBerry AtHoc components. Click **Change** to browse for the location that you want or click **Next** to accept the default location.

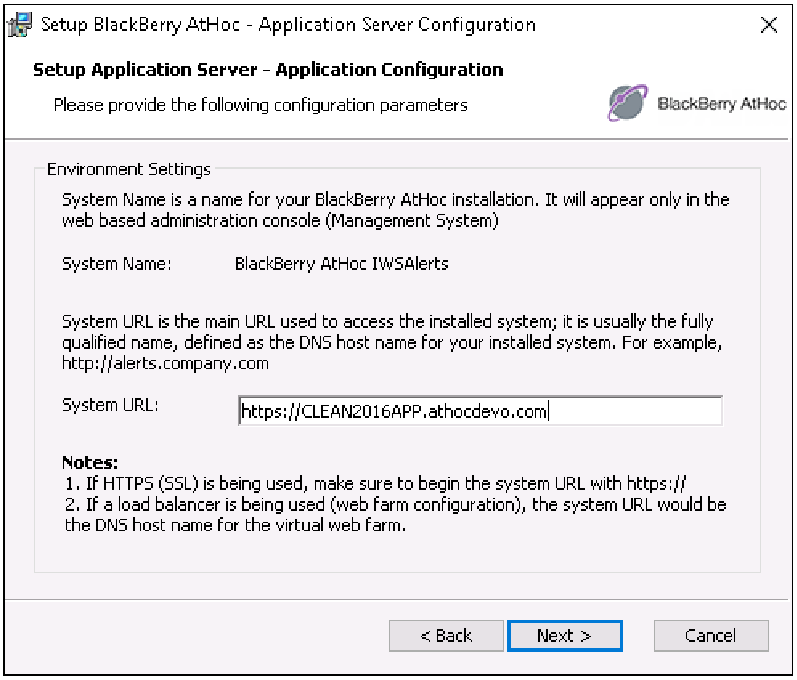


Setup Application Server - Set Folder

Please select folder(s) to install BlackBerry AtHoc components

Application Server Home Folder:
C:\Program Files (x86)\AtHocENS\

9. Enter the system URL to access BlackBerry AtHoc, then click **Next**.
10. Ensure that a fully qualified URL is used.



Setup Application Server - Application Configuration

Please provide the following configuration parameters

Environment Settings

System Name is a name for your BlackBerry AtHoc installation. It will appear only in the web based administration console (Management System)

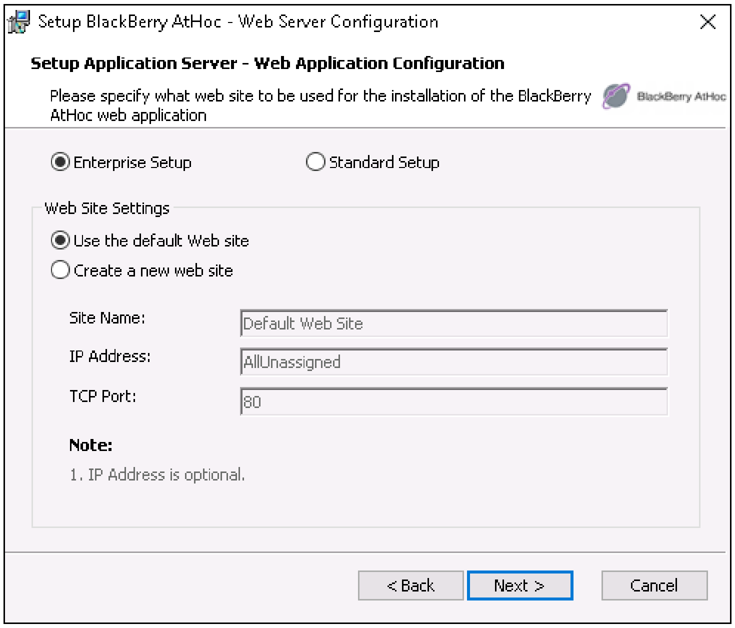
System Name: BlackBerry AtHoc IWSAlerts

System URL is the main URL used to access the installed system; it is usually the fully qualified name, defined as the DNS host name for your installed system. For example, http://alerts.company.com

System URL: https://CLEAN2016APP.athocdevo.com

Notes:
1. If HTTPS (SSL) is being used, make sure to begin the system URL with https://
2. If a load balancer is being used (web farm configuration), the system URL would be the DNS host name for the virtual web farm.

11. Specify the IIS configuration type:
    - **The type of setup:** Choose Enterprise Setup for a regular configuration or Standard Setup for the AtHoc Mobile Alerting System (MAS).
    - **The Web Site Settings for the BlackBerry AtHoc Web application installation:** Use the default Web site or choose a new Web site that you want and provide the associated details.



Setup BlackBerry AtHoc - Web Server Configuration

Setup Application Server - Web Application Configuration

Please specify what web site to be used for the installation of the BlackBerry AtHoc web application

● Enterprise Setup ○ Standard Setup

Web Site Settings

● Use the default Web site

○ Create a new web site

Site Name: Default Web Site

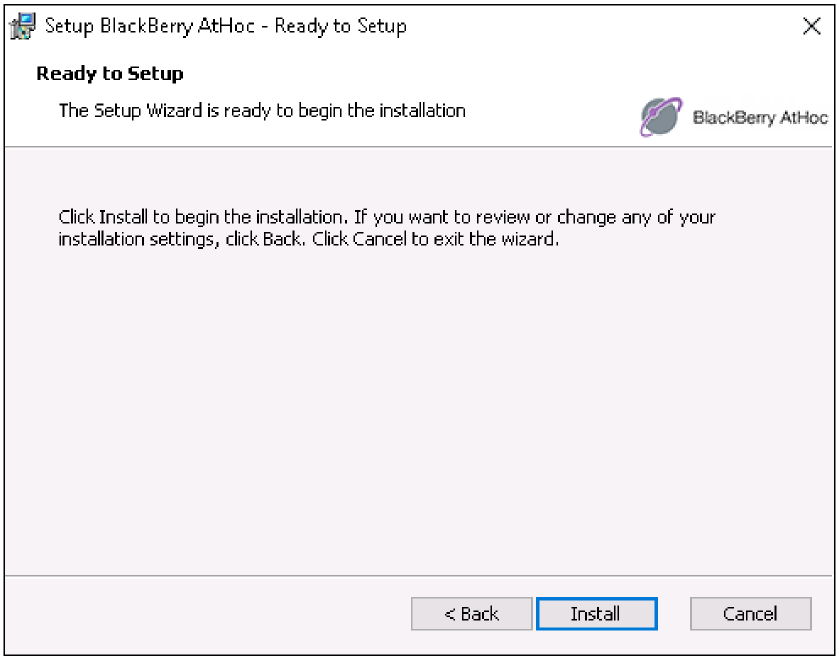
IP Address: AllUnassigned

TCP Port: 80

Note:

1. IP Address is optional.

12. Click **Install** to begin the database server installation or click **Back** to change the installation settings.



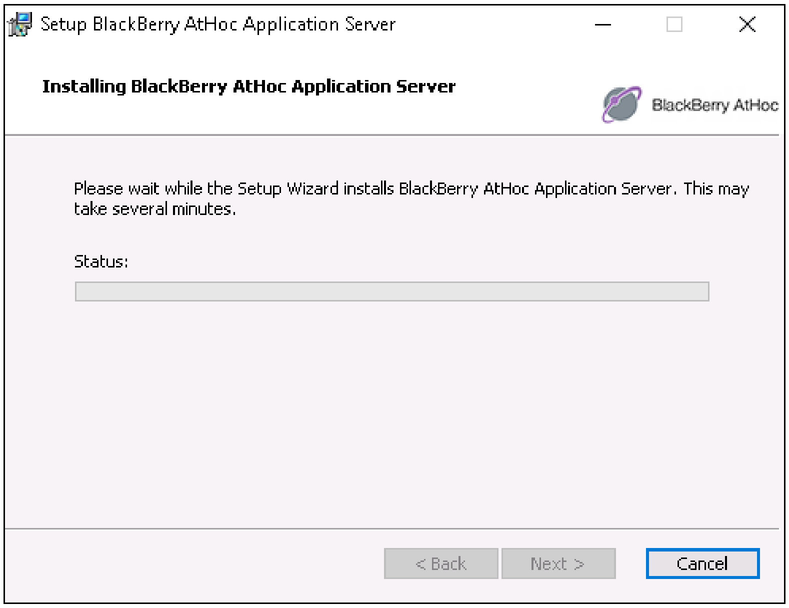
Setup BlackBerry AtHoc - Ready to Setup

Ready to Setup

The Setup Wizard is ready to begin the installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

13. View the onscreen progress bar to gauge the status of the installation.



Installing BlackBerry AtHoc Application Server

Please wait while the Setup Wizard installs BlackBerry AtHoc Application Server. This may take several minutes.

Status:

14. When the installation completes, click **Finish** to exit the Setup Wizard.

Required file system permissions

The following rights are needed for User and IUSR access to AtHoc folders:

Folder	Accounts	Rights	Set by MSI
<%AtHocENS%>\ServerObjects\uploadStage	Users	Modify	Y
<%AtHocENS%>\CommonSiteData\AthocData\Upload	Users	Modify	Y
<%AtHocENS%>\wwwroot\client\Content\charttmpfolder	IUSR Users	Modify	Y
<%AtHocENS%>\wwwroot\D911Server\tempMedia	IUSR Users	Modify	Y

Chapter 5: Upgrade BlackBerry AtHoc

This chapter describes how to upgrade an existing installation of BlackBerry AtHoc.

See the *BlackBerry AtHoc Capacity Planning Guidelines* for the hardware and software requirements for installing and upgrading BlackBerry AtHoc.

Discontinued support for Windows 2008 and SQL Server 2008

Support for Windows 2008 and SQL 2008 was removed. You cannot install or upgrade BlackBerry AtHoc until you upgrade Windows and SQL to one of the following supported versions:

- Windows 2012R2 (64 bit)
- Windows 2016
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014 (without MEMOPT)
- Microsoft SQL Server 2012

Upgrade preparation

This section describes the steps you need to complete to prepare to upgrade to the new release.

Note: Before you perform an upgrade, make sure that BlackBerry AtHoc and any modules are fully functional. After the upgrade, verify that BlackBerry AtHoc and any modules are working.

See the *BlackBerry AtHoc Capacity Planning Guidelines* for the hardware and software requirements for installing and upgrading BlackBerry AtHoc.

Supported upgrade paths

The following table describes the upgrade paths that are supported for this release.

Installed version	Upgrade
7.0.0.2	7.3
6.1.8.87CP1CHF3	7.3

You can also perform a direct installation of version 7.3.

Database server preparation

Complete the following preparation tasks for upgrading the database server.

All versions preparation steps

Required unless indicated.

Backup critical data

Backup databases, archive alerts, and clean up old alerts and diagnostic logs that are no longer needed.

Databases

- Stop any replication or failover activities with Double Take software, or with operating system-level replication.
- To avoid overwriting critical data, save the database backups on a different drive than the drive on which AtHocENS folder and the SQL Server files are located.
- Name the backup files with the correct database names. Using the correct names helps you to recover the correct files during a failure. For example, name the backup file for the ngaddata database as `ngaddata_upgrade_7312013.bak`.
- Ensure that TempDB, in SQL Server, has enough space before the upgrade. The upgrade will fail if it runs out of space. To learn about TempDB requirements, see TempDB (System) Database Configuration in this guide.

Alerts and user data

- End *all* alerts, before upgrading.
  - Live alerts may be lost during an upgrade. The AtHoc Installer attempts to end all alerts, but it is better to end them before running the installer.
  - If you do not end alerts before you upgrade, you might lose alerts or have issues when closing the active alerts.
  - Run SQL to end all Accountability events.
- To reduce upgrade time, reduce the size of the database and the Diagnostics log.
  - Purge old or unneeded alerts to decrease the database size. For example, if you need to save alerts for one year, purge alerts older than a year to reduce the database size. Use the SYSTEM TASK in each organization to purge the alerts.
  - Purge the Diagnostic log by exporting or archiving the Diagnostic log data and then clear the log.
- If you are not using AD Sync, backup your user data. You can export all users in critical organizations to Microsoft Excel .csv files.

Application servers preparation

The following sections describe actions that you need to take to prepare to upgrade the application servers.

Stop services

Stop IIS. Set World Wide Web Publishing Service to Manual.

In a multiple application server environment, repeat the above step on each application server.

Back up custom code

Back up custom code if it exists.

Back up duplicated device configurations

If you duplicated any devices, save the XML files for the duplicated devices that are in the following directories to a temporary directory:

- `\AtHocENS\ServerObjects\utils\AddOnModules\Packages`
- `\AtHocENS\ServerObjects\utils\AddOnModules\IIM\Enable`

Important: After you complete the upgrade, copy the files back to these folders.

Application server upgrade

During an upgrade, run the AtHoc installer (MSI) on the application server. The MSI uses a Windows authentication connection to SQL Server. The user's machine or domain login must have a login in SQL Server, and that login must be a sysadmin. See the note below if Windows authentication is not possible and you must use SQL Server authentication.

Note: If a trusted connection cannot be used, you can specify a specific account for the AtHoc Installer to use during the upgrade by appending the following parameters to the msiexe command line in the BAT file:

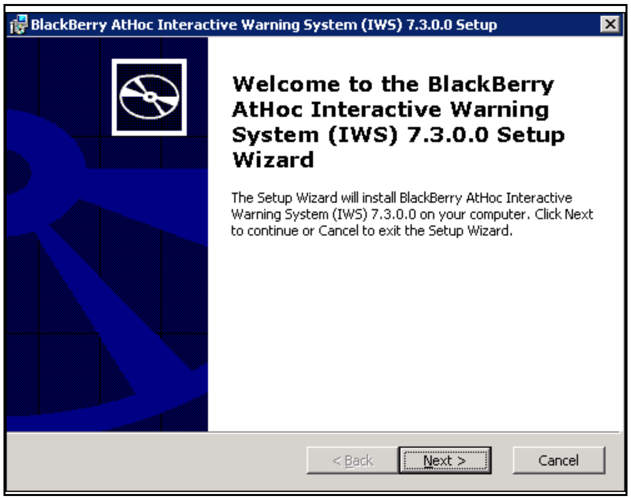
- IS_SQLSERVER_AUTHENTICATION=1
- IS_SQLSERVER_USERNAME=sa_account_name
- IS_SQLSERVER_PASSWORD=sa_account_password

Upgrading application servers and a database server that are on separate machines requires running the AtHoc Installer (MSI) *one time on each application server, then after all application servers are upgraded run it again on one of the application servers*.

> **Note:** If the database is upgraded before all app servers are upgraded, you won't be able to upgrade the remaining app servers.

1. Start the installation by opening an elevated command prompt, navigate to the folder with the .BAT file, then type the .BAT file name and press Enter to run it. The .BAT file name follows the naming convention "AtHocIWS_AirForce_7.0.x.x_build.bat.

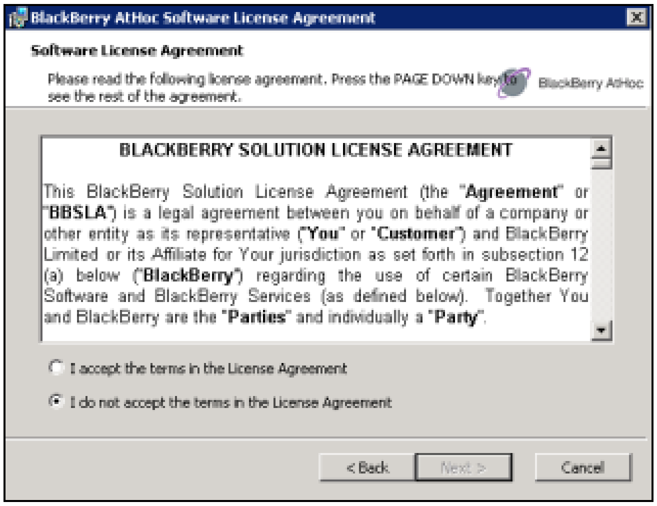
   Tip: The .BAT file distributed with the MSI generates a log file of the installer actions. The log file, `ATHOC_yyyy_mm_dd_hh_mm_AM|PM.log`, is created in the root of C:.
2. To open an elevated command prompt, locate cmd.exe in the program search, then right-click on cmd.exe and choose Run as Administrator. If the User Account Control window appears, click Yes to run the Windows Command Prompt as Administrator.)"
3. In the Welcome screen, click **Next**.


BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 Setup

Welcome to the BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 Setup Wizard

The Setup Wizard will install BlackBerry AtHoc Interactive Warning System (IWS) 7.3.0.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Accept the Software License Agreement, then click **Next**.


BlackBerry AtHoc Software License Agreement

Software License Agreement

Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.

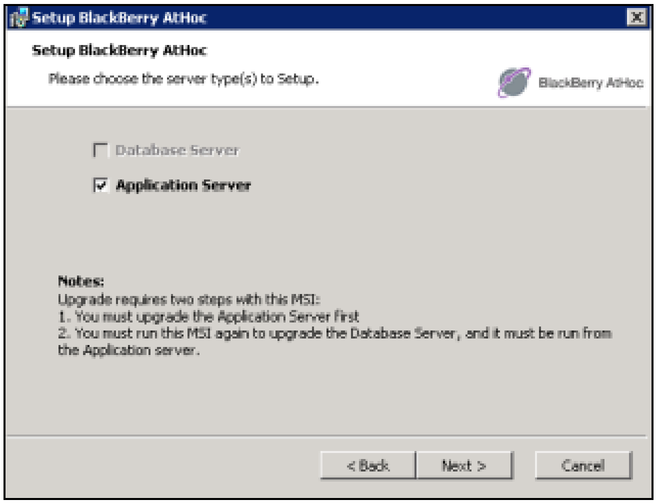
BLACKBERRY SOLUTION LICENSE AGREEMENT

This BlackBerry Solution License Agreement (the "**Agreement**" or "**BBSLA**") is a legal agreement between you on behalf of a company or other entity as its representative ("**You**" or "**Customer**") and BlackBerry Limited or its Affiliate for Your jurisdiction as set forth in subsection 12 (a) below ("**BlackBerry**") regarding the use of certain BlackBerry Software and BlackBerry Services (as defined below). Together You and BlackBerry are the "**Parties**" and individually a "**Party**".

○ I accept the terms in the License Agreement

● I do not accept the terms in the License Agreement

5. Agree to the upgrade prompt (window not shown).
6. Select the **Application Server** check box, then click **Next**.


Setup BlackBerry AtHoc

Setup BlackBerry AtHoc

Please choose the server type(s) to Setup.

☐ Database Server

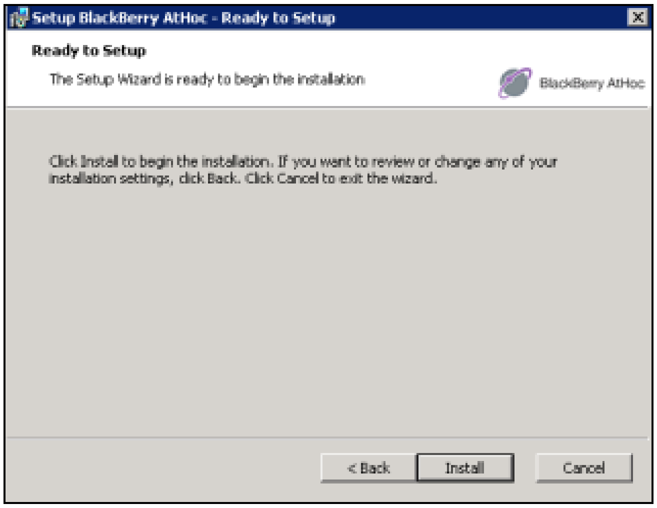
☑ Application Server

Notes:
Upgrade requires two steps with this MSI:
1. You must upgrade the Application Server first
2. You must run this MSI again to upgrade the Database Server, and it must be run from the Application server.

