



BlackBerry AtHoc

Install and Configure BlackBerry AtHoc

7.18

Contents

- Getting started..... 7**
 - How to use this guide.....7
 - System overview.....7
 - AtHoc server.....8
 - Operators (administrators and publishers).....9
 - AtHoc desktop app.....9

- System components and configuration..... 10**
 - Main modules..... 10
 - BlackBerry AtHoc physical configuration..... 10
 - Database server..... 10
 - Application servers..... 10
 - Application servers and common system resources..... 10
 - Support for products, processes, procedures, and protocols..... 11
 - Backups..... 11
 - System maintenance and operation monitoring..... 11
 - Connectivity..... 11
 - IPv6 support..... 12
 - Delivery gateway..... 12

- BlackBerry AtHoc account requirements..... 13**
 - Required group policies..... 13

- Upgrade BlackBerry AtHoc..... 14**
 - Upgrade preparation..... 14
 - Supported upgrade paths..... 14
 - Database server preparation 14
 - All versions preparation steps..... 14
 - Backup critical data..... 14
 - Databases..... 14
 - Alerts and user data..... 14
 - Application server preparation..... 15
 - Stop services..... 15
 - Back up custom code..... 15
 - Back up duplicated device configurations..... 15
 - Database server upgrade..... 15
 - Application server upgrade..... 16

- Postinstallation or upgrade configuration..... 18**
 - Set antivirus file exclusions for database log and tempDB files..... 18
 - Update certificate metadata for AuthServices..... 18
 - IIS postinstallation checklist..... 19

| | |
|---|----|
| Application pool configuration tables..... | 19 |
| (Optional) Enable the TLS 1.2 protocol..... | 42 |
| Application server changes..... | 42 |
| Database server changes..... | 42 |
| (Optional) Configure the application server for Windows authentication..... | 43 |
| (Optional) Configure client certificates on the application server..... | 43 |
| (Optional) Set the SSL client certificate..... | 44 |
| (Optional) Install certificates for cloud delivery services..... | 46 |
| (Optional) Configure new access card formats for operator auto-login..... | 47 |
| Gather information from the customer..... | 47 |
| Update BlackBerry AtHoc management system security policy..... | 47 |
| (Optional) Update the application server registry for smart card login..... | 47 |
| (Optional) Enable FIPS on each application server..... | 48 |
| (Optional) System Archive account requirement..... | 48 |
| Configure .NET framework to use a web proxy..... | 49 |
| (Optional) Restore the XML files for duplicated devices..... | 49 |
| (Optional) Set up error pages for Self Service throttling..... | 50 |
| External error pages for Self Service throttling..... | 50 |

Advanced server configuration.....52

| | |
|--|----|
| Migrate a preinstalled server..... | 52 |
| Stop services..... | 52 |
| Application server changes..... | 52 |
| Start IIS..... | 52 |
| Migrate to an enterprise hierarchy..... | 52 |
| Plan the enterprise hierarchy..... | 52 |
| Best practices..... | 53 |
| Run the Enterprise Migrator tool..... | 54 |
| Migrate organizations to the enterprise..... | 54 |
| Promote user attributes and alert folders..... | 54 |
| What's next?..... | 55 |
| Duplicate organizations across systems..... | 55 |
| Create organizations on the source server..... | 56 |
| Duplicate organizations on the source server..... | 56 |
| Configure AtHoc database operations to use Windows authentication..... | 57 |
| Configure IIS processor affinity..... | 57 |
| Increase the IIS file size upload limit..... | 58 |
| Database recovery setting..... | 59 |

IIS 10.0 Security Technology Implementation Guide..... 60

| | |
|---|----|
| Server STIG..... | 60 |
| IIST-SV-000102: Enable enhanced logging..... | 60 |
| IIST-SV-000103: Enable log file and Event Tracing for windows..... | 60 |
| IIST-SV-000110: Produce log records..... | 61 |
| IIST-SV-000111: Produce log records..... | 61 |
| IIST-SV-000115: Protect log information..... | 62 |
| IIST-SV-000117: Do not perform user management..... | 62 |
| IIST-SV-000118: Contain only necessary functions..... | 63 |
| IIST-SV-000119: Must not be both a website server and a proxy server..... | 63 |
| IIST-SV-000120: Remove code samples, example applications, and tutorials..... | 64 |
| IIST-SV-000121: Delete accounts created by uninstalled features..... | 64 |

| | |
|--|----|
| IIST-SV-000123: Remove unnecessary features, utilities, plug-ins, and modules..... | 64 |
| IIST-SV-000124: Disable MIMEs that invoke OS shell programs..... | 65 |
| IIST-SV-000125: Disable WebDAV..... | 65 |
| IIST-SV-000130: Limit installed Java software..... | 66 |
| IIST-SV-000131: Limit access to only administrative accounts..... | 66 |
| IIST-SV-000134: Use cookies to track session state..... | 66 |
| IIST-SV-000135: Accept only system-generated session identifiers..... | 67 |
| IIST-SV-000138: Disable directory browsing..... | 67 |
| IIST-SV-000139: Index only web content..... | 68 |
| IIST-SV-000140: Modify warning and error messages..... | 68 |
| IIST-SV-000141: Follow access policy..... | 68 |
| IIST-SV-000142: Restrict inbound connections..... | 69 |
| IIST-SV-000144: Conform to minimum file permission requirements..... | 69 |
| IIST-SV-000145: Allocate sufficient log record storage capacity..... | 70 |
| IIST-SV-000147: Restrict access to web administration tools..... | 71 |
| IIST-SV-000149: Disable IPP..... | 71 |
| IIST-SV-000152: Use TLS to send session IDs..... | 72 |
| IIST-SV-000153: Use TLS to maintain confidentiality..... | 72 |
| IIST-SV-000154: Use approved TLS version..... | 73 |
| IIST-SV-000156: Assign passwords..... | 73 |
| IIST-SV-000158: Remove unspecified file extensions..... | 73 |
| IIST-SV-000159: Configure a global authorization rule..... | 74 |
| IIST-SV-000200: Configure the Max Connections setting..... | 74 |
| IIST-SV-000205: Enable HSTS..... | 75 |
| IIST-SV-000160: Require authentication for an SMTP relay..... | 75 |
| Application STIG..... | 75 |
| IIST-SI-000201: Enable session state..... | 76 |
| IIST-SI-000202: Configure session state cookie settings..... | 76 |
| IIST-SI-000206: Enable the log file and ETW..... | 76 |
| IIST-SI-000210: Produce log records containing sufficient information..... | 77 |
| IIST-SI-000214: Disable MIMEs that invoke OS shell programs..... | 77 |
| IIST-SI-000216: Set resource mappings..... | 78 |
| IIST-SI-000217: Disable WebDAV..... | 78 |
| IIST-SI-000221: Restrict anonymous access accounts..... | 79 |
| IIST-SI-000223: Generate unique session identifiers..... | 80 |
| IIST-SI-000224: Separate document directory and system files..... | 80 |
| IIST-SI-000225: Limit the maxURL..... | 80 |
| IIST-SI-000226: Limit the size of web requests..... | 81 |
| IIST-SI-000227: Configure the Maximum Query String limit..... | 81 |
| IIST-SI-000228: Prohibit non-ASCII characters in URLs..... | 82 |
| IIST-SI-000229: Prohibit double encoded URL requests..... | 82 |
| IIST-SI-000231: Disable directory browsing..... | 82 |
| IIST-SI-000233: Modify warning and error messages..... | 83 |
| IIST-SI-000234: Disable debugging and trace information..... | 83 |
| IIST-SI-000238: Use a logging mechanism..... | 84 |
| IIST-SI-000244: Use TLS to send session IDs..... | 84 |
| IIST-SI-000255: Set an application pool recycle time..... | 85 |
| IIST-SI-000257: Enable application pool pinging monitor..... | 85 |
| IIST-SI-000259: Enable application pool rapid fail protection settings..... | 86 |
| IIST-SI-000261: Keep interactive scripts in unique and designated folders..... | 86 |
| IIST-SI-000262: Add restrictive access controls for interactive scripts..... | 87 |
| IIST-SI-000263: Remove backup interactive scripts..... | 88 |
| IIST-SI-000264: Display the required DoD banner page..... | 88 |