7. If any prerequisites are missing, the installer will display a message listing them. Click **OK** on the message, the installation will abort. Install the prerequisites and run the MSI again.

   For detailed information about the prerequisites, see Installation Requirements.

8. Click **Install**.



Setup BlackBerry AtHoc - Ready to Setup

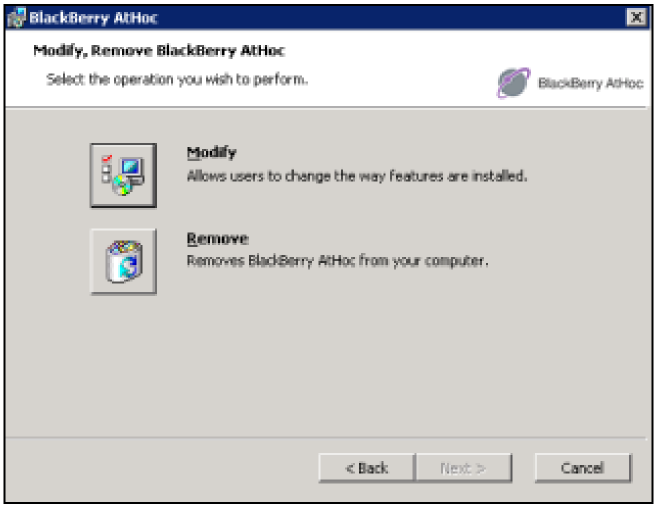
Ready to Setup

The Setup Wizard is ready to begin the installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Database server upgrade

1. Run the MSI a second time to upgrade the database server. Click **Modify** on the first screen.



BlackBerry AtHoc

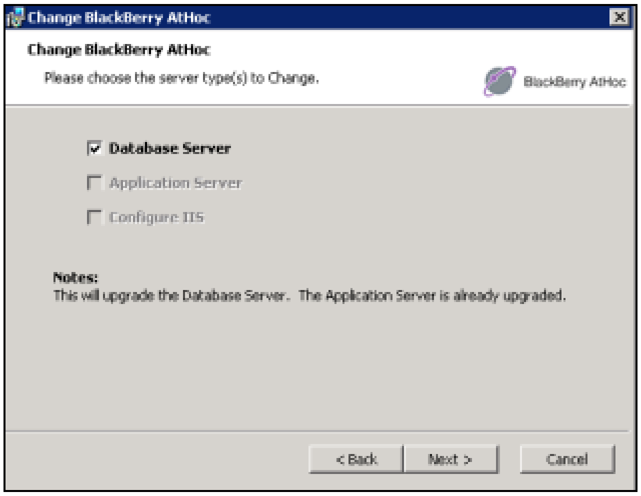
Modify, Remove BlackBerry AtHoc

Select the operation you wish to perform.

Modify
Allows users to change the way features are installed.

Remove
Removes BlackBerry AtHoc from your computer.

2. Select the **Database Server** check box, then click **Next**.



Change BlackBerry AtHoc

Change BlackBerry AtHoc

Please choose the server type(s) to Change.

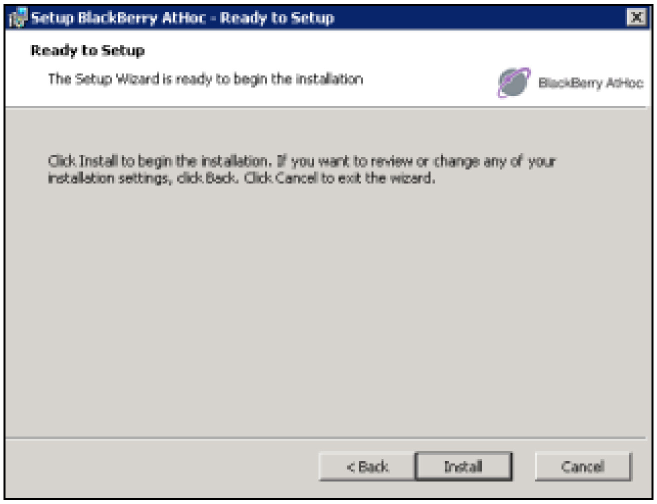
☑ Database Server

□ Application Server

□ Configure IIS

Notes:
This will upgrade the Database Server. The Application Server is already upgraded.

3. Click **Install** and follow the prompts in the Setup wizard.



Setup BlackBerry AtHoc - Ready to Setup

Ready to Setup

The Setup Wizard is ready to begin the installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Chapter 6: Post-installation or upgrade configuration

This chapter describes component configurations that are performed once BlackBerry AtHoc is installed. There is no recommended order to the sections in this chapter.

(Optional) Configure client certificates on the application server

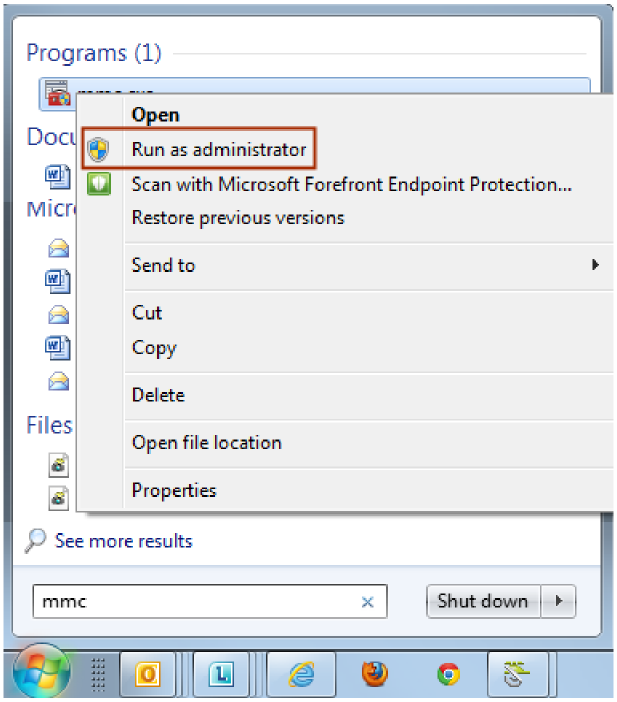
These step are required if client certificates are intended to be used with the BlackBerry AtHoc system.

Configure Client Certificates on each application server so that they can make secure outbound requests to the database server.

To install and configure the client certificate, complete the following steps.

Note: These steps assume that you already have a certificate with a private key.

1. Log in to the application server.
2. Copy the client certificate to the file system.
3. Open Microsoft Management Console (MMC).
   a. From the Start menu, find MMC.

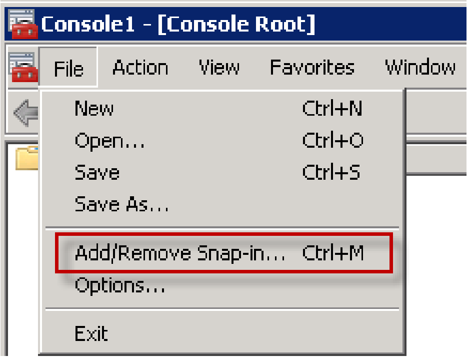


   b. Right click and select **Run as administrator**.

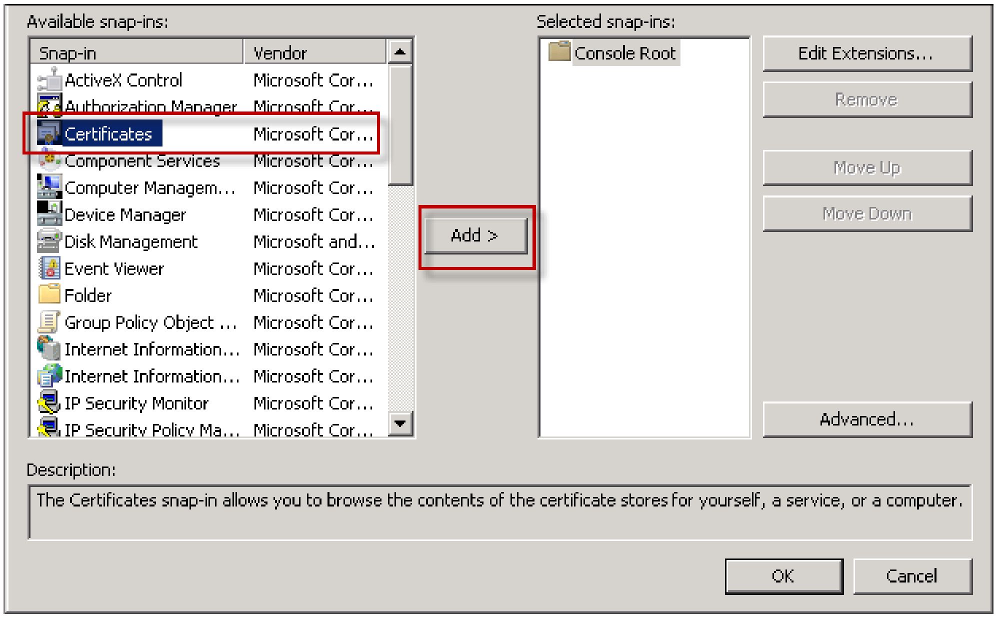
   The console opens.

4. Add the certificate snap-in.

   a. Click **File** and click **Add/Remove Snap-in...**



   b. Click **Certificates** and click **Add**.



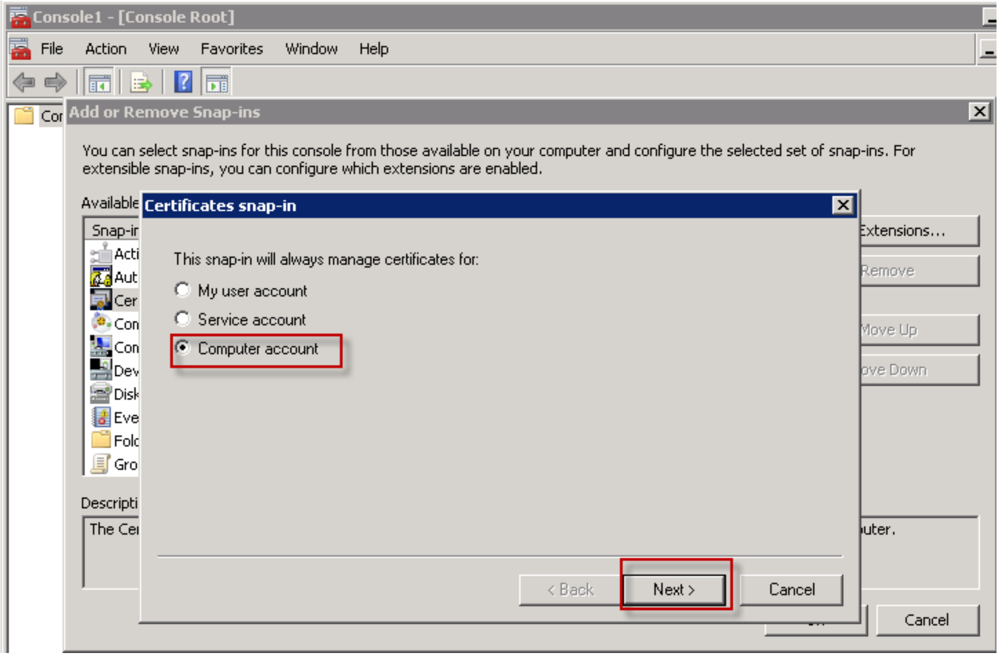
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Information...	Microsoft Cor...
Internet Information...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

   The Certificate snap-ins dialog opens.

   c. Select **Computer account** and click **Next**.



Console1 - [Console Root]

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Certificates snap-in

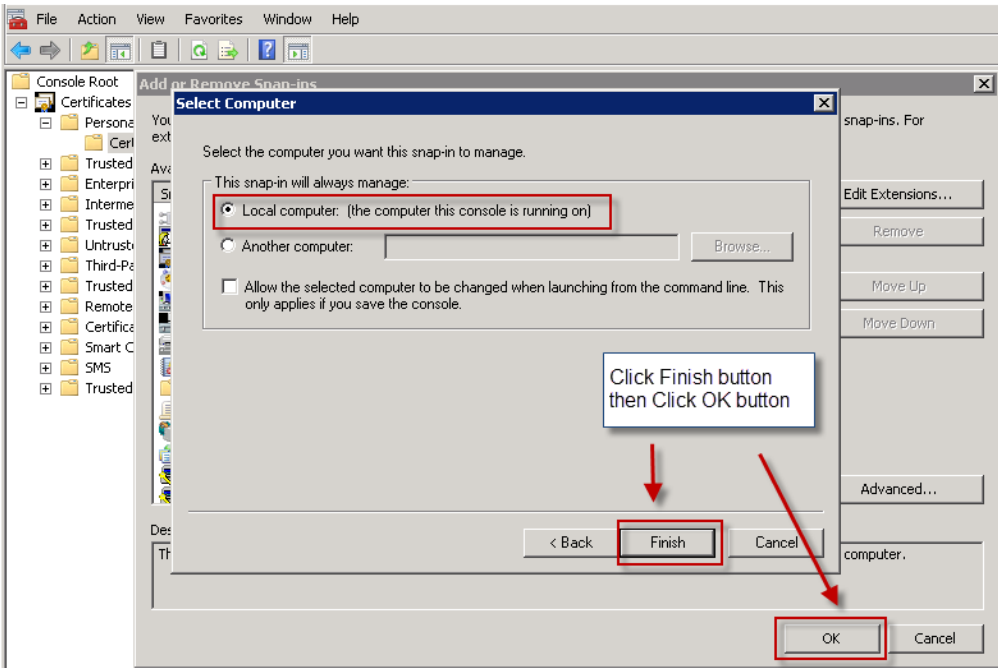
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

d. Select **Local Computer**.



Add or Remove Snap-ins

Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Click Finish button then Click OK button

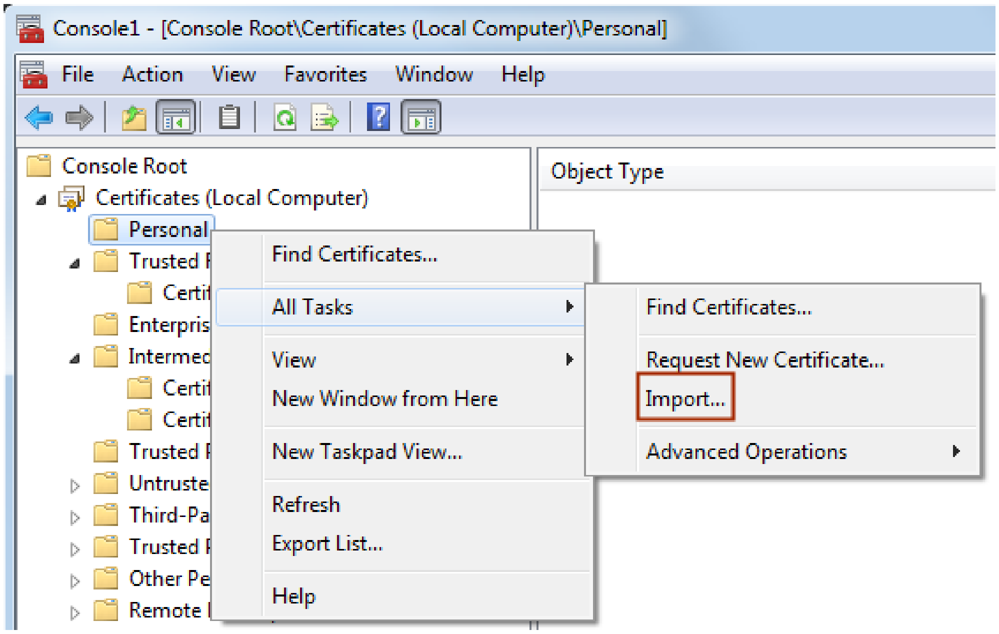
e. Click **Finish** and click **OK**.

5. Import the client certificate.

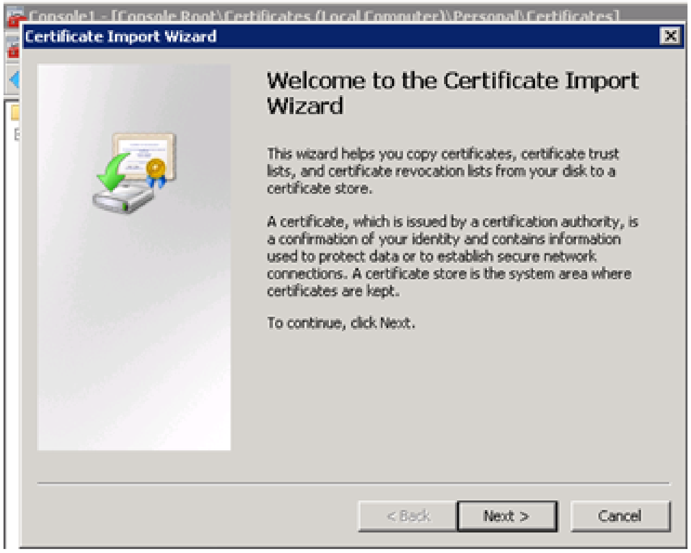
a. Copy the certificate file to the application server.

b. Open MMC and navigate to **Certificates > Personal**.

c. Right-click **Personal** and select **Import**.



d. Complete the import wizard.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
Certificate Import Wizard
< Back
Next >
Cancel

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

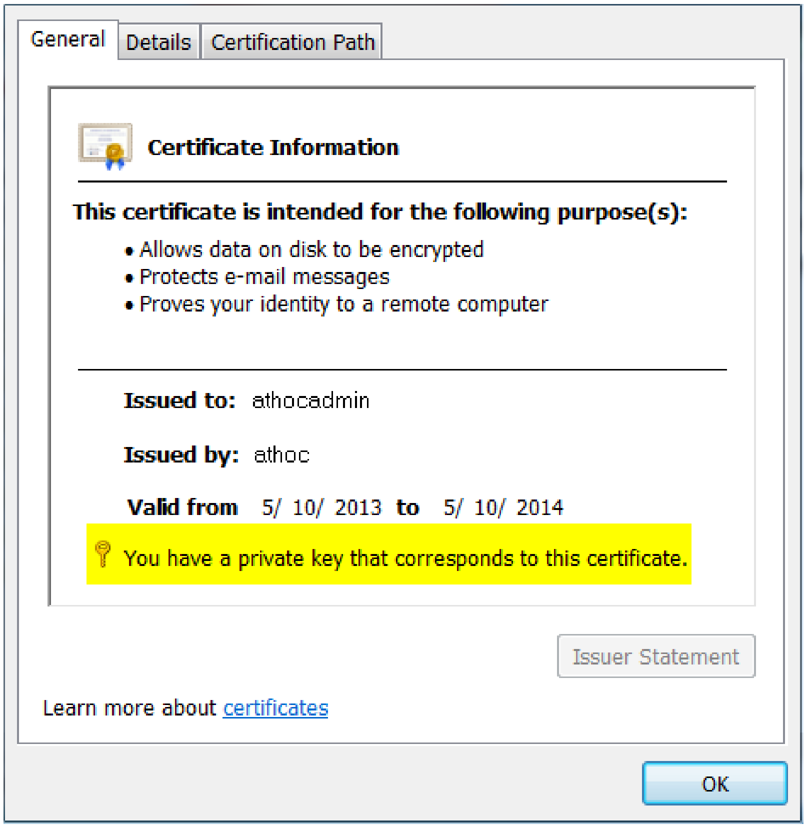
To continue, click Next.

Wizard notes

- The certificate that you import must be have a private key and be of the file type .PFX or .P12.
- Store the certificate in the Personal store.

6. Verify that the client certificate has a private key by opening the certificate.

   On the **General** tab, look for a note following the **Valid from** field.