| | |
|---|------------|
| IIS 8.5 Security Technology Implementation Guide..... | 90 |
| Server STIG..... | 90 |
| IISW-SV-000103: Enable log file and Event Tracing windows..... | 90 |
| IISW-SV-000107: Sufficient web server log records for location of web server events..... | 90 |
| IISW-SV-000108: Sufficient web server log records for source of web server events..... | 91 |
| IISW-SV-000110: Sufficient web server log records to establish the outcome of web server events..... | 91 |
| IISW-SV-000111: Sufficient web server log records to establish identity..... | 92 |
| IISW-SV-000112: Web server must use Event Tracing for Windows logging option..... | 92 |
| IISW-SV-000120: Samples, examples, and tutorials must be removed from production server..... | 93 |
| IISW-SV-000124: Web server must have MIMEs that invoke OS shell programs disabled..... | 93 |
| IISW-SV-000146: Web server must not impede ability to write log record content to an audit log..... | 94 |
| IISW-SV-000153: Web server must maintain the confidentiality of controlled information during transmission..... | 94 |
| IISW-SV-000154: Web server must maintain the confidentiality of controlled information during transmission..... | 95 |
| Application STIG..... | 95 |
| IISW-SI-000206: Enable log file and Event Tracing windows..... | 96 |
| IISW-SI-000209: Sufficient website log records to establish identity..... | 96 |
| IISW-SI-000210: Sufficient website log records to establish identity..... | 97 |
| IISW-SI-000211: Website must use Event Tracing for Windows logging option..... | 97 |
| IISW-SI-000214: Website must have MIMEs that invoke OS shell programs disabled..... | 98 |
| IISW-SI-000228: Non-ASCII characters in URLs must be prohibited..... | 98 |
| | |
| Verifying BlackBerry AtHoc is operational..... | 100 |
| Basic BlackBerry AtHoc test procedures..... | 100 |
| Extended BlackBerry AtHoc test procedures..... | 105 |
| | |
| Appendix A: Troubleshooting..... | 106 |
| | |
| Appendix B: Organization duplicator object management..... | 108 |
| | |
| BlackBerry AtHoc Customer Support Portal..... | 113 |
| | |
| Documentation feedback..... | 114 |
| | |
| Legal notice..... | 115 |

Getting started

BlackBerry® AtHoc® critical event management is a 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 process.

How to use this guide

Read the overview of BlackBerry AtHoc components and configuration in [Main modules](#), [BlackBerry AtHoc physical configuration](#), and [Support for products, processes, procedures, and protocols](#).

- To upgrade an existing installation, follow the instructions in [Upgrade BlackBerry AtHoc](#) and [Postinstallation or upgrade configuration](#).

For more information about advanced topics, including migrating a pre-installed server, configuring IIS processor affinity, increasing the maximum file upload size, and other topics, see [Advanced server configuration](#).

System overview

The BlackBerry AtHoc critical event management solution is a flexible, commercial software solution for enterprise-class, subscription-based mass communication. The 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

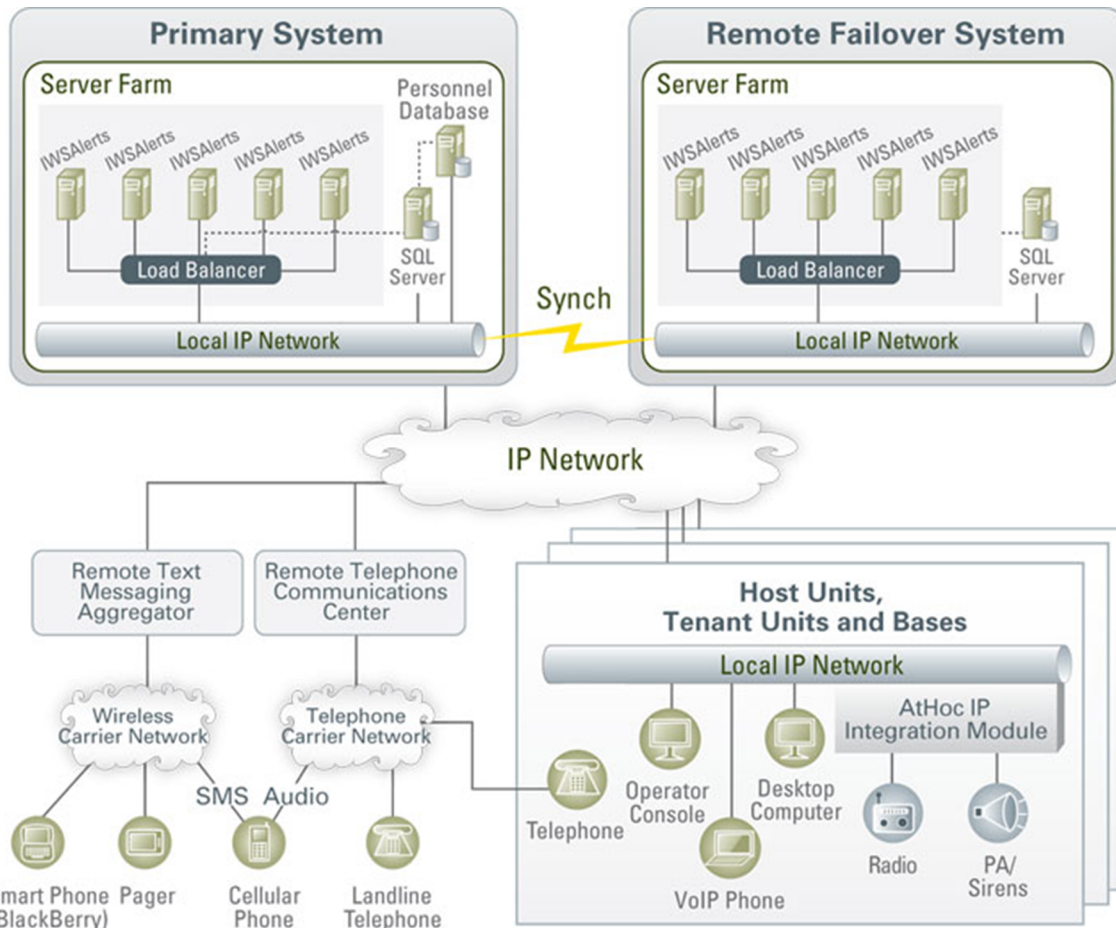


Figure 1: BlackBerry AtHoc system elements

AtHoc server

The AtHoc server does the following:

- 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.
- Integrates 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.


- Provides 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 permissions.

AtHoc desktop app

The AtHoc Desktop App appears as a small purple globe  in the end user's system tray. The AtHoc desktop app serves the following functions in the BlackBerry AtHoc system:

- When new alert content is published, the AtHoc desktop app displays an audio/visual notification as a desktop pop-up.
- Users can dismiss the desktop pop-up, choose a response option (when sent), and click a link to obtain additional information about the emergency condition.
- Additional delivery devices include: web delivery, email, mobile devices, phones, pagers, TTY/TDD devices, SMS, Giant voice, LMR, and instant messaging.
- The BlackBerry AtHoc desktop app can be installed on a Windows or macOS client.

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.

System components and configuration

Main modules

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

- **Database server:** The database server is based on Microsoft SQL Server.
- **Application server (one or more servers):** The application server acts as a web-based application server that provides all user-related interactions. The application server also runs the BlackBerry AtHoc 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 BlackBerry AtHoc desktop app, web browsers, and various delivery gateways such as telephony and SMS. Additionally, the servers provide integration points with enterprise application suites, such as LDAP, Active Directory, HR, and your organization's portals.

In cases where redundancy is needed, a BlackBerry AtHoc disaster recovery solution can be implemented so that notification capabilities can be transferred to an alternate site if the primary BlackBerry AtHoc platform becomes unreachable.

BlackBerry AtHoc physical configuration

Although all server components can be installed on the same server, you should install each server on different servers. The database server should be located on one server, and each application server installed on another server.

Database server

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

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.

You can set up a disaster recovery 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.
- **Microsoft Message Queuing (MSMQ):** BlackBerry AtHoc uses MSMQ to queue 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.

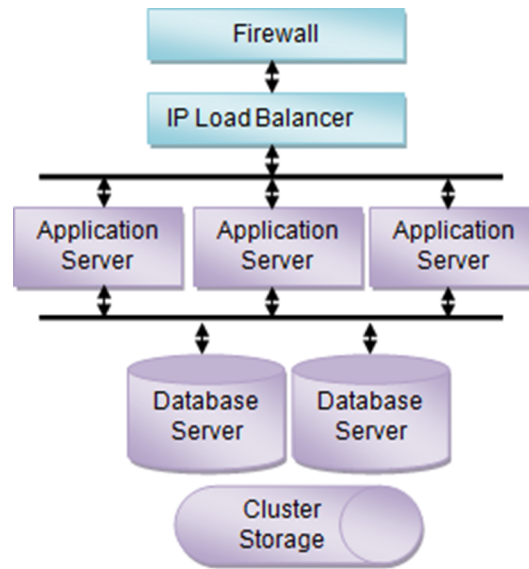


Figure 2: BlackBerry AtHoc physical configuration in a redundant setup (single site)

Support for products, processes, procedures, and protocols

The following third-party components are used to support the BlackBerry AtHoc implementation:

- 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 OpenView and Tivoli.

Connectivity

Connectivity refers to the following items:

- **Local connectivity:** Local connectivity provides the connection between the local computers that BlackBerry AtHoc is installed on. 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 BlackBerry AtHoc desktop app. For HTTPS configuration, a Web PKI certificate must be installed on the web servers.

- **Accessing external HTTP or HTTPS sources:** External HTTP or HTTPS sources are used for integration with external applications and data sources used 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.

IPv6 support

The BlackBerry AtHoc critical event management solution is compatible with IPv6 networks. Both servers and clients can operate in an IPv6-only infrastructure as well as in a hybrid IPv4/IPv6 environment.