Certificate Information

This certificate is intended for the following purpose(s):

- Allows data on disk to be encrypted
- Protects e-mail messages
- Proves your identity to a remote computer

Issued to: athocadmin

Issued by: athoc

Valid from 5/ 10/ 2013 to 5/ 10/ 2014

You have a private key that corresponds to this certificate.

7. Repeat this process for each application server.

When you configure the IWS Services application pool accounts, ensure that the account has access to the client certificate.

When you configure IIS, ensure that the web service has access to the client certificate.

(Optional) Set the SSL client certificate

In installations that require SSL client certificates on the application servers, such as CAC support, IIS folders must be set to **Require** client certificates instead of accepting client certificates.

Note: Indications that this setting has not been made include: desktop pop-ups display one or more security prompts; the Weather Alerting Module is not functional, and integration with external systems that use the AtHoc SDK APIs do not work.

The `csi` folder should be set to ignore certificates when using CAC, or users will be prompted to enter their ID every few minutes.

To set the preference for client certificates, complete the following steps:

1. Open the **Internet Information Services Manager**.
2. Expand Sites, then expand Default Web Site or the named site. Select a Web application and open SSL Settings.
3. Select the **Ignore**, **Accept**, or **Require** radio button under client certificates. Use the recommendations for each folder, provided in the table that follows these steps.
4. Click **Apply**.

The following table provides a reference for client certificate settings for Department of Defense, Federal Government, and any other customers that use smart cards or soft certificates for client authentication to web servers.

Application or virtual directory	SSL client certificates
Aspnet_client	Require
api	Require
ast	Require
athoc-cdn	Require
athoc-iws	Require
Cap Event Logging	Require
Cascade Alert Agent	Require
CatalogV3	Require
client[1]	Require
config[2]	Ignore if you have desktop clients deployed. Require if not.
corp	Require
csi[2]	Ignore if you have desktop clients deployed. Require if not.
D911Server	Require
Data	Require
DataExport	Require
Default Web Site	Require
EasyConnect	Require
EmailPublishing	Require
EmailResponse	Require
Enterprise Online Help	Require
EventQueueListening	Require
Graphics[2]	Ignore if you have desktop clients deployed. Require if not.
Gw	Require
AtHoc System	Require
Icons	Require
Images	Require
Include	Require
Integrated Weather Alerts[3]	Require
IWSAlertsHelpXBrowser	Require
monitor	Require

Application or virtual directory	SSL client certificates
Redirector	Require
sdk	Accept if you have desktop clients deployed. Require if not.
SelfService	Require
Self Service/AuthWin	Require
sps	Require
Sso	Require
Syndication	Require if your IIM devices have client certificates installed, or If no IIM devices are deployed. Ignore if not.
Toolbarremover	Require
TwitterConfig	Require
User	Require
WebHelp	Require
webhelppegasus	Require
webhelppegasus_Affiliate	Require
wis	Require

1. BlackBerry AtHoc health monitors do not currently support client certificate authentication. Setting the `client` Web directory to “Require Client Certificates” might cause the BlackBerry AtHoc Management System health monitor to falsely show that the system is down. BlackBerry AtHoc recommends disabling this monitor in this configuration.
2. If `config`, `csi`, and `Graphics` are set to “Require Client Certificates” and you have desktop clients deployed, one of two things can happen:
   - Users experience periodic prompts for client certificate pin authentication.

     OR
   - The SSL stack on the IIS web server becomes overwhelmed with SSL renegotiation issues. This condition looks like your Web server is under a denial of service attack, with page loads becoming slower and eventually timing out with errors.
3. Make sure the Symantec/Verisign certificate chain for the target system is properly represented in the Windows Certificate Manager.

(Optional) Install a MIR3 certificate

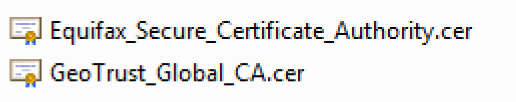
You might need to install a root certificate to access `mir3.com`.

If the root certificate is required, complete the following steps for each BlackBerry AtHoc application server:

1. Go to the following URL.:

   `https://www.geotrust.com/resources/root-certificates/index.html`

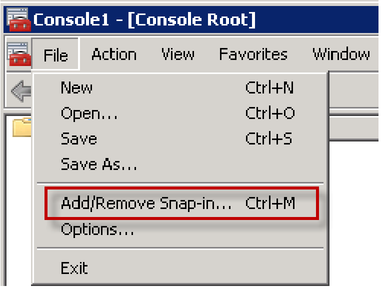
2. Locate and download the following certificate files to the application server and rename the extension to `.CER`:



Equifax_Secure_Certificate_Authority.cer
GeoTrust_Global_CA.cer

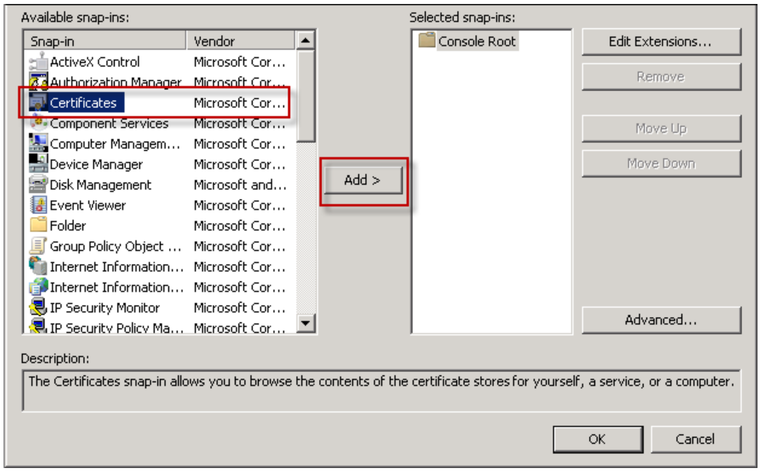
3. Open the Windows **Start** menu and in the search field, type `mmc.exe`.

   The Microsoft Management Center (MMC) opens.



4. Click **File > Add/Remove Snap-in**
5. Click **Certificates**, click **Add**.

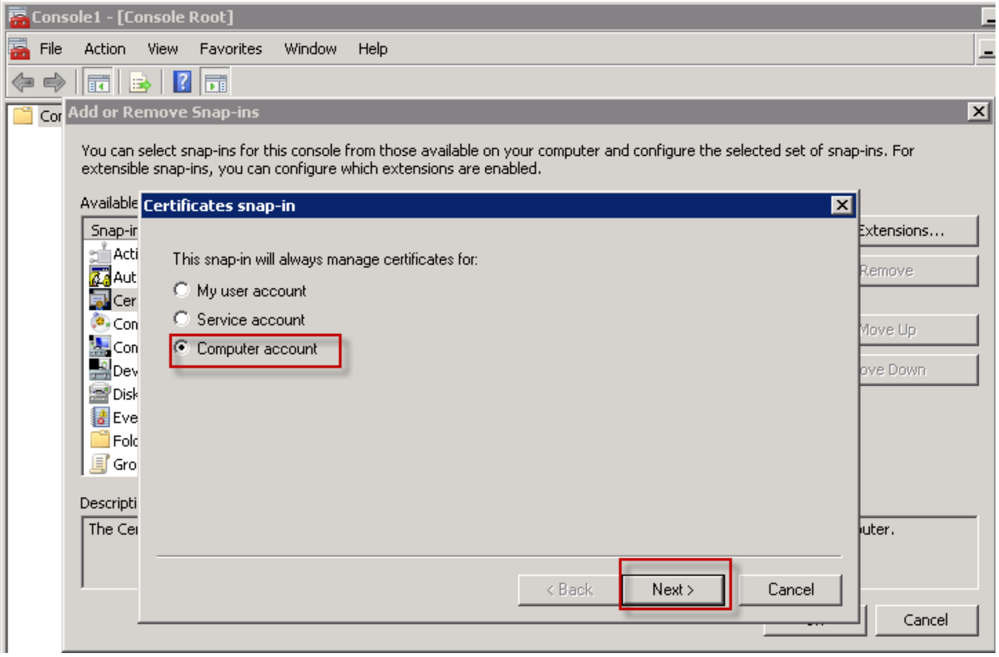
   The Certificate snap-ins dialog opens.



Available snap-ins:
Snap-in
Vendor
ActiveX Control Microsoft Cor...
Authorization Manager Microsoft Cor...
Certificates Microsoft Cor...
Component Services Microsoft Cor...
Computer Managem... Microsoft Cor...
Device Manager Microsoft Cor...
Disk Management Microsoft and...
Event Viewer Microsoft Cor...
Folder Microsoft Cor...
Group Policy Object ... Microsoft Cor...
Internet Information... Microsoft Cor...
Internet Information... Microsoft Cor...
IP Security Monitor Microsoft Cor...
IP Security Policy Ma... Microsoft Cor...
Add >
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
OK
Cancel

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

6. Select **Computer account** and click **Next**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

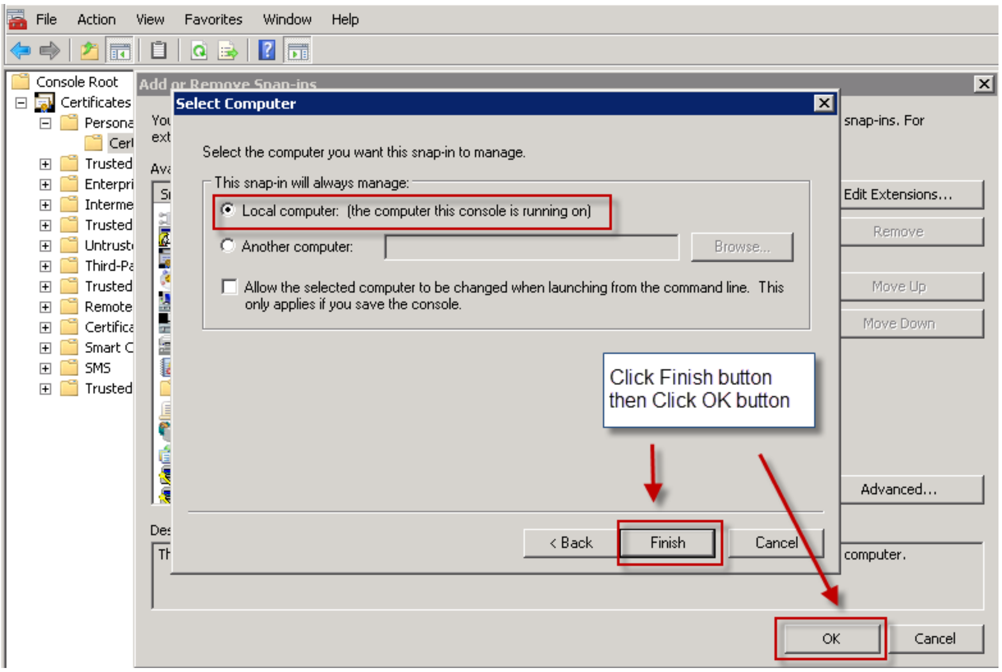
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

7. Select **Local Computer**.



Select the computer you want this snap-in to manage.

This snap-in will always manage:

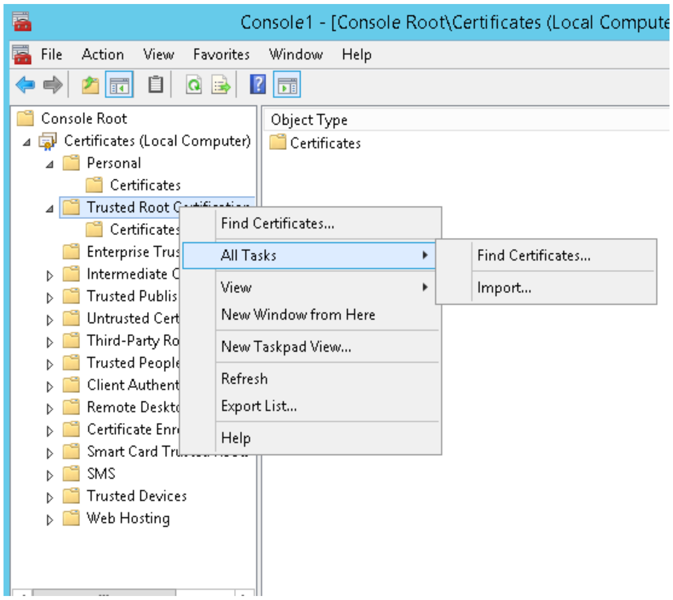
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

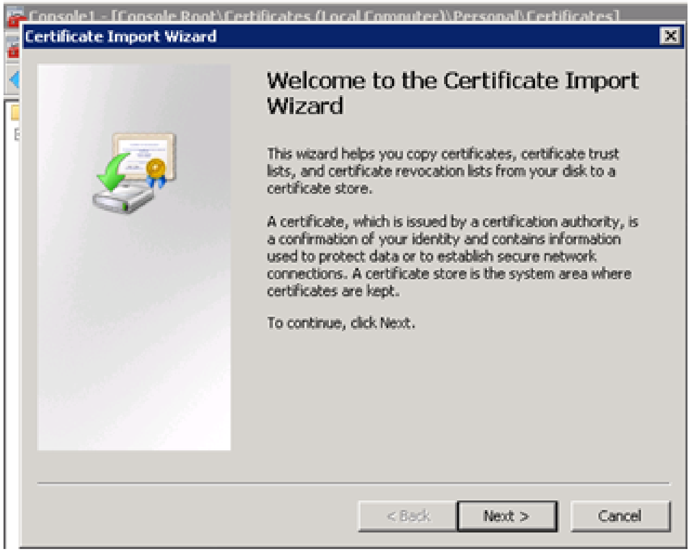
Click Finish button then Click OK button

8. Click **Finish** and click **OK**.
9. To import the certificate, copy the certificate file to the application server.
10. Open MMC and navigate to **Trusted Root Certificate Authorities** > **Certificates**



11. Right-click **Certificates** and click **All Tasks** > **Import**.

    The Certificate Import Wizard opens.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
Certificate Import Wizard
< Back
Next >
Cancel

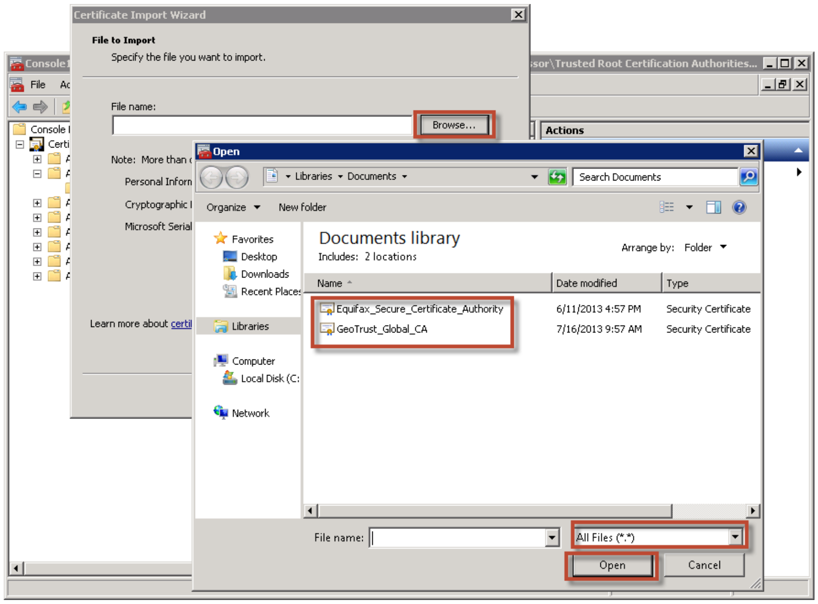
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

12. Click **Next** and click **Browse**.
13. Navigate to where you saved the certificates.



14. After the File name field, select **All Files (*.*)** in the File type list.
15. Select a certificate and click **Open**.
16. Click **Next** twice, and click **Finish**.
17. Restart IIS.

Set anti-virus file exclusions for database log and tempDB files

Anti-virus real-time scanning at the file level can occasionally cause abnormal system behavior, like high CPU utilization.

You should exclude the following items from real-time scanning:

- The `ffmpeg.exe` file
- The IIS Temporary Compressed Files folder located at:

  `%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files`

(Optional) Configure new access card formats for operator auto-login

BlackBerry AtHoc supports several types of log-in configurations. Operators can manually login using a username and password, a personal identification verification (PIV) card, or a Common Access Card (CAC) card.

The following list displays the high-level steps to configure operator authentication using CAC or PIV cards:

1. Gather information from the customer to determine what type of PIV or CAC card will be used by operators. If the card type is not supported, contact BlackBerry AtHoc Support.

2. Restart IIS.
3. Configure AtHoc security settings.

Gather information from the customer

If the organization using an access card requires a format not supported by BlackBerry AtHoc, you need to request support. Gather 5 to 10 samples of the customer client certificate strings and the variable name in the HTTP header from the organization that stores the certificate string. Provide AtHoc with the examples.

For example:

```
Subject: DC=edu, DC=athoc, O=internal, OU=people, OID.0.9.2342.19200300.100.1.1-
1=jsmith@athoc.com, CN=Jane Smith <mapping identifier>
```

```
Subject: DC=edu, DC=athoc, O=internal, OU=people, OID.0.9.2342.19200300.100.1.1-
1=jdoe@athoc.com, CN=John Doe <mapping identifier> (affiliate)
```

BlackBerry AtHoc creates a primary and an alternate regular expression (regex) that allows users to log in with their PIV or CAC cards. The expression extracts the MID from the certificate string. It then compares the MID with values in the database to determine the user identity and logs the user in, automatically.

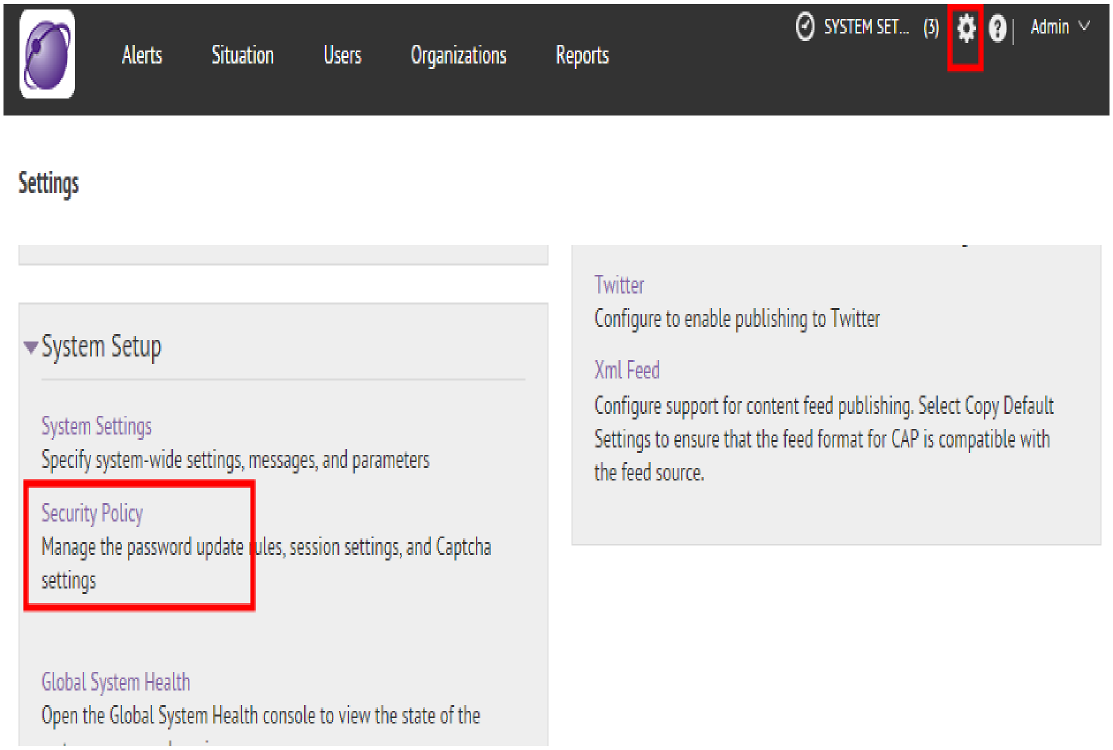
BlackBerry AtHoc provides an SQL UPDATE script to run. This script updates the GLB_CONFIG_TAB so that operators can log in with their access cards.