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.

BlackBerry AtHoc account requirements

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

Required group policies

The following account policies and their values are the defaults on Windows Server before any changes are made 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 following 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 |

Upgrade BlackBerry AtHoc

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

Upgrade preparation

This section describes the steps that you need to complete before you upgrade to a new release.

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.

All live alerts and events are ended automatically during the upgrade.

Note: Before upgrading to BlackBerry AtHoc release 7.18, upgrade BlackBerry Feed Service (BFS) to version 1.2.

Supported upgrade paths

The supported upgrade path is: 7.17 > 7.18.

Database server preparation

Complete the following preparation tasks to upgrade 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 that the AtHocENS folder and the SQL Server files are located on.
- 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`.

Alerts and user data

- 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 Archive 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.

Application server preparation

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

The following pre-installed Windows components may need to be upgraded:

| Component | Notes |
|---|---|
| .NET Framework v. 4.7.2. | If an earlier version is installed, upgrade to version 4.7.2. If a later version is installed, uninstall it and then install version 4.7.2. |
| dotnet-hosting-6.0.14-win.exe (or latest 6.x.x release) | This version is included in the asp .net hosting bundle which can be found in the AtHoc repo at: .../IWS/Server/7.18.0.0/Prereqs/ |
| Windows PowerShell | Windows PowerShell 5.1 Note: Windows Server 2016 and 2019 include Windows PowerShell 5.1 by default. |

Stop services

- Stop IIS: Set World Wide Web Publishing Service to Manual: `netsh stop w3svc`
- Stop web app workers: `iisreset -stop`

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.

Database server upgrade

1. Run the setup kit on the database server to upgrade it.
2. Download the BlackBerry AtHoc setup kit .zip file to the server.
3. Right-click the setup kit .zip file and select **Properties** > **General** > **Unblock** to unblock the file.
4. Extract the contents of the setup kit .zip file into a temporary directory.

Important: Due to Windows OS file path length limitations, some of the included utilities may not extract correctly. To avoid this issue, use a short path for the extraction directory. For example, `C:\setup`. Keep the total number of characters to 20 or less, including the drive letter, colon, and slashes.

5. Use the `<setupkit_root>/user.yml` configuration file to provide product-specific setup parameters.

This file is included in the setup kit as a template with blocks of related parameters that are commented out and a brief description for each block. To use the parameters in a block, remove the # from the parameter, update it, and save the file.

Note: YAML is indent-sensitive. When you remove the # from a parameter in the block, make sure that you keep the original indentation. You must also remove the # from the block header, even if you update only one parameter in the block. You can validate the YAML at <https://yaml-online-parser.appspot.com/> before you save the file.

Uncomment the following lines in the user.yml file:

```
selected_roles:
- db

args:
  user_input: user.yml

  sql_server_instance: .
  db_name: ngaddata

  admin_db_auth: sql
  admin_db_user: 'sa'
  admin_db_pw: '<password>'

  app_db_auth: sql
  app_db_user: ngad
  app_db_pw: <password>

  db_dir: C:\Program Files (x86)\AtHocENS\Database
  db_log_dir: C:\Program Files (x86)\AtHocENS\Database\Log
  db_archive_dir: C:\Program Files (x86)\AtHocENS\Database\Archive
  app_dir: C:\Program Files (x86)\AtHocENS

  system_url: https://<hostname>.athocdevo.com
```

6. Do one of the following:
 - a. Right-click the SetupKit.exe file from the root folder and run as an administrator.
 - b. Run Windows PowerShell as an administrator and then run the .\SetupKit.exe script to upgrade the AtHoc database server.
7. The SetupKit.exe file starts the installation process and completes the following tasks:
 - Parses setup parameters from the user.yml file.
 - Creates log directory and writes to log files.
 - Installs each product in the following order: database, application, support modules.
 - Reports result and elapsed time.

When the upgrade is complete, the BlackBerry AtHoc is database installed and running.

Application server upgrade

Note: If you update the application and database servers on separate servers, you must run the AtHoc setup kit once on each application server.

1. Download the BlackBerry AtHoc setup kit .zip file to the server.
2. Right-click the setup kit .zip file and select **Properties** > **General** > **Unblock** to unblock the file.
3. Extract the contents of the setup kit .zip file into a temporary directory.

Important: Due to Windows OS file path length limitations, some of the included utilities may not extract correctly. To avoid this issue, use a short path for the extraction directory. For example, C:\setup. Keep the total number of characters to 20 or less, including the drive letter, colon, and slashes.

4. Use the `<setupkit_root>/user.yml` configuration file to provide product-specific setup parameters.

This file is included in the setup kit as a template with blocks of related parameters that are commented out and a brief description for each block. To use the parameters in a block, remove the `#` from the parameter, update it, and save the file.

Note: YAML is indent-sensitive. When you remove the `#` from a parameter in the block, make sure that you keep the original indentation. You must also remove the `#` from the block header, even if you update only one parameter in the block. You can validate the YAML at <https://yaml-online-parser.appspot.com/> before you save the file.

Uncomment the following lines in the `user.yml` file:

```
selected_roles:
- app
args:
  user_input: user.yml

  sql_server_instance: <sql-instance>.athocdevo.com
  db_name: ngaddata

  app_db_auth: sql
  app_db_user: ngad
  app_db_pw: <password>
```

5. Do one of the following:
 - a. Right-click the `SetupKit.exe` file from the root folder and run as an administrator.
 - b. Run Windows PowerShell as an administrator and then run the `.\SetupKit.exe` script to upgrade the AtHoc application server.
6. The `SetupKit.exe` file starts the upgrade process and completes the following tasks:
 - Parses setup parameters from the `user.yml` file.
 - Creates log directory and writes to log files.
 - Upgrades each product in the following order: database, application, support modules.
 - Reports result and elapsed time.

When the upgrade is complete, BlackBerry AtHoc is upgraded and running.

Postinstallation or upgrade configuration

This chapter describes component configurations that are performed after BlackBerry AtHoc is installed. There is no recommended order to the tasks described in this section.

Set antivirus file exclusions for database log and tempDB files

Real-time antivirus 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`.
- The SQL MDF database and the LDF log files.

Update certificate metadata for AuthServices

The `appsettings` configuration schema for `AuthServices` was changed in BlackBerry AtHoc release 7.11 to enable obtaining self-signed certificates from the Windows Certificate Store or invalid certificates from third-party vendors. Due to this change, the certificate metadata in the `appsettings.json` file must be modified after deployment.

Tip: You can still obtain the certificate from the Windows Certificate Store or from a disk. Set the `ValidCertsOnly` parameter to `false` to obtain self-signed and invalid certificates.

1. Obtain a valid certificate.
2. Import the valid certificate to the WINDOWS local store.
3. Open the certificate file and capture the Thumbprint and Passcode.
4. Open the `appsettings.json` file found at `AtHocENS\wwwroot\AuthServices\Auth\appsettings.json`.

It is possible to add multiple certificate files, but you should add only one certificate file.

5. Update the `appsettings.json` file with one of the following:
 - To configure the certificate from a file system, use the following text:

```
        {"Logging": {
          "IncludeScopes": false,
          "LogLevel": {
            "Default": "Error", // Trace, Debug, Information, Warning,
Error, Critical,
          None
          "System": "Information",
          "Microsoft": "Information"
        }
      },
      "Certificates": [
        {
          "CertificateLocation": "FileSystem", // Location:
FileSystem,
CertificateStore
```

```

        "RelativeFilePath": ".\\wwwroot\\Certificates\\
\\TokenSigningCertificate.pfx",
        "Passcode": "<passcode>"
    },
],
"AllowedHosts": "*" }

```

- To configure the certificate from the Windows Certificate Store, use the following text:

```

    { "Logging": {
      "IncludeScopes": false,
      "LogLevel": {
        "Default": "Error", // Trace, Debug, Information, Warning,
Error, Critical,
None
        "System": "Information",
        "Microsoft": "Information"
      }
    },
    "Certificates": [
      {
        "CertificateLocation": "CertificateStore",
        "StoreName": "Root", // My (Personal), Root (Trusted
Root), AddressBook,
AuthRoot, CertificateAuthority, TrustedPeople,
TrustedPublisher, Disallowed
        "StoreLocation": "LocalMachine", // CurrentUser,
LocalMachine
        "Thumbprint": "<thumbprint>",
        "Passcode": "<passcode>",
        "ValidCertsOnly": true // for getting debug or
development certificates
      }
    ],
    "AllowedHosts": "*" }

```

6. Update the values for Thumbprint and Passcode with the values you captured in Step 3.
7. Save and close the appsettings.json file.

IIS postinstallation checklist

After you install BlackBerry AtHoc, verify the following settings in IIS.

Note: In multiple application server environments, you must manually restart IIS on each application server after all application servers and the database have been upgraded.