Update BlackBerry AtHoc management system security policy

To change the auto-login for the BlackBerry AtHoc Management system, update the Security Policy settings in Administration Setup screen.

> **Note:** You must be in the system setup organization (VPS 3) to make this setting.

1. Log in to the BlackBerry AtHoc Management System as an administrator.
2. Click the Gear icon, then click **Security Policy** in the System Setup section.



Settings

System Setup

System Settings
Specify system-wide settings, messages, and parameters

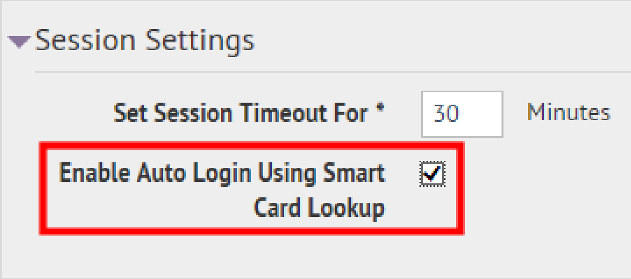
Security Policy
Manage the password update rules, session settings, and Captcha settings

Global System Health
Open the Global System Health console to view the state of the

Twitter
Configure to enable publishing to Twitter

Xml Feed
Configure support for content feed publishing. Select Copy Default Settings to ensure that the feed format for CAP is compatible with the feed source.

3. Select the CAC login option.



Session Settings

Set Session Timeout For * 30 Minutes

Enable Auto Login Using Smart Card Lookup ☑

4. Save your changes.
5. Log out and test by using a CAC or PIV card.

(Optional) Update the application server registry for smart card login

For smart card login, update the registry on the application server to enable users to select a CAC certificate.

To add a value to the SCHANNEL registry key, complete the following steps:

1. From the Windows Start menu, type `regedit`.
2. Navigate to the following node:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

3. Right-click the **SCHANNEL** node and click **New**.

4. Click **DWORD (32-bit) Value**.

   The new value is created.
5. Enter the name of the new value: `ClientAuthTrustMode`
6. You must enter the value when the name field becomes available for editing because you cannot change the name later.
7. Double-click on the new value and enter the following value in the field.

   Data: `2`
8. Click **OK** to save the values.

(Optional) Enable FIPS on each application server

Enable Federal Information Processing Standards (FIPS)

Note: FIPS requires an HTTPS environment

To enable FIPS, complete the following steps:

1. Set the following key to **1**:

   `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy`

   Note: If the key is set to 0, then FIPS is disabled.
2. Reboot the server to apply the change.

(Optional) Archive and MAS export service account requirements

Note: This task is required only for OnPrem 7.3 installations.

In order for the System Archive and MAS Export functions to work, the IWS Services application pool identities need a domain service account with **sysadmin** access on SQL Server. A viable alternative is the built-in Local System account, however, additional configuration on SQL is required.

Add all Application Servers' *domain\computer$* account as a new login to SQL Server and grant it the Server Role of sysadmin.

The backup folder path must also exist on the SQL server and the application pool identities must have write access to that folder. The backup folder path is defined in the System Setup VPS under System Settings.

If you use a client certificate for this server, ensure that the account has permission to access that client certificate. For more information, see Configure client certificates on the application server section of this guide.

To set up a service account for IWS Services applications pools, complete the following steps:

1. Stop the IWS Services (application pools) in IIS.
   - AtHoc Regular Scheduler Pool
   - AtHoc Alert Coordinator Pool

- AtHoc PSS Polling Agent Pool
- AtHoc Tracking Processor Pool
- AtHoc Delivery Coordinator Pool
- AtHoc Advanced Scheduler Pool
- AtHoc Tracking Summary Coordinator Pool
- AtHoc Batch Coordinator Pool
- AtHoc User Termination Coordinator Pool

2. For *each* application pool, complete the following steps:
   a. Select the application pool, and open **Advanced Settings**.
   b. Under Process Model, edit **Identity**.
   c. Choose **Custom Account** and enter a username and password.
   d. Restart the application pool.

Server proxy configuration

This section describes how to configure server proxy specification.

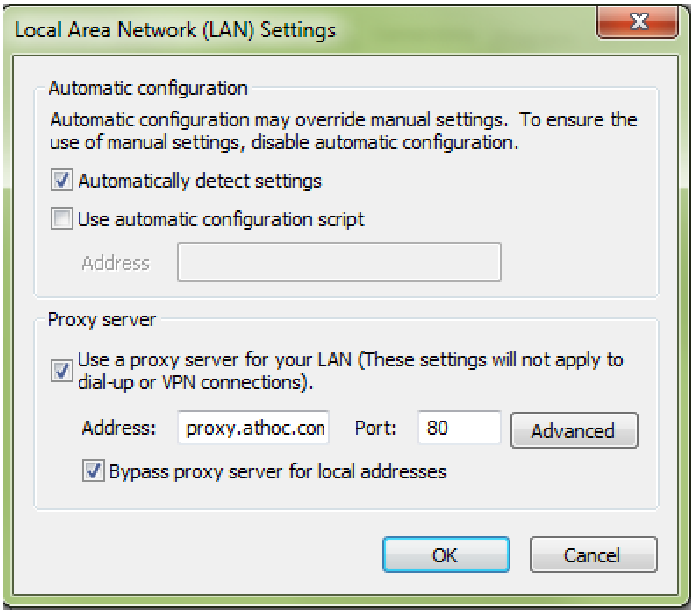
Note: This section is relevant only if you need to set a proxy for a server to access the external Web. If there is no such need, skip this section.

BlackBerry AtHoc uses the MSXML3 http component to make all of its HTTP calls. As these calls are made using the WinInet, a separate proxy configuration must exist for this component.

BlackBerry AtHoc installation does not support authenticating the proxy to perform HTTP calls to access external Web resources. If you have such a configuration, contact BlackBerry AtHoc.

To configure the server proxy, complete the following steps:

1. (Optional) If the proxy server is not configured for Internet Explorer, configure the proxy server:
   a. From Internet Explorer, open **Internet options**.
   b. Open the **Connections** tab and click **LAN Settings**.
   c. Select **Use a proxy server for your LAN**.
   d. Configure the proxy server based on your organization requirements.
   For example, you can specify an IP or URL address, port number, and specify whether or not to bypass the proxy server for local addresses.



Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: proxy.athoc.con Port: 80

☑ Bypass proxy server for local addresses

e. Click **OK** to save the LAN Settings, and click **OK** to close the Internet Options screens.

2. Open a Command Prompt with Administrator rights.
3. Navigate to the following directory:
   `C:\Windows\SysWow64\`
4. Type the following command:
   ```
   netsh winhttp show proxy
   ```
5. In the same folder in CMD, enter the following command to import the Proxy settings from Internet Explorer into the 32 bit WinHTTP module:
   ```
   netsh winhttp import proxy ie
   ```

IIS post-installation checklist

After installing BlackBerry AtHoc, verify the following settings in IIS.

Note: After upgrading to 7.3, you must manually start IIS.

Application pool configuration tables

The installation configures Application Pools using the settings described in the section. The configuration that you use depends on whether you use a Mass Alerting Service (MAS) laptop or server installations. Use *Standard* for MAS and *Enterprise* for all other installations. Additionally, the AtHocProcessor service has been replaced by the IWS Services website that uses the Net.Pipe protocol and Net.Pipe Listener Adapter service. The configurations of the application pools are described in the following tables:

- Table 1: Application Pool Configuration
- Table 2: Application Pool - Web Application Association for AtHoc Web site – Enterprise configuration
- Table 3: Application Pool - Web Application Association for AtHoc Web site – Standard configuration (for MAS)
- Table 4: Application Pool - IWS Services Configuration (formerly AtHocProcessor service)
- Table 5: Application Pool - Web Application Association for IWS Services Web site

Table 1: Application pool configuration

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc Web API v2 .NET core pool
General										
.NET Framework Version	No Managed code	v4.0	v4.0	v4.0	v4.0	v4.0	v4.0	v4.0	v4.0	v4.0
Enable 32-Bit Applications	True	True	True	False	True	True	True	True	True	True
Managed Pipeline Mode	Integrated	Classic	Classic	Integrated	Classic	Integrated	Classic	Classic	Classic	Integrated
Queue Length	65535	1000	65535	65535	65535	65535	65535	1000	65535	65535
Start Automatically	True	True	True	True	True	True	True	True	True	True

Table 1: Application pool configuration

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc Web API v2 .NET core pool
CPU										
Limit	0	0	0	0	0	0	0	0	30	0
Limit Action	NoAction	NoAction	NoAction	NoAction	NoAction	NoAction	NoAction	NoAction	Throttle	NoAction
Limit Interval (minutes)	5	5	5	5	5	5	5	5	5	5
Processor Affinity Enabled	False	False	False	False	False	False	False	False	False	False
Processor Affinity Mask	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295
Process Model										
Identity[1]	—	—	—	—	—	—	—	—	—	—
Idle Time-out (minutes)	0	0	0	0	0	0	0	0	0	0
Load User Profile	True	True	True	True	True	True	True	True	True	True
Maximum Worker Processes	1	1	1	2	2	1	1	1	2	1
Ping Enabled	True	True	True	True	True	True	True	True	True	True
Ping Maximum Response Time (seconds)	90	90	90	90	90	90	90	90	90	90
Ping Period (seconds)	30	30	30	30	30	30	30	30	30	30
Shutdown Time Limit (seconds)	90	90	90	90	90	90	90	90	90	90

Table 1: Application pool configuration

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc Web API v2 .NET core pool
Startup Time Limit (seconds)	90	90	90	90	90	90	90	90	90	90
Process Orphaning										
Enabled	False	False	False	False	False	False	False	False	False	False
Executable	—	—	—	—	—	—	—	—	—	—
Executable Parameters	—	—	—	—	—	—	—	—	—	—
Rapid-Fail Protection										
"Service Unavailable" Response Type	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel
Enabled	False	False	False	False	False	False	False	False	False	False
Failure Interval (minutes)	5	5	5	5	5	5	5	5	5	5
Max Failures	5	5	5	5	5	5	5	5	5	5
Shutdown Executable	—	—	—	—	—	—	—	—	—	—
Shutdown Executable Parameters	—	—	—	—	—	—	—	—	—	—
Recycling										
Disable Overlapped Recycle	False	False	False	False	False	False	False	False	False	False
Disable Recycling for Configuration Change	False	False	False	False	False	False	False	False	False	False

Table 1: Application pool configuration

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc Web API v2 .NET core pool
Generate Recycle Event Log Entry										
Application Pool Configuration Changed	False	False	False	False	False	False	False	False	False	False
Isapi Reported Unhealthy	False	False	False	False	False	False	False	False	False	False
Manual Recycle	False	False	False	False	False	False	False	False	False	False
Private Memory Limit Exceeded	True	True	True	True	True	True	True	True	True	True
Regular Time Interval	True	True	True	True	True	True	True	True	True	True
Request Limit Exceeded	False	False	False	False	False	False	False	False	False	False
Specific Time	False	False	False	False	False	False	False	False	False	False
Virtual Memory Limit Exceeded	True	True	True	True	True	True	True	True	True	True
Private Memory Limit (KB)	1800000	1800000	1800000	1800000	1800000	1800000	1800000	1800000	1800000	1800000
Regular Time Interval (minutes)	0	0	0	0	0	0	0	0	0	0
Request Limit	0	0	0	0	0	0	0	0	0	0
Specific Times										

Table 1: Application pool configuration

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc Web API v2 .NET core pool
[0]	01:38:00	01:33:00	01:32:00	01:34:00	01:34:00	01:36:00	01:33:00	01:35:00	01:33:00	01:38:00
Virtual Memory Limit (KB)	0	0	0	0	0	0	0	0	0	0

[1] ApplicationPoolIdentity

Table 2: Application Pool - Web Application associations for the IWS web site - enterprise configuration

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc Web API v2 .NET core pool
api										X
ast			X							
athoc-cdn						X				
athoc-iws						X				
AuthServers	X									
CascadeAlertAgent			X							
client							X			
config				X						
csi				X						
D911Server		X								
Data			X							
DataExport			X							

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc Web API v2 .NET core pool
EasyConnect			X							
EmailResponse									X	
Graphics			X							
Monitor			X							
Redirector			X							
sdk								X		
sps				X						
sso			X							
Syndication			X							
TwitterConfig			X							
wis					X					

Table 3: Application Pools - Web application association for IWS Web site - standard configuration for MAS

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc WebAPI v2 .NET core pool
ast			X							
athoc-cdn						X				
athoc-iws						X				
CapEventLogging			X							
CascadeAlertAgent			X							
client			X							

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool	AtHoc self service	AtHoc WebAPI v2 .NET core pool
config			X							
csi			X							
D911Server			X							
Data			X							
DataExport			X							
EasyConnect			X							
EmailResponse			X							
EventQueueListening			X							
Graphics			X							
Monitor			X							
Redirector			X							
sdk			X							
SelfService			X							
sps			X							
sso			X							
Syndication			X							
TwitterConfig			X							
wis			X							

Table 4: IWS Services application pool configuration

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination cooordinator pool
General									
.NET Framework Version	v4.6.1	v4.6.1	v4.6.1	v4.6.1	v4.6.1	v4.6.1	v4.6.1	v4.6.1	v4.6.1
Enable 32-Bit Applications	True	True	True	True	True	True	True	True	True
Managed Pipeline Mode	Integrated	Integrated	Integrated	Integrated	Integrated	Integrated	Integrated	Integrated	Integrated
Queue Length	1000	1000	1000	1000	1000	1000	1000	1000	1000
Start Automatically	True	True	True	True	True	True	True	True	True
CPU									
Limit	0	0	0	0	0	0	0	0	0
Limit Action	NoAction	NoAction	NoAction	NoAction	NoAction	NoAction	NoAction	NoAction	NoAction
Limit Interval (minutes)	5	5	5	5	5	5	5	5	5
Processor Affinity Enabled	False	False	False	False	False	False	False	False	False
Processor Affinity Mask	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295
Process Model									
Identity[1]	—	—	—	—	—	—	—	—	—
Idle Time-out (minutes)	0	0	0	0	0	0	0	0	0
Load User Profile	True	True	True	True	True	True	True	True	True

Table 4: IWS Services application pool configuration

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination cooordinator pool
Maximum Worker Processes	1	1	1	1	1	1	1	1	1
Ping Enabled	True	True	True	True	True	True	True	True	True
Ping Maximum Response Time (seconds)	90	90	90	90	90	90	90	90	90
Ping Period (seconds)	30	30	30	30	30	30	30	30	30
Shutdown Time Limit (seconds)	90	90	90	90	90	90	90	90	90
Startup Time Limit (seconds)	90	90	90	90	90	90	90	90	90
Process Orphaning									
Enabled	False	False	False	False	False	False	False	False	False
Executable	—	—	—	—	—	—	—	—	—
Executable Parameters	—	—	—	—	—	—	—	—	—
Rapid-Fail Protection									
"Service Unavailable" Response Type	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel
Enabled	False	False	False	False	False	False	False	False	False
Failure Interval (minutes)	5	5	5	5	5	5	5	5	5

Table 4: IWS Services application pool configuration

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination cooordinator pool
Max Failures	5	5	5	5	5	5	5	5	5
Shutdown Executable	—	—	—	—	—	—	—	—	—
Shutdown Executable Parameters	—	—	—	—	—	—	—	—	—
Recycling									
Disable Overlapped Recycle	True	True	True	True	True	True	True	True	True
Disable Recycling for Configuration Change	False	False	False	False	False	False	False	False	False
Generate recycle event log entry									
Application Pool Configuration Changed	False	False	False	False	False	False	False	False	False
Isapi Reported Unhealthy	False	False	False	False	False	False	False	False	False
Manual Recycle	False	False	False	False	False	False	False	False	False
Private Memory Limit Exceeded	True	True	True	True	True	True	True	True	True
Regular Time Interval	True	True	True	True	True	True	True	True	True
Request Limit Exceeded	False	False	False	False	False	False	False	False	False

Table 4: IWS Services application pool configuration

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination cooordinator pool
Specific Time	False	False	False	False	False	False	False	False	False
Virtual Memory Limit Exceeded	True	True	True	True	True	True	True	True	True
Private Memory Limit (KB)	800000	800000	800000	800000	800000	800000	800000	800000	800000
Regular Time Interval (minutes)	0	0	0	0	0	0	0	0	0
Request Limit	0	0	0	0	0	0	0	0	0
Specific Times									
[0]	04:30:00	04:30:00	04:30:00	04:30:00	04:30:00	04:30:00	04:30:00	04:30:00	04:30:00
Virtual Memory Limit (KB)	0	0	0	0	0	0	0	0	0

[1] ApplicationPoolIdentity

Table 5: Application pools - web application association for IWS services web site

	AtHoc PSS polling agent pool	AtHoc advanced scheduler pool	AtHoc regular scheduler pool	AtHoc tracking processor pool	AtHoc delivery coordinator pool	AtHoc Alert coordinator pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool
Advanced Scheduler		X						
Alert Coordinator						X		
Batch Coordinator								X
Delivery Coordinator					X			
PSS Polling Agent	X							

	AtHoc PSS polling agent pool	AtHoc advanced scheduler pool	AtHoc regular scheduler pool	AtHoc tracking processor pool	AtHoc delivery coordinator pool	AtHoc Alert coordinator pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool
Regular Scheduler			X					
Tracking Processor				X				
Tracking Summary Coordinator							X	

IIS handler mappings

The following handler mappings are required:

Handler name	Path	Description
asp.net	*	AtHoc Wildcard Script Map
ASPClassic	*.asp	Handler for classic ASP
AXD-ISAPI-4.0_32bit	*.axd	web site administration requests handler
cshtml-ISAPI-4.0_32bit	*.cshtml	Required by MVC
HttpRemotingHandlerFactory-rem-ISAPI-4.0_32bit	*.rem	Web service handler
HttpRemotingHandlerFactory-soap-ISAPI-4.0_32bit	*.soap	Web service handler
MvcScriptMap	*.mvc	Required by MVC
OPTIONSVerbHandler	*	URL-less page handler
PageHandlerFactory-ISAPI-2.0	*.aspx	ASP.NET v.2 page handler
PageHandlerFactory-ISAPI-4.0_32bit	*.aspx	ASP.NET v.4 page handler
SecurityCertificate	*.cer	processes SSL certificates
SimpleHandlerFactory-ISAPI-2.0	*.ashx	Generic Web handler.
SimpleHandlerFactory-ISAPI-4.0_32bit	*.ashx	Generic Web handler.
svc-ISAPI-4.0_32bit	*.svc	Web service handler
TRACEVerbHandler	*	URL-less page handler
WebServiceHandlerFactory-ISAPI-2.0	*.asmx	Web service handler
WebServiceHandlerFactory-ISAPI-4.0_32bit	*.asmx	Web service handler
StaticFile	*	URL-less page handler

Verification checklist

Use the following check list to ensure that all of the following items exist and are configured as described:

√	Item	Description
	ISAPI and CGI Extensions	• **IIS 7**: ISAPI and CGI Restrictions should have Active Server Pages and ASP.NET v4.0 (32-bit) in the Allowed category.
	Default web site	Ensure the default web site points to the `<AtHocENS\wwwroot>` folder.
	Virtual directories	The AtHoc website must contain the following virtual directories: • Data—Points to <`AtHocENS>\CommonSiteData\AtHocData` • Graphics—Points to `&lt;AtHocENS&gt;\CommonSiteData\Graphics`
	Web applications	The AtHoc website must contain the following Web applications: CapEventLogging CascadeAlertAgent client config csi DataExport EasyConnect EmailPublishing EmailResponse EventQueueListening Redirector sdk SelfService Sps sso Syndication TwitterConfig WeatherModule Wis
	ASP.NET version	All Web applications must point to the ASP.Net 4.0 version. **IIS 7**: this is set in the Basic or Advanced settings of each Application Pool.
	Application pools	The following Application Pools are created during the application server installation and must be present: • **AtHoc Default Pool** • **AtHoc Desktop Pool** • **AtHoc Management System Pool** • **AtHoc SDK Pool** • **AtHoc Self Service**

√	Item	Description
	Integrated Weather Alerts	Verify that the internal routing from the application server to the domain name is functioning correctly over HTTP.
	MIME Types	Verify that the following MIME types exist: • .mp4, video/mp4 • .webm, video/webm • .woff, application/x-wor
	Web.config files	—
	IWS services	This web site appears offline because it uses the net.pipe binding with no HTTP or HTTPS binding.
	Default web site	Ensure the AtHoc Web site points to the `<AtHocENS\wwwroot>` folder.
	Response headers	There are six response headers for Default Web Site: • Content-Security-Policy, Value: default-src https: data: 'unsafe-inline' 'unsafe-eval' • Strict-Transport-Security, Value: max-age=31536000; includeSubDomains; Preload • X-Content-Type-Options, Value: nosniff • X-Xss-Protection, Value: 1;mode=block • X-Frame-Options, Value: SAMEORIGIN • X-Powered-By, Value: AtHoc Inc.