Application pool configuration tables

The installation configures application pools using the settings described in the following sections. The configurations of the application pools are described in the following tables:

- [Table 1: Application pool configuration](#)
- [Table 2: Application Pool - Web application associations for the AtHoc website - Enterprise configuration](#)
- [Table 3: AtHoc services application pool configuration](#)
- [Table 4: Application pools - web application association for AtHoc services web site](#)

Table 1: Application pool configuration

Table 1a: General, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|----------------------------|------------------------------------|--------------------|--------------------|-------------------------------|--------------------|
| General | | | | | |
| .NET framework version | No Managed code | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 |
| Enable 32-bit applications | True | True | True | False | True |
| Managed pipeline mode | Integrated | Classic | Classic | Integrated | Classic |
| Queue length | 65535 | 1000 | 65535 | 65535 | 65535 |
| Start automatically | AlwaysRunning | AlwaysRunning | AlwaysRunning | AlwaysRunning | AlwaysRunning |

Table 1a: General, part 2

| | AtHoc IWS pool | AtHoc management system pool | AtHoc SDK pool |
|----------------------------|--------------------|------------------------------|--------------------|
| General | | | |
| .NET framework version | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 |
| Enable 32-bit applications | True | True | True |
| Managed pipeline mode | Integrated | Classic | Classic |
| Queue length | 65535 | 65535 | 1000 |
| Start automatically | AlwaysRunning | AlwaysRunning | AlwaysRunning |

Table 1a: General, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|----------------------------|-------------------------|--------------------|---------------------------------|
| General | | | |
| .NET framework version | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 |
| Enable 32-bit applications | True | True | True |
| Managed pipeline mode | Integrated | Integrated | Integrated |
| Queue length | 65535 | 1000 | 65535 |
| Start automatically | AlwaysRunning | AlwaysRunning | AlwaysRunning |

Table 1b: CPU, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|----------------------------|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| CPU | | | | | |
| Limit | 0 | 0 | 0 | 0 | 0 |
| Limit action | NoAction | NoAction | NoAction | NoAction | NoAction |
| Limit interval (minutes) | 5 | 5 | 5 | 5 | 5 |
| Processor affinity enabled | False | False | False | False | False |
| Processor affinity mask | 4294967295 | 4294967295 | 4294967295 | 4294967295 | 4294967295 |

Table 1b: CPU, part 2

| | AtHoc IWS pool | AtHoc management system pool | AtHoc SDK pool |
|--------------------------|----------------|------------------------------|----------------|
| CPU | | | |
| Limit | 0 | 0 | 0 |
| Limit action | NoAction | NoAction | NoAction |
| Limit interval (minutes) | 5 | 5 | 5 |

| | AtHoc IWS pool | AtHoc management system pool | AtHoc SDK pool |
|----------------------------|----------------|------------------------------|----------------|
| CPU | | | |
| Processor affinity enabled | False | False | False |
| Processor affinity mask | 4294967295 | 4294967295 | 4294967295 |

Table 1b: CPU, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|----------------------------|-------------------------|--------------------|---------------------------------|
| CPU | | | |
| Limit | 30 | 0 | 0 |
| Limit action | Throttle | NoAction | NoAction |
| Limit interval (minutes) | 5 | 5 | 5 |
| Processor affinity enabled | False | False | False |
| Processor affinity mask | 4294967295 | 4294967295 | 4294967295 |

Table 1c: Process model, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|------------------------------------|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| Process model | | | | | |
| Identity (ApplicationPoolIdentity) | – | – | – | – | – |
| Idle time-out (minutes) | 0 | 0 | 0 | 0 | 0 |
| Load user profile | True | True | True | True | True |
| Maximum worker processes | 1 | 1 | 1 | 2 | 2 |
| Ping enabled | True | True | True | True | True |

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|--------------------------------------|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| Process model | | | | | |
| Ping maximum response time (seconds) | 90 | 90 | 90 | 90 | 90 |
| Ping period (seconds) | 30 | 30 | 30 | 30 | 30 |
| Shutdown time limit (seconds) | 90 | 90 | 90 | 90 | 90 |
| Startup time limit (seconds) | 90 | 90 | 90 | 90 | 90 |

Table 1c: Process model, part 2

| | AtHoc IWS pool | AtHocmanagement system pool | AtHoc SDK pool |
|--------------------------------------|----------------|-----------------------------|----------------|
| Process model | | | |
| Identity (ApplicationPoolIdentity) | | — | — |
| Idle time-out (minutes) | 0 | 0 | 0 |
| Load user profile | True | True | True |
| Maximum worker processes | 1 | 1 | 1 |
| Ping enabled | True | True | True |
| Ping maximum response time (seconds) | 90 | 90 | 90 |
| Ping period (seconds) | 30 | 30 | 30 |
| Shutdown time limit (seconds) | 90 | 90 | 90 |
| Startup time limit (seconds) | 90 | 90 | 90 |