Configure role-based permissions for the AtHoc Mobile App

After you install or upgrade AtHoc, you must configure access to advanced mobile features.

Starting with Release 6.1.8.85 R3 SP4, you configure role-based permissions for the AtHoc mobile application for all features except receiving alerts. Role-based permissions use a distribution list to enable or disable advanced features for a set of users. With this feature, organizations can determine who gets access to the advanced features, at a more granular level.

For example, you can create a distribution list of users that can send Emergency (Duress) or Field Reports, or that can check in or be tracked on the map.

Prerequisite: AtHoc mobile application Version 2.4

When using the AtHoc Mobile App version 2.4 or later

To ensure that all mobile users have the correct permissions, complete the following steps:

1. Log on to the AtHoc Application Server as a system administrator.
2. Enable the AtHoc Mobile App device on the AtHoc Application Server; for more information see Enable delivery gateways section of this guide.
3. Log in to the AtHoc Management System as an administrator.

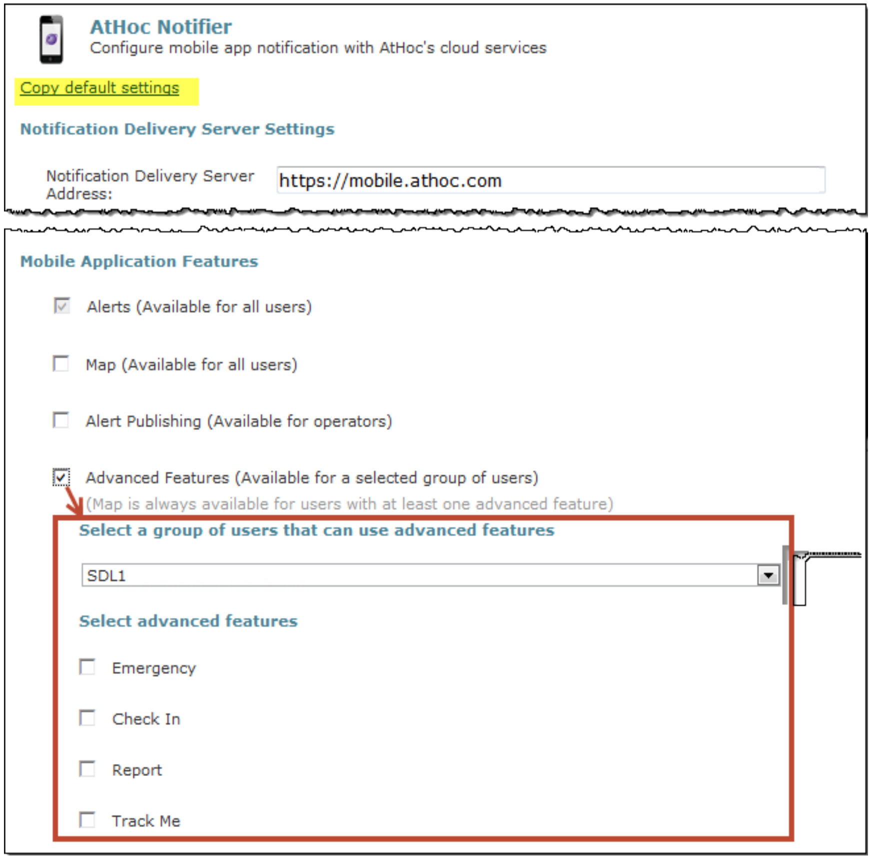
4. Create a distribution list for a group of users that need to have advanced features. For example, you might create a distribution list for users that can send field reports.

   To learn how to create a distribution list, see *AtHoc Administration Guide*.

5. Navigate to **Administration > Setup** and click **Mobile App Gateway** (formerly AtHoc Mobile Notifier Gateway).

   The gateway settings open.

6. Select the **Copy default settings** link, and provide the delivery server settings, username, and password.



AtHoc Notifier
Configure mobile app notification with AtHoc's cloud services

Copy default settings

Notification Delivery Server Settings

Notification Delivery Server Address: https://mobile.athoc.com

Mobile Application Features

☑ Alerts (Available for all users)

□ Map (Available for all users)

□ Alert Publishing (Available for operators)

☑ Advanced Features (Available for a selected group of users)
(Map is always available for users with at least one advanced feature)

Select a group of users that can use advanced features

SDL1

Select advanced features

□ Emergency

□ Check In

□ Report

□ Track Me

7. For Mobile App users with Version 2.4 or later, select **Map** to provide Map access when SSA is available on the system.

8. Select **Alert Publishing** to allow operators to publish alerts from the mobile application.

9. Select **Advanced Features** to provide additional features, such as reporting, emergency alerting, and user tracking.

   The advanced features expand.

10. Select a group (distribution list) for users that a need one or more advanced features.

11. Select the advanced features that the users need, such as Emergency or Report.
12. Select any other choices that you need and save your changes.
13. To verify the changes, by checking a mobile device for users in the distribution list.

(Optional) Restore the XML files for duplicated devices

If you backed up duplicated device XML files, restore the XML files to the following directories from the temporary directory:

```
\AtHocENS\ServerObjects\utils\AddOnModules\Packages
```

```
\AtHocENS\ServerObjects\utils\AddOnModules\IIM\Enable
```

(Optional) Migrate the CAP Feed Poller agent

Note: This task is required only for OnPrem 7.3 installations.

Perform the following steps to migrate the CAP Events Poller agent from the system VPS (VPS3) to a private VPS (VPS1):

1. Disable existing CAP Feed Poller agents:

   ```
   update dbo.SCD_SCHEDULE_TAB set IS_DISABLED='Y' where name like 'CAP Feed Poller%'
   ```

2. Extract the Metastore XML from existing CAP Feed Poller agents:

   ```
   select provider_id, agent_name, agent_common_name, convert(xml, meta_store) meta_store from prv_agent_
   tab where agent_common_name like 'CapFeedPoller%'
   ```

3. Only one entry should be returned. If more than one entry is returned, make sure to save only the Metastore XML from the CAP Feed Poller. For additional help, contact your AtHoc support team.
4. Create a new CAP Feed Poller agent and place it on VPS1:

   ```
   exec [dbo].[ENABLE_DISABLE_CAP_POLLING_AGENT] @enable = 1
   ```

5. Find the CAP Feed Poller entry in Integration Manager on VPS1 and paste the Metastore XML extracted in Step 2 in the Metastore field.
6. Delete the old CAP Feed Poller agents:

   ```
   delete from dbo.SCD_Schedule_TAB where name like 'CAP Feed Poller%' and name <> 'Cap feed poller - 1'
   ```

   ```
   delete from dbo.PRV_AGENT_TAB where provider_id <> 1 and agent_common_name like 'CapFeedPoller%'
   ```

7. Test the new CAP Feed Poller agent by checking the following:
   a. The CAP Feed Poller agent appears in VPS1
   b. The CAP Feed Poller agent is removed from the VPS on which it was originally installed
   c. The CAP Feed Poller is enabled and running in the system jobs for VPS3

8. In BlackBerry AtHoc for VPS3, navigate to **Settings** > **System Setup** > **System Jobs**. If the CAP Feed Poller is disabled, enable it and check that the History log is updating.

(Optional) Migrate the CAP Event Processor agent

Note: This task is required only for OnPrem 7.3 installations.

Perform the following steps to move an existing CAP Event Processor agent from the system VPS (VPS3) to a private VPS (VPS1):

1. Disable the existing CAP Event Processor agent:

   ```
    update dbo.SCD_SCHEDULE_TAB set IS_DISABLED='Y'where name like 'Cap Event Processor%'
   ```

2. Create a new CAP Event Processor agent and place it on Organization 1:

   ```
   exec [dbo].[ENABLE_DISABLE_CAP_EVENT_PROCESSOR] @enable = 1
   ```

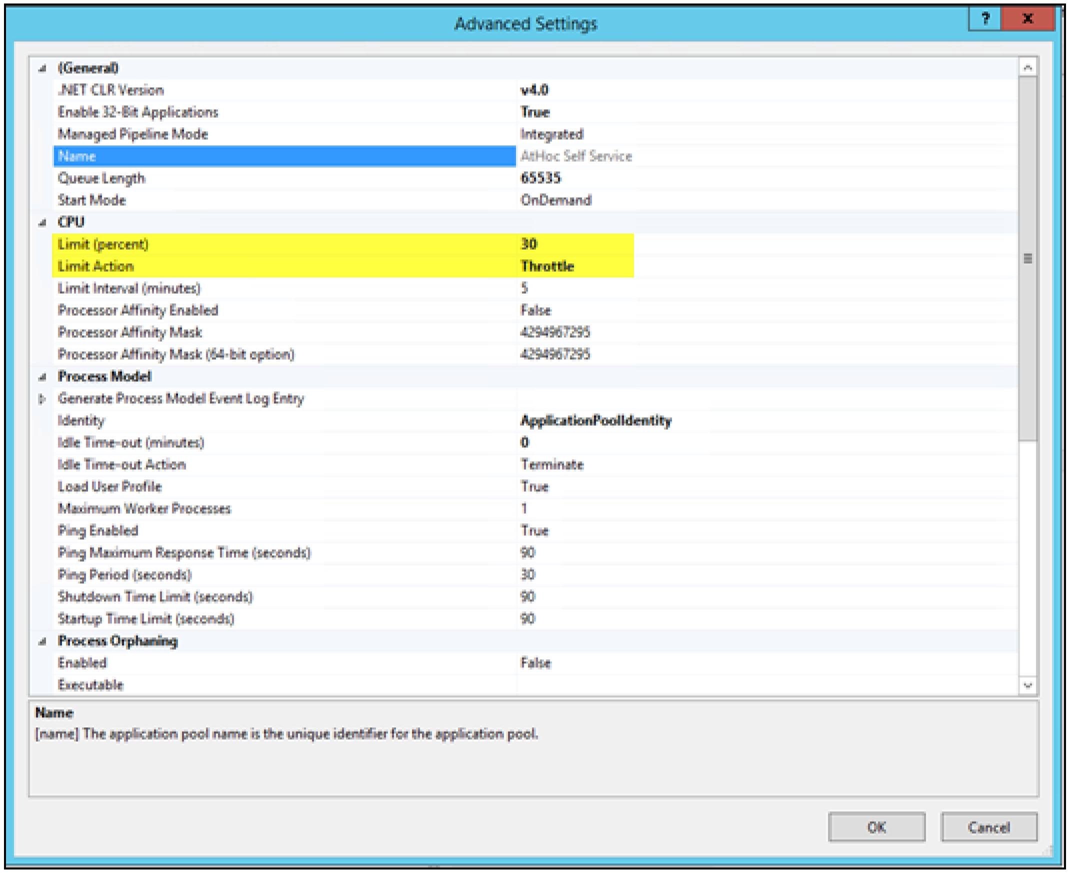
3. Test the new agent.
4. Test the new CAP Event Processor agent by checking the following:
   a. The CAP Event Processor agent appears in VPS1
   b. The CAP Event Processor agent is removed from the VPS on which it was originally installed
   c. The CAP Event Processor is enabled and running in the system jobs for VPS3
5. Delete the old CAP Event Processor agent:

   ```
   update dbo.SCD_SCHEDULE_TAB set IS_DISABLED = 'N' where name like 'Cap Event Processor%'
   delete from dbo.PRV_AGENT_TAB where provider_id <> 1 and agent_common_name like 'CapEventProcessor%'
   ```

(Optional) Set up error pages for Self Service throttling

Self Service is implemented as a separate application which runs in its own application pool. In a production environment, the Self Service application shares CPU resources with other applications like the Operator management system. To ensure that alerting is not negatively affected by the Self Service application during heavy loads to the Self Service application, the AtHoc Self Service application pool that Self Service runs under will be throttled so that it uses only 30% of the available CPU at any time. This ensures that BlackBerry AtHoc alerts can always be published, even during heavy loads to Self Service. One impact of this change is that during heavy loads in Self Service, you might encounter some slowness in the Self Service application.

Starting with release 6.1.8.90, the throttling changes are applied automatically by the installer during new installation and upgrade. On the Advanced Settings screen for AtHoc Self Service in IIS, shown below, notice that under the CPU section the value for **Limit (percent)** has been changed to `30` and the value for **Limit Action** has been changed to `Throttle`.



(General)	
.NET CLR Version	v4.0
Enable 32-Bit Applications	True
Managed Pipeline Mode	Integrated
Name	AtHoc Self Service
Queue Length	65535
Start Mode	OnDemand
CPU	
Limit (percent)	30
Limit Action	Throttle
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit option)	4294967295
Process Model	
Generate Process Model Event Log Entry	
Identity	ApplicationPoolIdentity
Idle Time-out (minutes)	0
Idle Time-out Action	Terminate
Load User Profile	True
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconds)	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90
Process Orphaning	
Enabled	False
Executable	

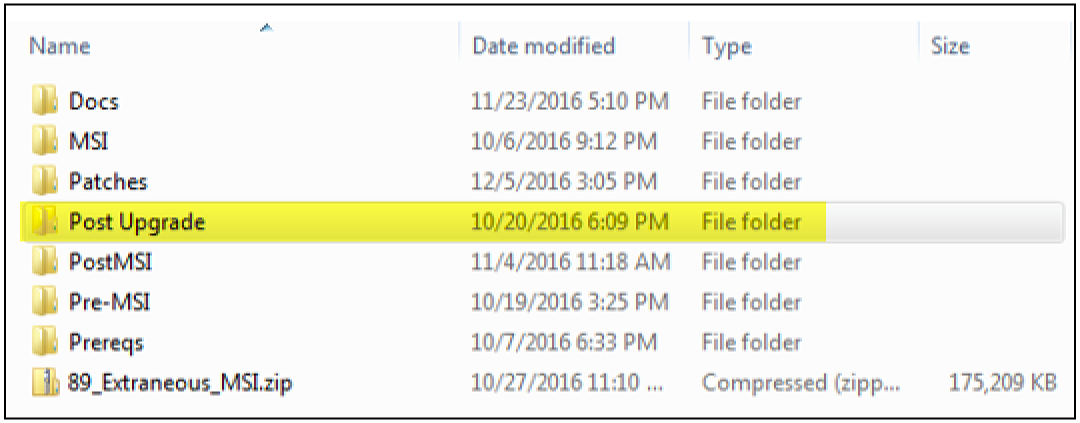
Name

[name] The application pool name is the unique identifier for the application pool.

External error pages for Self Service throttling

When the AtHoc Self Service application is throttled to use only 30% of CPU, it is likely that IIS will display errors with a status code of “503” or “500” when the system is under heavy load and unable to handle requests. If these errors occur, IIS displays a default error page that does not contain a lot of useful information for users.

These errors are usually not customizable at the IIS level on the same server, as documented by Microsoft. BlackBerry AtHoc provides friendly messages in static pages that can be used in place of the default error pages, provided that the BlackBerry AtHoc System is deployed behind a proxy server or load balancer that supports error message customization. The Systems Administrators can configure these load balancers or proxy servers to trap these errors and redirect to the friendlier messages instead. The error pages are available in the **Post Upgrade** folder as a separate sub-folder named **errorpages**.



Name	Date modified	Type	Size
Docs	11/23/2016 5:10 PM	File folder	
MSI	10/6/2016 9:12 PM	File folder	
Patches	12/5/2016 3:05 PM	File folder	
Post Upgrade	10/20/2016 6:09 PM	File folder	
PostMSI	11/4/2016 11:18 AM	File folder	
Pre-MSI	10/19/2016 3:25 PM	File folder	
Prereqs	10/7/2016 6:33 PM	File folder	
89_Extraneous_MSI.zip	10/27/2016 11:10 ...	Compressed (zipp...	175,209 KB

System administrators can take the **errorpages** folder and host it on any web server that is capable of serving HTML, CSS, and Javascript pages.

Note: Usually, the server where you host your error pages is different than the IWS Server where you are running the IWS applications.

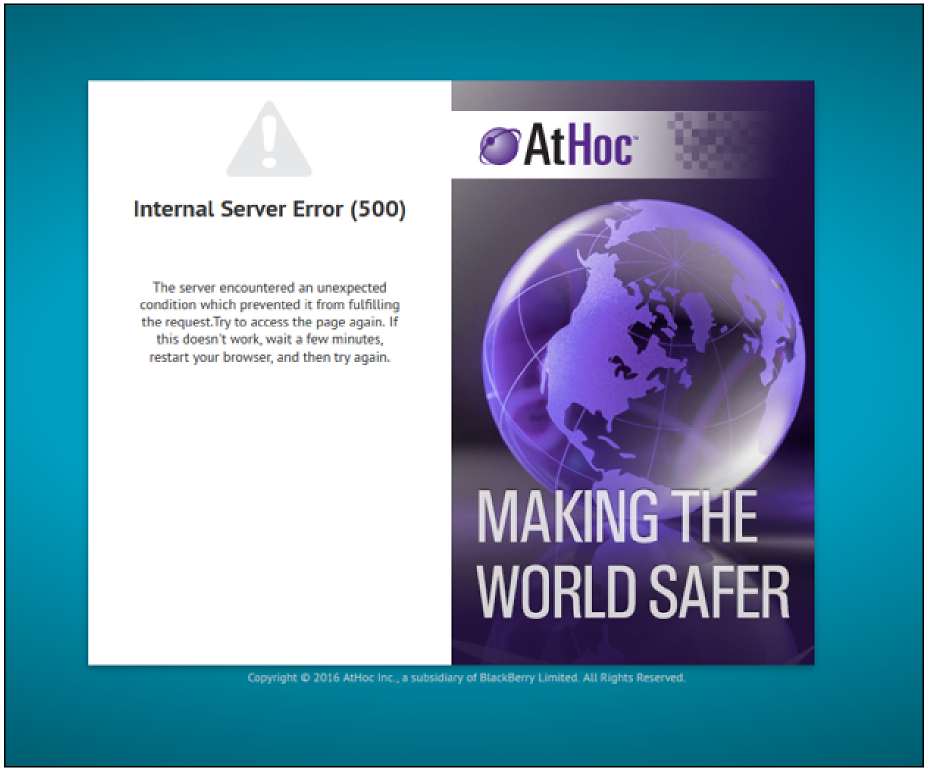
To host the folder, Administrators copy the folder and make it publicly available from their web server. For example, if the System Administrator hosted these pages directly under the root folder of the web server, the error pages can then be accessed using the following URL, where `<domainnameofserver>` refers to the actual domain name of the server:

Error page	Error page URL	Message
500 – Internal Server Error	https://<domainnameofserver>/errorpages/index.html?code=500	The server encountered an unexpected condition which prevented it from fulfilling the request. Try to access the page again. If this doesn't work, wait a few minutes, restart your browser, and then try again.
503 – Service Unavailable	https://<domainnameofserver>/errorpages/index.html?code=503	The server is unable to load the page you are requesting. This could be because increased traffic is overwhelming the server. Wait a few minutes and then try again.

After these pages are hosted on a different server than the IWS Server, the System Administrator can configure the individual proxy server or load balancers to redirect to the static hosted pages based on the error that IIS returns to the client.

Note: Because the configuration process varies depending on the type of load balancer or proxy server being used, the configuration process is not documented here.

A sample friendly error page is shown below.



Internal Server Error (500)

The server encountered an unexpected condition which prevented it from fulfilling the request.Try to access the page again. If this doesn't work, wait a few minutes, restart your browser, and then try again.

Copyright © 2016 AtHoc Inc., a subsidiary of BlackBerry Limited. All Rights Reserved.

(Optional) Enable the Inbound Event Manager for IPAWS

Note: For IPAWS only

After you finish the installation or the upgrade of the database server, enable the Inbound Event Manager (IEM) for IPAWS.

To enable IEM, complete the following steps:

1. Deploy the database script files:
   a. Open SQL Server Management Studio and connect to the database server.
   b. Log in as “sa” (or “ngad”).
   c. From the Query window, open `Enable_IEM.sql`.
   d. **Click Execute** from the Query window
2. Restart IIS and the AtHoc Services.

Update alert templates with locations

If you have an alert template that was created in release 6.1.8.91 or earlier release, and contains custom or predefined locations, you must update these templates after you upgrade to release 7.3.

Update alert templates with custom locations

To update an alert template that contains custom locations, complete the following steps:

1. Log in to the BlackBerry AtHoc management console.
2. In the navigation bar, click **Alerts** > **Alert Templates**.
3. Open the alert template you want to update.
4. In the **Content** section, click the **Edit Location** (✎) icon. The interactive map opens.
5. Expand the **Location Summary** field.
6. Verify that only custom locations are present. If predefined locations are also present in the map, click **Cancel** and perform the steps in the **Update alert templates with predefined locations** section instead.
7. If only custom locations are present, click **Apply**. You are returned to the Alert Template screen.
8. Click **Save**.

Update alert templates with predefined locations

To update an alert template that contains predefined locations, or a combination of custom and predefined locations, complete the following steps:

1. Log in to the BlackBerry AtHoc management console.
2. In the navigation bar, click **Alerts** > **Alert Templates**.
3. Open the alert template you want to update.
4. In the Content section, click the **Edit Location** (✎) icon. The interactive map opens.
5. Expand the **Location Summary** field.
6. Verify that at least one predefined location is present.
7. If any custom locations are also present, you can still proceed with the steps in this task.
8. Take note of all predefined locations present in the map.
9. In the Location Summary menu, click the **X** button next to each predefined location to remove it.
10. If any custom locations are also present, do not remove them.

11. Expand the **Select Predefined Locations** menu.
12. Select the predefined locations that you noted in Step 7.
13. In the Select By Location menu, click **Calculate**.
14. Click **Apply**. You are returned to the Alert Template screen.
15. Click **Save**.

Uninstall ImageMagick

After you finish the upgrade from BlackBerry AtHoc release 7.0.0.2 to 7.3, you must manually uninstall ImageMagick from your application server.

To uninstall ImageMagick, complete the following steps:

1. On the application server, go to the Control Panel.
2. In the Control Panel, select **Programs** > **Programs and Features** > **Uninstall a program**.
3. Select **ImageMagick-7.0.2-Q6**.
4. Rick-click and select **Uninstall**. A confirmation window opens.
5. Click **Yes** to start the uninstallation. When the uninstallation is complete, a confirmation window opens.
6. Click **OK**.
7. Check your Program Files folder to verify that the ImageMagick folder no longer appears.

Chapter 7: Advanced server configuration

Migrate a pre-installed server

In some cases, BlackBerry AtHoc provides a customer with a pre-installed server. In other cases, there is a need to move an installed server to another domain.

Stop services

Stop IIS.

Database changes

Update the following fields in the `SYSTEM_PARAMS_TAB` table in the NGADDATA database:

– `ENVIRONMENT_URL` - update to URL using "https" if adding SSL support

– `SYSTEM_TIME_ZONE`

Application server changes

1. Uninstall and re-install MSMQ.
2. Update the connection string in the registry of all application servers.
3. Update the `<Server=Server Name>` parameter in the following keys:
    - `HKEY_LOCAL_MACHINE\Software\AtHocServer\OleDbConnectionString`

Start IIS

To perform management system changes, under the **Administration >Parameters >Configuration Options** tab, update the following:

- Time zone
- Homepage URL

Migrate to an enterprise hierarchy

After you upgrade to this release, you can migrate to an BlackBerry AtHoc enterprise. The enterprise provides system-wide alerting and content management for all organizations on your system.

During the upgrade, standard out-of-the-box attributes and alert folders are migrated to System Setup (3) from all other organizations and are now inherited by all other organizations from System Setup. Following the upgrade, run the Enterprise Migrator tool to organize the hierarchy structure and promote user attributes and alert folders.

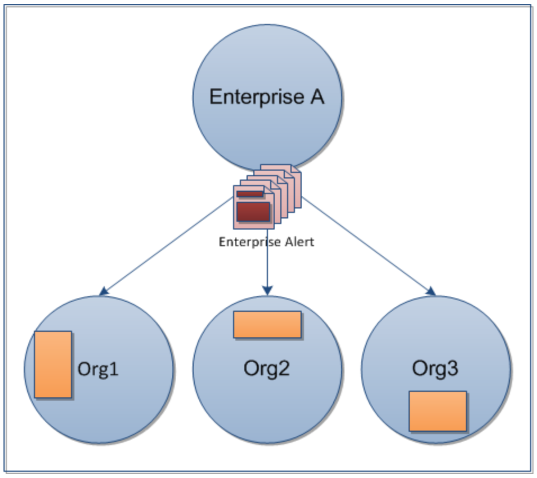
Plan the enterprise hierarchy

Important: Plan your hierarchy prior to using the tool. After you save your changes you CANNOT change the hierarchy.

The Enterprise Migrator tool displays the organizations currently in your BlackBerry AtHoc system. By default, new organizations that are created in the system are listed under the System Setup node. These are standalone Enterprise organizations. They can be used as either an Enterprise organization or moved under an Enterprise to become a sub-organization.

In an AtHoc Enterprise, there are three levels:

- The top level is System Setup. The System Administrator role manages the system by logging into the System Setup organization. User attributes and alert folders can be created here, which all organizations in the system inherit.
- The next level is Enterprise. There can be multiple enterprise organizations associated with System Setup. The enterprise administrator manages the enterprise organization and sub-organizations. The administrator can create enterprise-level attributes and folders for the enterprise organization that is inherited by its children.



- The third level is sub organization (or member organization). Each Enterprise organization can have a unlimited number of sub-organizations. The organization administrator manages the local organization only. The administrator can create organization-level attributes and folders for the local organization. A sub-organization has peers, but no children.

Using the migration tool, you will choose one organization that acts as the Enterprise organization, and the rest that are members (sub organization). System Setup is the default and top-level organization. An enterprise organization inherits from System Setup and a sub-organization inherits from the enterprise organization.

- Typically, content is managed at the Enterprise level because it provides one place to control the content and send alerts to all users in sub organizations. The sub organization level contains content specific to a subset of the Enterprise, customized for a particular organization.
- The Enterprise Migrator tool migrates existing operators that have an Enterprise Administrator role in a sub-organization to Organization Administrator. Other operator permissions remain unchanged.
- When you move an organization into the Enterprise, the connect relationships and user accounts remain unchanged for the organization.

Important: Enterprise hierarchy uses inheritance for user attributes and alert folders. Content created at the system level can be seen by Enterprise and sub-organizations, but not edited. Content created at the sub organization level cannot be seen at the Enterprise or system levels.

Best practices

- Rename user attributes with the name “Organization”. BlackBerry BlackBerry AtHoc provides an Enterprise user attribute with this name.
- Plan the promotion of attributes and alert folders:
  - Using Enterprise attributes and alert folders is a good way to enforce consistency.
  - If more than one organization uses the same user attribute, the attribute should be promoted to the Enterprise level.
  - If organizations use different values for the same user attribute, all values are promoted to the Enterprise level.
  - Think about situations in which you need to alert the entire Enterprise. What attributes do you need to target all users in an alert?. These attributes should be promoted to the Enterprise level.
  - Attributes that are for only one sub-organizations should stay at the sub-organization level.
- Create end users and operators for sub-organizations at the sub-organization level, not the Enterprise level.
- You can see all users from sub-organizations from the Enterprise organization so there is no reason to create any users at this level aside from Enterprise operators (operators that need to send alerts more than one sub-organization).
- Create a new Enterprise organization rather than reuse a headquarters organization if there are existing users. Move the headquarters organization under the Enterprise level.

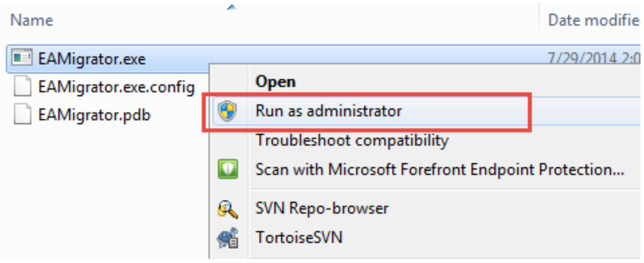
Run the Enterprise Migrator

The Enterprise Migrator tool is provided with the installation package. Using this tool, you can specify the relationship between parent and child organizations.

To run the tool, complete the following steps:

1. Log in to the BlackBerry AtHoc server and change to the following directory:
2. Locate the following executable file: `EAMigrator`.

   `..\AtHocENS\ServerObjects\Tools`
3. Right-click the file and select **Run as Administrator**.



4. The Enterprise Migrator opens.

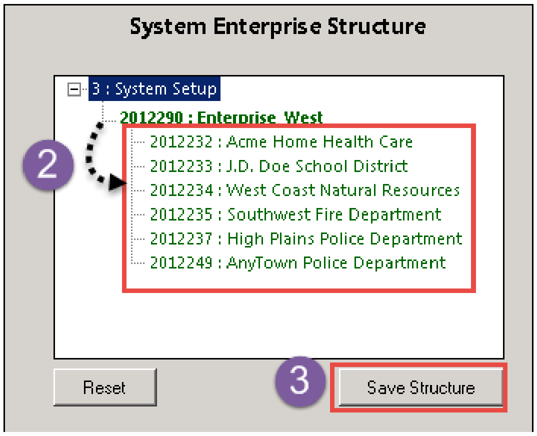
Migrate organizations to the enterprise

Run the Enterprise Migration tool to create or modify an Enterprise hierarchy, and to promote attributes and alert folders from sub-organizations to the Enterprise or System level.

To organize the Enterprise Hierarchy, complete the following steps:

1. Plan your hierarchy prior to using the tool. After you save your changes you CANNOT change them!
2. The list of organizations shows all standalone organizations, except for basic organizations. If an organization is missing, it likely has an incorrect database type.
3. In the first column of the Enterprise Migrator, drag and drop any organization under another organization to specify the Enterprise and sub-organization levels.

   For example, the following image shows seven organizations. When the tool opens, all are considered standalone organizations. Six organizations have been dragged under Enterprise West, migrating them to sub-organizations.


System Enterprise Structure
3 : System Setup
2012290 : Enterprise West
2012232 : Acme Home Health Care
2012233 : J.D. Doe School District
2012234 : West Coast Natural Resources
2012235 : Southwest Fire Department
2012237 : High Plains Police Department
2012249 : AnyTown Police Department
2
3
Reset
Save Structure

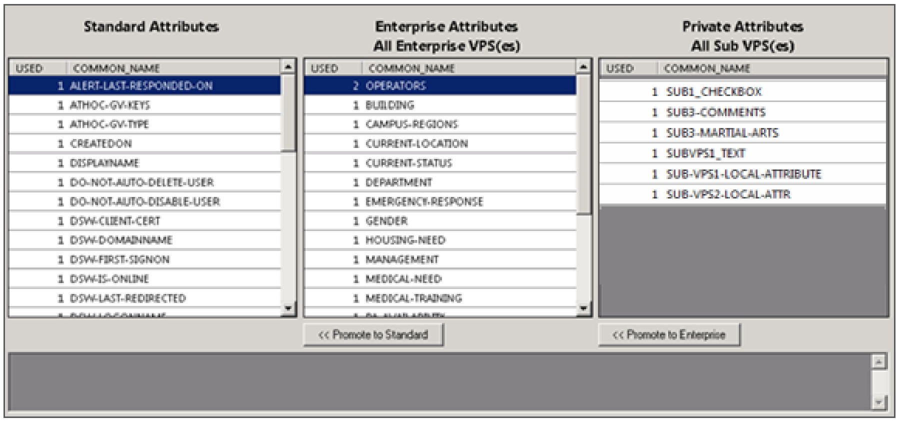
4. Verify your structure. This is very Important. You CANNOT undo this step!
5. Click **Save Structure** to save the changes.

Promote custom attributes and alert folders

During migration, you specify at which level the custom attributes and alert folders are defined: at the system, the enterprise, or the sub-organization. If just a small group of users in a sub-organization needs access to an attribute, it should be handled locally. However, for most user attributes or alert folders, the system or Enterprise level is the typical location.

To promote custom attributes:

1. Open the Enterprise Migrator tool and click the **User Attributes** button.
2. Determine how many instances there are of an attribute at the sub-organization and Enterprise organization level and promote if it seems efficient. If you promote an attribute to the Enterprise level, it is promoted from all the sub-organizations within that enterprise.
3. Verify that you want to promote the attributes. You cannot undo this step.



Standard Attributes

USED	COMMON_NAME
1	ALERT-LAST-RESPONDED-ON
1	ATHOC-GV-KEYS
1	ATHOC-GV-TYPE
1	CREATEDON
1	DISPLAYNAME
1	DO-NOT-AUTO-DELETE-USER
1	DO-NOT-AUTO-DISABLE-USER
1	DSW-CLIENT-CERT
1	DSW-DOMAINNAME
1	DSW-FIRST-SIGNON
1	DSW-IS-ONLINE
1	DSW-LAST-REDIRECTED

Enterprise Attributes
All Enterprise VPS(es)

USED	COMMON_NAME
2	OPERATORS
1	BUILDING
1	CAMPUS-REGIONS
1	CURRENT-LOCATION
1	CURRENT-STATUS
1	DEPARTMENT
1	EMERGENCY-RESPONSE
1	GENDER
1	HOUSING-NEED
1	MANAGEMENT
1	MEDICAL-NEED
1	MEDICAL-TRAINING

Private Attributes
All Sub VPS(es)

USED	COMMON_NAME
1	SUB1_CHECKBOX
1	SUB3-COMMENTS
1	SUB3-MARTIAL-ARTS
1	SUBVPS1_TEXT
1	SUB-VPS1-LOCAL-ATTRIBUTE
1	SUB-VPS2-LOCAL-ATTR

4. Select the attribute name and click **Promote to Enterprise** or **Promote to System** to move them up to a higher level.

   Promote an attribute from sub-organization to Enterprise if the entire enterprise needs to use the attribute. Keep the attribute at sub-organization if you want to restrict access to that organization. For example, promote a general attribute like `DepartmentName` to Enterprise because each employee needs to be grouped in a department. Alternatively, keep an attribute like `SoftballTeam` at the sub-organization because its members have joined a lunchtime league.
5. Click the **Alert Folders** button.
6. Select an alert folder type to promote, and click **Promote to Enterprise** or **Promote to System** based on what types of alerts certain personnel should see.

   For example, promote an alert folder like `FireDrills` from sub-organization to Enterprise if the entire enterprise needs to receive alerts from that alert folder. Keep the alert folder like `ExecutiveSafety` at sub-organization if you want to restrict access to operators and users that have a need to know.
7. Save your changes.

You have completed the reorganization.

What’s next?

Grant roles to the enterprise administrator for access to the sub-organizations.

1. Restart IIS after you have made the structure or content changes.
2. Log in to the Enterprise organization as an administrator.
3. Create a user and grant this user the Enterprise Administrator role.

4. Change to each sub-organization and grant the same user the Organization Administrator role.

Duplicate organizations across systems

Use the Organization Duplicator to make a copy of an organization on another server to set up a failover system, or to migrate to a new server. This tool is located on the application server.

Prerequisites:

- Two configured organizations on different database servers:
  - **Source server**: The server location of the organization to be duplicated
  - **Target server**: The server location where the organization is to be duplicated
- The source server should have configured users, alert templates, map layers, and other objects

Objects that are not duplicated:

- Global Health Monitors
- AtHoc Connect Organizations
- Incoming Alerts
- Sent Alerts
- User Accounts
- Distribution Lists - Static only

For detailed information about what is duplicated, refer to the "Organization Duplicator Object Management" section of this guide.

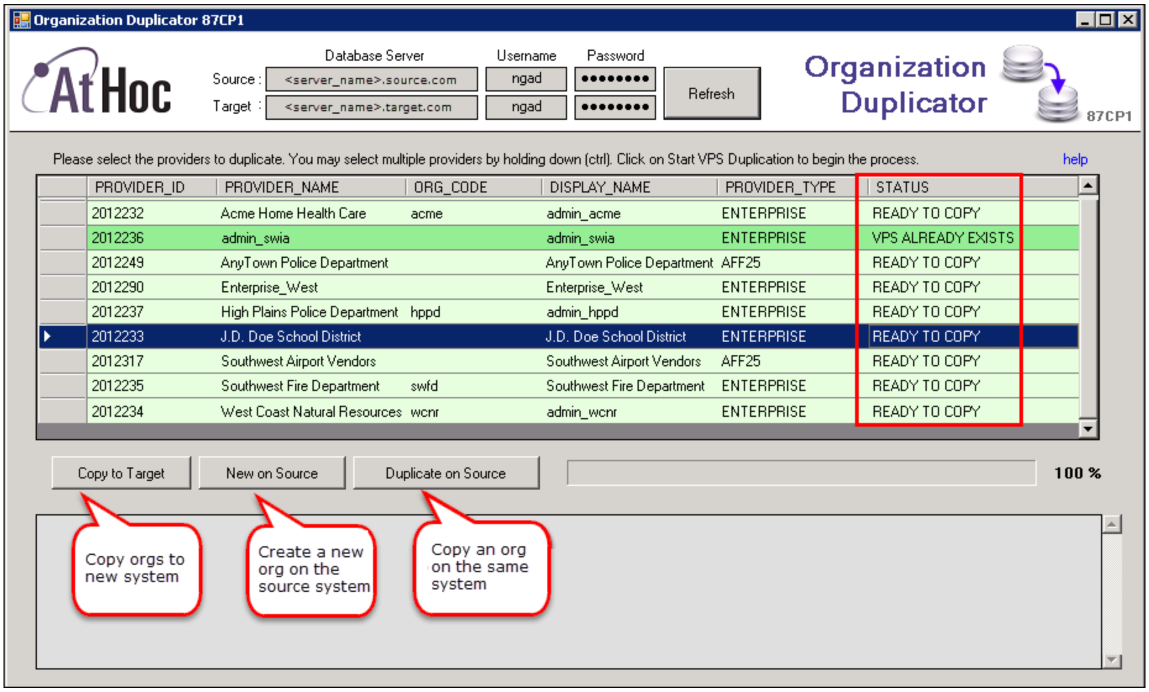
To duplicate an organization, complete the following steps:

1. Log in to the application server for the source system and navigate to the following directory:

   `AtHocENS/ServerObjects/Tools/VPSDuplicator`
2. Run the Organization Duplicator tool as an administrator.
3. Provide the source and target server information:
   - Source:
     - Database Server: The source application server name. For example:

       `DBSourceServer.mynetwork.com`
     - Username and Password of the ngad database.
   - Target:
     - Database Server: The target application server name. For example:

       `DBTargetServer.mynetwork.com`
     - Username and Password of the ngad database.
4. Click **Connect** to establish a connection and view the organizations that can be duplicated.



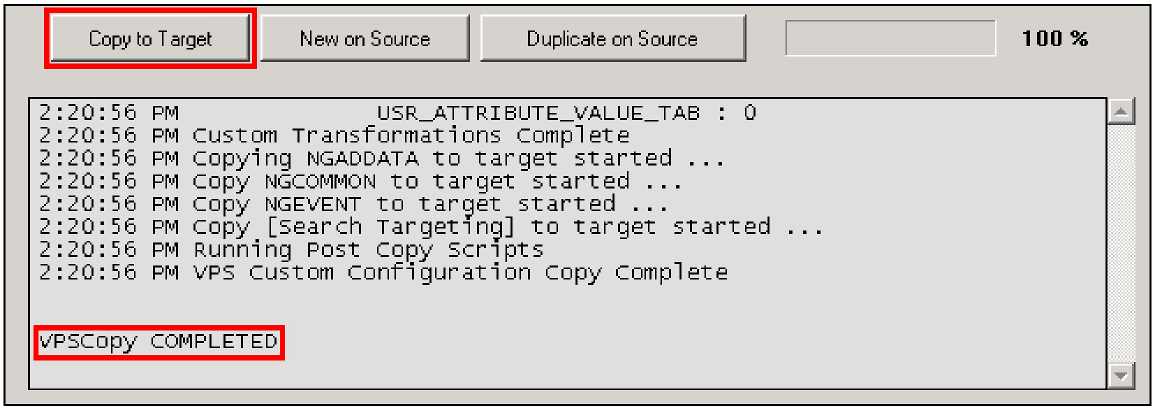
	Database Server	Username	Password
Source :	<server_name>.source.com	ngad	••••••••
Target :	<server_name>.target.com	ngad	••••••••

Please select the providers to duplicate. You may select multiple providers by holding down (ctrl). Click on Start VPS Duplication to begin the process.

PROVIDER_ID	PROVIDER_NAME	ORG_CODE	DISPLAY_NAME	PROVIDER_TYPE	STATUS
2012232	Acme Home Health Care	acme	admin_acme	ENTERPRISE	READY TO COPY
2012236	admin_swia		admin_swia	ENTERPRISE	VPS ALREADY EXISTS
2012249	AnyTown Police Department		AnyTown Police Department	AFF25	READY TO COPY
2012290	Enterprise_West		Enterprise_West	ENTERPRISE	READY TO COPY
2012237	High Plains Police Department	hppd	admin_hppd	ENTERPRISE	READY TO COPY
2012233	J.D. Doe School District		J.D. Doe School District	ENTERPRISE	READY TO COPY
2012317	Southwest Airport Vendors		Southwest Airport Vendors	AFF25	READY TO COPY
2012235	Southwest Fire Department	swfd	Southwest Fire Department	ENTERPRISE	READY TO COPY
2012234	West Coast Natural Resources	wcnr	admin_wcnr	ENTERPRISE	READY TO COPY

5. Select the organizations to be duplicated. The Status column indicates whether the organization is ready to copy.

   The message log indicates whether the duplication was successful.



```
2:20:56 PM              USR_ATTRIBUTE_VALUE_TAB : 0
2:20:56 PM Custom Transformations Complete
2:20:56 PM Copying NGADDATA to target started ...
2:20:56 PM Copy NGCOMMON to target started ...
2:20:56 PM Copy NGEVENT to target started ...
2:20:56 PM Copy [Search Targeting] to target started ...
2:20:56 PM Running Post Copy Scripts
2:20:56 PM VPS Custom Configuration Copy Complete

VPSCopy COMPLETED
```

Create or duplicate organizations on the source server

You can also use the Organization Duplicator to create or duplicate organizations on the source server.

To create a new organization , complete the following steps:

1. Click **New on Source**.
2. Enter the organization name and organization code (around 5 characters).
3. Select the type of organization.
4. Click **OK**.

5. You cannot select an organization administrator using the tool.

   The message log shows whether the new organization has been created.

To duplicate an existing organization, complete the following steps:

1. Click **Duplicate on Source**.
2. Enter the organization name and the number of copies of the organization that should be created.
3. If you select a value higher than 1, organizations are created with the following string appended to the name: “Copy 0001”.
4. Click **OK**.

   The message log shows whether the duplicated organizations have been created.

Note: After duplicating the organization, verify operator permissions to the new organization.

- Use the system administration role to do initial set up. To access the Users menu, use Advanced Operator Manager to assign your user account the Organization Administrator role.
- **Distribution List permissions**: Ensure that users with accounts in a different organization have distribution list permission in the new organization. Use Advanced Operator Manager to provide access distribution lists.
- **Basic Organization roles:** If operators from other organizations need permission for a Basic organization, use Advanced Operator Manager to configure permissions. Grant either the "Admin" or the "Operator" roles. If you choose other roles, you can get unexpected results.

Configure AtHoc database operations to use Windows authentication

Run the configuration script on *each* application server so that AtHoc database operations use Windows authentication. This script ensures a trusted connection from the application server to connect to database server. All AtHoc applications need to run under a Windows domain account.

1. From the application server, open a command prompt and run as administrator.
2. Navigate to the following directory: <*%AtHocENS%*>`\ServerObjects\Tools\`
3. Run the following script, using 32-bit version of cscript:
   `setWindowsAuth.vbs <%`*DomainName*`%> <%`*Domain AccountName*`%> <%`*DomainAccountPassword*`%>`

   Where:

`DomainName`	The Windows domain name of the application server
`Domain Account Name`	The name of the Windows domain account
`DomainAccountPassword`	The password of the Windows domain account

The script makes the following updates:

- Creates a new user in SQL Server and makes that user the database owner of all AtHoc databases
- Updates the connection string for BlackBerry AtHoc to use a trusted connection

- Modifies all AtHoc application pool identities in IIS to use the new domain account
- Modifies the Anonymous account in IIS from IUSR to the new domain account

Configure IIS processor affinity

On multi-CPU servers, Application Pools can be configured to establish affinity between worker processes and an individual Processor to more efficiently use CPU caches. This configuration also isolates Applications such that if one application causes a CPU to stop responding, other CPU’s continue to function normally. Processor affinity is used in conjunction with the processor affinity mask setting to specify CPUs.

To configure processor affinity, complete the following steps:

1. Create a .vbs file named affinity.vbs, copy the following data, and save it in your temp folder.

   ```
   set appPoolObj=GetObject("IIS://localhost/W3svc/AppPools/DefaultAppPool")
   ' Set the properties. Enable processor affinity for processors 0,1,2,3:
   appPoolObj.Put "SMPAffinitized", TRUE
   appPoolObj.Put "SMPProcessorAffinityMask", &HFF
   ' Save the property changes in the metabase:
   appPoolObj.SetInfo
   WScript.Echo "After: " & appPoolObj.SMPAffinitized & ", " & appPoolObj.SMPProcessorAffinityMask
   ```

2. Change the value of **SMPProcessorAffinityMask** in `affinity.vbs` to reflect the number of cores available.

   The value for SMPProcessorAffinityMask must be entered as hexadecimal.

To specify which specific cores to use, complete the following steps:

1. Create the value as binary (each core is represented by 1 bit) and then transformed into a hexadecimal. The easiest way to do this is to use a Windows scientific calculator.
2. As an example, eight cores in binary would be represented as `11111111`.

To use only the first four cores (for example, all cores in the same chip for a quad-core), select one of the following:

- `00001111`

OR

- `11110000` (if dual-quad).

To use every other core, complete the following steps:

1. Enter **`10101010`** (or `01010101`) in a Windows scientific calculator in binary data (Bin) and then click **Hex** to see the equivalent value in hexadecimal (&AA or &55).
2. Stop IIS and run the `affinity.vbs` file in command prompt. (`cscript affinity.vbs`)

   You should see the mask change to the correct decimal value for the hexadecimal value that was used. If you are not sure what the decimal value should be, check the Windows calculator.

3. Reset the IIS.
4. Open the Performance Monitor (`perfmon`) performance tab to verify that the correct core combination is used.

Increase the IIS file size upload limit

When uploading files, IIS may return an HTTP 500 error because the maximum file size limit has been exceeded. For example, this can occur when a relatively small number of users are imported from a CSV file, or when uploading very large audio files.

To prevent this from happening, complete the following steps:

1. In IIS Manager, click on the **client** web application.
2. Double-click the ASP feature icon.
3. Expand the Limits Properties.
4. Change the value of the Maximum Requesting Entity Body Limit.

This entry specifies the maximum number of bytes allowed in the entity body of an ASP request. The default is 200000 bytes.

Note: The MSI sets this to 20480000 (20 Mb). If audio files larger than that will need to be uploaded, this value needs to be increased.

Database recovery setting

If the recovery model is set to Full, the transaction log files must be backed up before they become full. Otherwise, all operations on the database will completely halt and the system will freeze. It is very important to understand the backup strategy for the site and configure these settings carefully.

Note: The default setting for recovery is **Simple**.

Chapter 8: IIS 8.5
Security Technology Implementation Guide

In release 7.3, BlackBerry AtHoc was upgraded to IIS Security Technology Implementation Guide (STIG) release 8.5. The following sections describe the server and application tasks you need to complete to achieve IIS 8.5 STIG compliance in your BlackBerry AtHoc system.

The following topics are documented in this chapter:

Server STIG

This section describes the tasks you need to complete to ensure your servers comply with the IIS 8.5 STIG.

IISW-SV-000103: Enable log file and Event Tracing windows

Both the log file and Event Tracing for Windows (ETW) for the IIS 8.5 web server must be enabled.

To check compliance with IISW-SV-000103, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 server name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Log file only** option is selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 server name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, select the **Both log file and ETW event** option.
5. In the Actions pane, click **Apply**.

IISW-SV-000107: Sufficient web server log records for location of web server events

The IIS 8.5 web server must produce log records that contain sufficient information to establish where IIS 8.5 web server events occurred.

To check compliance with IISW-SV-000107, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.

3. Under **IIS**, double-click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Click **Select Fields**.
6. Verify that the **Service Name** and **Protocol Version** fields are selected.

If the **Service Name** and **Protocol Version** fields are not checked, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.
3. Click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Select the **Service Name** and **Protocol Version** fields.
6. Click **OK**.
7. In the Actions pane, click **Apply**.

IISW-SV-000108: Sufficient web server log records for source of web server events

The IIS 8.5 web server must produce log records that contain sufficient information to establish the source of IIS 8.5 web server events.

To check compliance with IISW-SV-000108, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Click **Select Fields**.
6. Verify that **Server Name** and **Host** are checked.

If the **Server Name** and **Host** fields are not checked, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Select the **Server Name** and **Host** fields.
6. Click **OK**.
7. In the Actions pane, click **Apply**.

IISW-SV-000110: Sufficient web server log records to establish the outcome of web server events

The IIS 8.5 web server must produce log records that contain sufficient information to establish the outcome (success or failure) of IIS 8.5 web server events.

To check compliance with IISW-SV-000110, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is set to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, verify that the following fields are configured:
   - Request Header >> Connection
   - Request Header >> Warning
   - Server Variable >> HTTP_CONNECTION

If any of these fields are not configured, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Verify that **Format:** under **Log File** is set to **W3C**.
5. Click **Fields**.
6. Select the following custom fields:
   - Request Header >> Connection
   - Request Header >> Warning
   - Server Variable >> HTTP_CONNECTION
7. Click **OK**.
8. In the Actions pane, click **Apply**.

IISW-SV-000111: Sufficient web server log records to establish identity

The IIS 8.5 web server must produce log records that contain sufficient information to establish the identity of any user, subject, or process associated with an event.

To check compliance with IISW-SV-000111, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.

3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that the format is set to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, verify that **User Agent**, **User Name**, and **Referrer** are selected.
7. Under **Custom Fields**, verify that the following fields are selected:
    - Server Variable >> HTTP_USER_AGENT
    - Request Header >> User-Agent
    - Request Header >> Authorization
    - Response Header >> Content-Type

If any of these fields are not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that the format is set to **W3C**.
5. Select **Fields**.
6. Under **Standard Fields**, select **User Agent**, **User Name**, and **Referrer**.
7. Under **Custom Fields**, select the following fields:
    - Server Variable >> HTTP_USER_AGENT
    - Request Header >> User-Agent
    - Request Header >> Authorization
    - Response Header >> Content-Type
8. Click **OK**.
9. Under Actions, click **Apply**.

IISW-SV-000112: Web server must use Event Tracing for Windows logging option

The IIS 8.5 web server must use the Event Tracing for Windows (ETW) logging option.

To check compliance with IISW-SV-000112, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Verify that the **W3C** format is selected for **Log File**.
5. Verify that the **Both log file and ETW event** log event destination option is selected.

If the **W3C** or the **Both log file and ETW event** options are not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. For the Log File, select **W3C** from the **Format** list.
5. For Log Event Destination, select the **Both log file and ETW event** option.
6. In the Actions pane, click **Apply**.

IISW-SV-000120: Samples, examples, and tutorials must be removed from production server

All IIS 8.5 web server sample code, example applications, and tutorials must be removed from a production IIS 8.5 server.

To check compliance with IISW-SV-000120, complete the following steps:

1. Navigate to the **inetpub\** folder.
2. Check for any executable sample code, example applications, or tutorials that are not explicitly used by a production website.
3. Navigate to the **Program Files\\Common Files\\System\\msadc** folder.
4. Check for any executable sample code, example applications, or tutorials that are not explicitly used by a production website.
5. Navigate to the **Program Files (x86)\\Common Files\\System\\msadc** folder.
6. Check for any executable sample code, example applications, or tutorials that are not explicitly used by a production website.

If any of the folders or sub folders above contain any executable sample code, example applications, or tutorials that are not explicitly used by a production website, your server is not compliant.

If your server is not compliant, remove any executable sample code, example applications, or tutorials that are not explicitly used by a production website.

IISW-SV-000124: Web server must have MIMEs that invoke OS shell programs disabled

The IIS 8.5 web server must have Multipurpose Internet Mail Extensions (MIMEs) that invoke OS shell programs disabled.

To check compliance with IISW-SV-000124, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **MIME Types** icon.

4. From the **Group by** list, select **Content Type**.
5. Click **Select Fields**.
6. Under **Application**, verify that the following MIME types for OS shell program extensions have been removed from the list of extensions:
    - .exe
    - .dll
    - .com
    - .bat
    - .csh

If any of these OS shell MIME types are configured, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. Select **Content Type** from the **Group by:** list.
5. Under **Application**, remove the following MIME types for OS shell program extensions from the list of extensions:
    - .exe
    - .dll
    - .com
    - .bat
    - .csh
6. In the Actions pane, click **Apply**.

IISW-SV-000146: Web server must not impede ability to write log record content to an audit log

The IIS 8.5 web server must not impede the ability to write specified log record content to an audit log server.

To check compliance with IISW-SV-000146, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Both log file and ETW event** option is not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Select the **Both log file and ETW event** option.
5. In the Actions pane, click **Apply**.

IISW-SV-000153: Web server must maintain the confidentiality of controlled information during transmission

An IIS 8.5 web server must maintain the confidentiality of controlled information during transmission through the use of an approved TLS version.

To check compliance with IISW-SV-000153, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Access an administrator command prompt.
4. Type **regedit<enter>** to access the registry of the server.
5. Navigate to the following registry paths:
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server`
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server`
6. Verify that **DisabledByDefault** has a REG_DWORD value of **0**.
7. Navigate to the following registry paths:
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server`
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server`
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server`
8. Verify that **DisabledByDefault** has a REG_DWORD value of **1**.

If any of the listed registry paths do not exist or are configured with the incorrect value, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Access an administrator command prompt.
4. Type **regedit<enter>** to access the registry of the server.
5. Navigate to the following registry paths:
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server`
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server`
6. Set the **DisabledByDefault** REG_DWORD value to **0**.
7. Navigate to the following registry paths:
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server`
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server`
    - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server`
8. Set the **DisabledByDefault** REG_DWORD value to **1**.

IISW-SV-000154: Web server must maintain the confidentiality of controlled information

The IIS 8.5 web server must maintain the confidentiality of controlled information during transmission through the use of an approved TLS version.

To check compliance with IISW-SV-000154, complete the following steps:

1. Review the web server documentation.
2. Review the web server deployed configuration.

3. Determine which version of TLS is being used.

If the TLS version is not an approved version according to NIST SP 800-52 or to the non-FIPS-approved enabled algorithms, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Configure the web server to use an approved TLS version according to NIST SP 800-52.
2. Disable any non-approved TLS versions.

Application STIG

This section describes the tasks you need to complete to ensure your application complies with the IIS 8.5 STIG.

IISW-SI-000206: Enable log file and Event Tracing windows

Both the log file and Event Tracing for Windows (ETW) for each IIS 8.5 website must be enabled.

To check compliance with IISW-SI-000206, complete the following steps for each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Both log file and ETW event** option is not selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log Event Destination**, select the **Both log file and ETW event** option.
5. In the Actions pane, click **Apply**.

IISW-SI-000209: Enable log file and Event Tracing windows

The IIS 8.5 web site must produce log records containing sufficient information to establish the identity of any user, subject, or process associated with an event.

To check compliance with IISW-SI-000209, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Under **Log File**, verify that the **Format:** field is configured to **W3C**.
4. Click **Fields**.

5. Under **Standard Fields**, verify that the **User Agent**, **User Name**, and **Referrer** fields are selected.
6. Under **Custom Fields**, verify that the following fields are selected:
   - Server Variable >> HTTP_USER_AGENT
   - Request Header >> User-Agent
   - Request Header >> Authorization
   - Response Header >> Content-Type

If any of the above fields are not selected, your application is not compliant.

If your application is not compliant, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Under Log File, set the **Format:** field to **W3C**.
4. Click **Fields**.
5. Under **Standard Fields**, select the **User Agent**, **User Name**, and **Referrer** fields.
6. Under **Custom Fields**, select the following fields:
   - Server Variable >> HTTP_USER_AGENT
   - Request Header >> User-Agent
   - Request Header >> Authorization
   - Response Header >> Content-Type
7. Click **OK**.
8. In the Actions pane, click **Apply**.

IISW-SI-000210: Sufficient website log records to establish identity

The IIS 8.5 web site must produce log records containing sufficient information to establish the identity of any user, subject, or process associated with an event.

To check compliance with IISW-SI-000210, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Under **Log File**, verify that the **Format:** field is configured to **W3C**.
4. Click **Fields**.
5. Under **Standard Fields**, verify that the **User Agent**, **User Name**, and **Referrer** fields are selected.
6. Under **Custom Fields**, verify that the following fields are selected:

- Server Variable >> HTTP_USER_AGENT
- Request Header >> User-Agent
- Request Header >> Authorization
- Response Header >> Content-Type

If any of the above fields are not selected, your application is not compliant.

If your application is not compliant, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Click the **Logging** icon.
4. Under **Log File**, set the **Format:** field to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, select the **User Agent**, **User Name**, and **Referrer** fields.
7. Under **Custom Fields**, select the following fields:
    - Server Variable >> HTTP_USER_AGENT
    - Request Header >> User-Agent
    - Request Header >> Authorization
    - Response Header >> Content-Type
8. Click **OK**.
9. In the Actions pane, click **Apply**.

IISW-SI-000211: Website must use Event Tracing for Windows logging option

The IIS 8.5 web server must use the Event Tracing for Windows (ETW) option.

To check compliance with IISW-SV-000211, complete the following steps for each website hosted on the IIS 8.5 web server.

1. Open the IIS 8.5 IIS Manager.
2. Select the website to review.
3. In the **IIS** section, double-click the **Logging** icon.
4. Verify that the **W3C** format is selected for **Log File**.
5. Verify that the **Both log file and ETW event** log event destination option is selected.

If the **W3C** or the **Both log file and ETW event** options are not selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Select the website to update.
3. In the **IIS** section, double-click the **Logging** icon.
4. For the Log File, select **W3C** from the **Format** list.
5. For Log Event Destination, select the **Both log file and ETW event** option.
6. In the Actions pane, click **Apply**.

IISW-SI-000214: Website must have MIMEs that invoke OS shell programs disabled

The IIS 8.5 website must have Multipurpose Internet Mail Extensions (MIMEs) that invoke OS shell programs disabled.

To check compliance with IISW-SI-000214, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 website.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by** list, select **Content Type**.
5. Click **Select Fields**.
6. Under **Application**, verify that the following MIME types for OS shell program extensions have been removed from the list of extensions:
   - .exe
   - .dll
   - .com
   - .bat
   - .csh

If any of these OS shell MIME types are configured, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 website.
3. Under **IIS**, double-click the **MIME Types** icon.
4. Select **Content Type** from the **Group by:** list.
5. Under **Application**, remove the following MIME types for OS shell program extensions from the list of extensions:
   - .exe
   - .dll
   - .com

- .bat
- .csh

6. In the Actions pane, click **Apply**.

IISW-SI-000228: Non-ASCII characters in URLs must be prohibited

Non-ASCII characters in URLs must be prohibited by any IIS 8.5 website.

To check compliance with IISW-SI-000228, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click website name.
3. Double-click the **Request Filtering** icon.
4. In the Actions pane, click **Edit Feature Settings**.
5. Verify that the **Allow high-bit characters** check box is not selected.

If the **Allow high-bit characters** check box is selected, your application is not compliant.

Note: If the website has operational reasons to set **Allow high-bit characters**, this vulnerability can be documented locally by the ISSM/ISSO.

If your application is not compliant, complete the following steps for each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 Manager.
2. Click the website name.
3. Double-click the **Request Filtering** icon.
4. In the Actions pane, click **Edit Feature Settings**.
5. Deselect the **Allow high-bit characters** check box.

Chapter 9: Verify BlackBerry AtHoc is operational

After completing a new install or upgrade of BlackBerry AtHoc, a thorough test of functionality should be performed to ensure that the system operates properly. This chapter presents a set of test procedures that cover the most important system functions.

The following topics are covered in this chapter:

Basic BlackBerry AtHoc test procedures

The following table provides detailed instructions on the basic BlackBerry AtHoc test procedures.

√	Description	Expected result
Log in		
1	Open a browser, and navigate to the Management System application. To do this, navigate to the `<AtHoc-ENS-URL>`. For example, `https://alerts.company.com` (if SSL is used).	The login page displays.
	Log in as the username `IWSAdmin` and password: `athoc123`.	The BlackBerry AtHoc Management System Home Page displays.
	In the Navigation bar, click the ⚙ **(Settings)** icon.	
	Click the **Organization Manager** link and create an Enterprise organization.	Complete Management setup steps from the Enterprise organization level.
Connect a client		
	Install a desktop software client, as described in the BlackBerry AtHoc Client Guide.	The desktop software is installed on the users PC and the user appears in the User manager.
Custom attributes		
	Open the Management System. In the Navigation bar, click the ⚙ **(Settings)** icon.	
	Click the **User Attributes** link in the Users section and click the **New** button.	
	Create a multi-select picklist attribute whose Attribute Name is **Test**.	
	Assign two pick-list values to the Test attribute: **T1** and **T2**.	
	Click **Save** to create the pick list attribute.	A pick list attribute named **Test** is created.

√	Description	Expected result
	Create a number attribute named **ID**.	A number attribute named **ID** is created.
	Create a text attribute named **Comments**.	A text attribute named **Comments** is created.
	Select the pick list attribute named **Test** and click **Delete**.	The **Test** attribute is deleted.
Hierarchy editing		
	In the Navigation bar, click the ⚙ **(Settings)** icon.	
	From the Settings screen, navigate to the Hierarchy Builder. Create two hierarchies: **Organizational** and **Distribution List**.	The **Organizational** and **Distribution List** hierarchies are created.
Distribution lists		
	In the Navigation bar, select the **Users** menu. Click the **Distribution Lists** link.	
	Create a static list named **Stat1** and add your user ID as a member.	The **Members** field displays `1`.
	Create a dynamic list named **Dyn1** and add a criteria that includes your user ID in the results.	
Import/Export users		
	In the Navigation bar, select the **Users** menu. Click the **Users** link.	
	Click the **More Actions** button. Select **Import**.	
	Download a template CSV file. An Excel spreadsheet opens and must (if new install) contain only the selected User ID.	**Note:** Excel must be installed on your machine. If you do not have Excel, use Notepad to view the CSV file content. The file must contain all static lists, custom attributes, and devices.
	Fill all of the required fields.	
	Save the file under the name `test.csv`.	
	Return to the Management system and continue from the Import User File screen.	

√	Description	Expected result
	Select the import .csv file: a. Click the **Browse** button. b. In the file selection dialog, navigate and select the test.csv file. c. Right-click and select **Open with** to confirm the selection of the file. d. Click **Open** e. Click **Import** .	The Import User Progress window displays and all users must be successfully processed. The **Last import** field must display the correct date and time of the Import.
	Click **Download Log** and in the File Download dialog, select **Open**.	An Excel spreadsheet opens and displays all the users from the CSV file. The AtHoc Import Result column contains the value *OK* and each user has a unique user ID.
	Compare the Users list with the Import .csv file. To open the .csv file: a. From the Users page, select click **More Actions>Import**. b. Click **Browse** and open the import .csv file.	An Excel spreadsheet opens and contains the current user and the users that were imported.
	In the Navigation bar, select the **Users** menu. Click the **Users** link.	All qualified users display in the table.
	Spot check users to verify that the correct details have been imported.	The details pane at the bottom of the screen displays the correct information for the selected end user.
Alert templates (formerly scenarios)		
	In the Navigation bar, click the **Alerting** menu. Click the **Alert Templates** link.	The Alert Templates list opens.
	Click the **New** button.	The New Alert Template screen opens.
	Create an alert template named **SC1**.	
	For the new template: • Check **Available for Quick Publish**. • Add the Title and Body. • Add a response option. • Target one or more users. • Select delivery to the following device: Desktop popup. • Check spelling.	

√	Description	Expected result
	Save the alert template.	An alert template named **SC1** is created.
Alert publishing		
	In the Navigation bar, click the **Alerting** menu. Click the **New Alert** link.	
	Publish an alert template: a. Select the **SC1** alert template and click **Edit Alert**. b. In the Targeting section, click **View List**. c. Click **Review and Publish**. d. Click **Publish**.	All qualified users are targeted. The Sent Alerts list displays the published alert with a Live status. If the status is still Scheduled, wait 15 seconds and re-select. Sent Alerts to refresh the display. The status must be live in no more than 15 seconds from scenario activation.
	Wait up to two minutes for the alert to arrive on the users desktop. After you receive the popup, click **Acknowledge and Close**.	The desktop popup displays and audio alert plays (if speakers are connected and audio is enabled). Upon acknowledgment, the popup must disappear.
Self Service		
	From the users machine, right-click the AtHoc desktop software system tray icon and select **Access Self Service**. For *Mac* users, left-click to open the status item menu. **Note:** The Safari browser is launched for any service selected from the status item menu.	A new browser window displays the Self Service Inbox which contains the just published alert (but only if the user authentication is set to Auto\Windows authentication).
	Navigate through the other Self Service tabs and verify that the displayed information is correct.	
Alert tracking reports		
	In the Navigation bar, click the **Alerting** menu. Click the **Sent Alerts** link.	The published alert appears in the list with a Live status.
	Hover the pointer over the published alert. The tool tip displays the title body and responses. Click the alert to open the details.	You can see the Delivery Summary, which lists the number of targeted users, the number of Sent to users, and the number of users who acknowledged the alert. You can also see a drop–down list of detail reports.

√	Description	Expected result
	Click the **Export > Export Full Report** link. Note that you must have Excel 2003 or higher installed on your machine to open the report.	You are asked to open the .csv file. The Detailed Alert tracking report must open and display the alert details and track information. You can see the users who received and acknowledged the alert.
Audio files		
	In the Navigation bar, click the ⚙ **(Settings)** icon. From Basic, click **Audio Files**.	
	Click **New**.	
	Enter an audio name and upload a large .WAV file: larger than 1 MB, but not more than 2 MB.	**Note:** You can record a .WAV file using the Windows Sound Recorder (Start / Programs / Accessories / Entertainment / Sound Recorder). A voice recording of 30 seconds must be 1 MB. After you record a voice, save it using **File / Save As**.
	After selecting the file to be uploaded, click **Save**.	Return to Audio Files.
	Select the newly created audio from the audio list in the right pane, then click **Play**.	Ensure the PC is equipped with speakers that are turned on, and that audio is enabled; you should hear the uploaded audio file.
Error logs		
	Check the Windows application event log and the AtHocEventViewer on the application server.	You must not see any unexplained errors in the log.

Extended BlackBerry AtHoc test procedures

√	Description	Expected result
	Perform detailed end user search.	
	Publish an alert targeted to a static list.	
	Publish an alert targeted to a dynamic list.	
	Publish an alert with different device preference options.	
	Create an operator with a user base.	
	Create/Enable/Disable/Delete an alert folder.	
	Manually create a new user and assign a custom attribute.	
	End a published alert.	
	Check navigation.	

Appendix A: Troubleshooting

Error code	Message	Cause	Resolution
None	The installation aborts as the following prerequisites are missing on the server. Install these components first: <*List of Missing Prerequisites*>	The listed prerequisites are not installed.	Install the missing prerequisites.
None	Error connecting to the database. Check that the database server is up and that the SQL Server services is running, then click **OK** to try again. Click **Cancel** to exit.	If this message appears after receiving a success with the **Test Connection** button, the application server installation is likely on a different domain than the installation for the database server (the MSI connects using Windows authentication).	Run the MSI with the `msiexec` command, and pass in the following parameters to specify a sys admin account: IS_SQLSERVER_ AUTHENTICATION=1 IS_SQLSERVER_ USERNAME=sa IS_SQLSERVER_ PASSWORD=the_password
None	ActiveX component can't create object: 'Scripting.FileSystemObject' MSI fails when attempting to run a VBScript custom action.	One or both of the following issues: • HBSS is enabled • McAfee overwrote the registry entry for VBScript.dll with its own entry	• Disable HBSS for installation • Check the value for the following parameter: `HKLM/Software/Classes/CLSID/{B54F3741-5B07-11cf-A4B0-00AA004A55E8}\InprocServer32,` Make sure the value is: `C:\Windows\system32\vbscript.dll`
None	SQL Server is not installed.	The MSI displays this error during a new database install if one of the following issues exists: • The version of SQL Server is lower than R2. • The MSI is being run from the application server.	• Install SQL Server R2 or higher. • Perform a new database server installation on the database server.

Error code	Message	Cause	Resolution
2146893-052	Connection was successfully established with the server but an error occurred during the pre-login handshake (provider: SSL provider, error 0. the local security authority cannot be connected).	The SQL Server password requirement is not met by the default password provided in the MSI.	Choose a different password than the default password for `ngad`. Enter a custom password that meets the strong password requirement of SQL Server.
2147217-843	Failed to connect to SQL database (-2147217843 database_name).	When you receive this during upgrade, it could be corruption in the MSI.	Contact BlackBerry AtHoc Support.
2147217-873	Failed to execute SQL string, error detail: The statement has been terminated.	One of the following issues: - Bad data - A bug in the SQL. For example, an SQL statement attempted to insert a null value into a column that does not accept nulls.	BlackBerry AtHoc Support may be able to help fix the data. If you contact BlackBerry AtHoc Support, be prepared to provide the MSI log file for analysis. If the cause is a bug in a SQL script, the bug fix will require building a new MSI.
2147217-887	Generic Error	A problem with the MSI.	Report to BlackBerry AtHoc Support; requires a fix and new installation package.
2147217-900	Failed to execute SQL string; Error detail; "Unclosed quotation mark after the character string.	Unclosed quotation mark. A bug in a SQL script.	A fix requires building a new MSI.
	No additional message.	During a new install, the `ngad` user password does not meet SQL Server password requirements.	Do not use the default password for `ngad`, enter a custom password that meets the strong password requirement of SQL Server
	The operating system returned the error "5(Access is denied." while attempting to "restoreContaininer::ValidateTargetForCreation" on <*path*>."	SQL Server service account does not have permission to create files.	Change the service account to “Local System account”.
	No additional message	The transaction log for database NGADDATA is full.	Shrink the NGADDATA database.
	No additional message	The Application server machine logon account did not have a logon on the Database server, or did not have a SQL Server logon with sys admin rights.	Grant the correct permissions or switch to an account that has the correct permissions.

Error code	Message	Cause	Resolution
2147217900	3a CreateUsers Error running ATH_CREATE_USERS sp: error -2147217900, exec dbo.ATH_DROP_USERS @dropLogin = 1	SQL Server is configured to require strong passwords, and the user chose to use the default password for the `ngad` database user, which does not meet strong password requirements.	Do not use the default password for `ngad`, enter a custom password that meets the strong password requirement of SQL Server.
	3a CreateUsers Error running ATH_CREATE_USERS sp: error -2147217900, The proposed new database owner is already a user or aliased in the database	The `ngad` user account was created manually (incorrectly).	Call your DBA, or contact BlackBerry AtHoc Support. Be prepared to provide the MSI log file for analysis.
2147319779	Library not registered	`Scrrun.dll` is not registered. This error occurs when one of the custom actions executes a `CreateObject` on `Scripting.FileSystemObject`. This error occurs on some locked down systems.	Register the 32-bit version of `scrrun.dll`.
2147467259	Unspecified error	A connection to the database server could not be made and returns the COM error code: E_FAIL "Unspecified error", which is a generic return code when a COM method call fails.	Make sure that the SQL Server service is running or call BlackBerry AtHoc Support.
	Failed to connect to SQL database...	The Windows authentication for the MSI was improperly handled.	Contact BlackBerry Athoc Support. Be prepared to provide the MSI log file for analysis.
None	3 SetTransactionLogSize - Error: MODIFY FILE failed. Size is greater than MAXSIZE. Provider-SQL0LEDB.I;Server-r=192.168.0.127;Initial Catalog-msdb;Integrated Security=SSPI.	The transaction log size is already set to a larger value than the size to which the MSI is attempting to set.	Decrease the size of the database that is specified in the error message. Set the transaction log size to a value less than 10 GB.
2147217900	3a IWSDBCA_IncreaseTransactionLogSize forUpgrade - Error: -214721790, Database 'ngevent' cannot be opened due to inaccessible files or insufficient memory or disk space. See the SQL Server error log for details.	Unsupported upgrade steps.	Contact BlackBerry AtHoc Support and ask for a copy of `ngevent.bak`, and restore it. Rerun the MSI after restoring `ngevent`.

Error code	Message	Cause	Resolution
None	Run the script outside the MSI to change the data type in OLP_ALERT_RECIPIENT_DEVICE_TAB.	The MSI detected over 1 million records in OLP_ALERT_RECIPIENT_DEVICE_TAB.	Run the SQL outside of the MSI; it might take several hours to complete. Contact BlackBerry AtHoc Support and ask for the "OLP_RCPT_DEVICE_TAB_DATA_TYPE_CHANGE" SQL script from the 6.1.8.80 archive and run it. Rerun the MSI after running the SQL script.
None	Assertion failed in `c:\documents` and `settings\robmen\local settings\temp\wp001\src\wcautil.cpp. 64 CustomAction ConfigureSql` called `WcaInitialize()` but not `WcaTerminate()` Abort=Debug, Retry=Skip, Ignore=Skip all	Wix or Windows Installer bug.	Rerun the MSI.

Appendix B: Organization duplicator object management

This section describes the objects that are copied during a single or cross-system duplication. Some objects are not duplicated depending on the type of the source organization or the account type.

The following table describes objects that are duplicated to the organization on the target server.

Organizations on Different Server

Feature	Objects	Details	Across servers	
			Duplicate	
			Enterprise/ sub (from SRC / SRC)	Basic (from SRC)
Server Configuration	Cascading Systems		Yes	
	Images			
	Gateways and Devices			
	Health Monitors	Actions only (not Global Health Monitors)		
System Setup (VPS 3)	Attributes		Yes	
	Channels			
Standard Organization Configuration	Provider Configuration		Yes	
	Page Layouts			
	Buttons			
	Gateways and Devices			
	Standard Hierarchy	Org Hierarchy, DL Hierarchy, Emergency Community		
	Standard DLs	Auto Delete Users Auto Disable Users		
	Alert Templates			
	Maps and Layers			

Feature	Objects	Details	Across servers	
			Duplicate	
			Enterprise/ sub (from SRC / SRC)	Basic (from SRC)
Custom Organization Configuration	Attributes		Yes	Yes
	Channels		Yes	Yes
	Audio		Yes	Yes
	Templates		Yes	Yes
	Mass Devices		Yes	Yes
	Custom DLs	Except Static List User Membership (see Users)	Yes	Yes
	Alert Templates	Except Targeting of Individual Users (see Users)	Yes	Yes
	Reports		Yes	Yes
	Schedules		Yes	Yes
	Operator Permissions		No	No
	Users, their DL Memberships, and Targeting	Organization Users	No	No
		Static DL User Membership	No	No
		Alert Templates Individual User Targeting	No	No

The following table describes objects that are created on the source server for a new organization, or duplicated to a new organization on the same server.

Organizations on Different Servers

Feature	Object	Details	Same Server					
			New			Duplicate		
			Enterprise (from 5)	Sub (from ENT)	Basic (from 6)	Enterprise (from SRC)	Sub (from SRC)	Basic (from SRC)
Server Configuration	Cascading Systems		No			No		
	Images							
	Gateways and Devices							
	Health Monitors	Actions only (not Global Health Monitors)						
System Setup (VPS 3)	Attributes		No			No		
	Channels							

Feature	Object	Details	Same Server					
			New			Duplicate		
			Enterprise (from 5)	Sub (from ENT)	Basic (from 6)	Enterprise (from SRC)	Sub (from SRC)	Basic (from SRC)
Standard Organization Configuration	Provider Configuration		Yes			Yes		
	Page Layouts							
	Buttons							
	Gateways and Devices							
	Standard Hierarchy	Org Hierarchy, DL Hierarchy, Emergency Community						
	Standard DLs	Auto Delete Users Auto Disable Users						
	Alert Templates							
	Maps and Layers							

Feature	Object	Details	Same Server					
			New			Duplicate		
			Enterprise (from 5)	Sub (from ENT)	Basic (from 6)	Enterprise (from SRC)	Sub (from SRC)	Basic (from SRC)
Custom Organization Configuration	Attributes		Yes	No	Yes	Yes	Yes	Yes
	Channels		Yes	No	Yes	Yes	Yes	Yes
	Audio		Yes	No	Yes	Yes	Yes	Yes
	Templates		Yes	No	Yes	Yes	Yes	Yes
	Mass Devices		Yes	No	Yes	Yes	Yes	Yes
	Custom DLs	Except Static List User Membership (see Users)	Yes	No	Yes	Yes	Yes	Yes
	Alert Templates	Except Targeting of Individual Users (see Users)	Yes	No	Yes	Yes	Yes	Yes
	Reports		Yes	No	Yes	Yes	Yes	Yes
	Schedules		Yes	No	Yes	Yes	Yes	Yes
	Operator Permissions		Yes	No	Yes	Yes	Yes	Yes
	Users, their DL Memberships and Targeting	Organization Users	No	No	No	No	No	No
		Static DL User Membership	No	No	No	No	No	No
		Alert Templates Individual User Targeting	No	No	No	No	No	No