Table 1c: Process model, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|--------------------------------------|-------------------------|--------------------|---------------------------------|
| Process model | | | |
| Identity (ApplicationPoolIdentity) | | – | – |
| Idle time-out (minutes) | 0 | 0 | 0 |
| Load user profile | True | True | True |
| Maximum worker processes | 2 | 1 | 1 |
| Ping enabled | True | True | True |
| Ping maximum response time (seconds) | 90 | 90 | 90 |
| Ping period (seconds) | 30 | 30 | 30 |
| Shutdown time limit (seconds) | 90 | 90 | 90 |
| Startup time limit (seconds) | 90 | 90 | 90 |

Table 1d: Process Orphaning, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|--------------------------|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| Process orphaning | | | | | |
| Enabled | False | False | False | False | False |
| Executable | – | – | – | – | – |
| Executable parameters | – | – | – | – | – |

Table 1d: Process orphaning, part 2

| | AtHoc IWS pool | AtHoc management system pool | AtHoc SDK pool |
|--------------------------|----------------|------------------------------|----------------|
| Process orphaning | | | |
| Enabled | False | False | False |
| Executable | — | — | — |
| Executable parameters | — | — | — |

Table 1d: Process orphaning, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|--------------------------|-------------------------|--------------------|---------------------------------|
| Process orphaning | | | |
| Enabled | False | False | False |
| Executable | — | — | — |
| Executable parameters | — | — | — |

Table 1e: Rapid-fail protection, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|-------------------------------------|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| Rapid-fail protection | | | | | |
| "Service Unavailable" response type | HttpLevel | HttpLevel | HttpLevel | HttpLevel | HttpLevel |
| Enabled | False | False | False | False | False |
| Failure Interval (minutes) | 5 | 5 | 5 | 5 | 5 |
| Max Failures | 5 | 5 | 5 | 5 | 5 |
| Shutdown Executable | — | — | — | — | — |
| Shutdown Executable Parameters | — | — | — | — | — |

Table 1e, Rapid-fail protection, part 2

| | AtHoc IWS pool | AtHoc management system pool | AtHoc SDK pool |
|-------------------------------------|----------------|------------------------------|----------------|
| Rapid-fail protection | | | |
| "Service Unavailable" response type | HttpLevel | HttpLevel | HttpLevel |
| Enabled | False | False | False |
| Failure interval (minutes) | 5 | 5 | 5 |
| Max failures | 5 | 5 | 5 |
| Shutdown executable | — | — | — |
| Shutdown executable parameters | — | — | — |

Table 1e, Rapid-fail protection, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|-------------------------------------|-------------------------|--------------------|---------------------------------|
| Rapid-fail protection | | | |
| "Service Unavailable" response type | HttpLevel | HttpLevel | HttpLevel |
| Enabled | False | False | False |
| Failure interval (minutes) | 5 | 5 | 5 |
| Max failures | 5 | 5 | 5 |
| Shutdown executable | — | — | — |
| Shutdown executable parameters | — | — | — |

Table 1f: Recycling, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|--|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| Recycling | | | | | |
| Disable overlapped recycle | False | False | False | False | False |
| Disable recycling for configuration change | False | False | False | False | False |

Table 1f: Recycling, part 2

| | AtHoc IWS pool | AtHoc management system pool | AtHoc SDK pool |
|--|----------------|------------------------------|----------------|
| Recycling | | | |
| Disable overlapped recycle | False | False | False |
| Disable recycling for configuration change | False | False | False |

Table 1f: Recycling, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|--|-------------------------|--------------------|---------------------------------|
| Recycling | | | |
| Disable overlapped recycle | False | False | False |
| Disable recycling for configuration change | False | False | False |

Table 1g: Generate recycle event log entry, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|---|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| Generate recycle event log entry | | | | | |
| Application pool configuration changed | False | False | False | False | False |
| Isapi reported unhealthy | False | False | False | False | False |
| Manual recycle | False | False | False | False | False |
| Private memory limit exceeded | True | True | True | True | True |
| Regular time interval | True | True | True | True | True |
| Request limit exceeded | False | False | False | False | False |
| Specific time | False | False | False | False | False |
| Virtual memory limit exceeded | True | True | True | True | True |
| Private memory limit (KB) | 1800000 | 1800000 | 1800000 | 1800000 | 1800000 |
| Regular time interval (minutes) | 0 | 0 | 0 | 0 | 0 |
| Request limit | 0 | 0 | 0 | 0 | 0 |

Table 1g: Generate Recycle Event Log Entry, part 2

| | AtHoc IWS pool | AtHoc AtHoc management system | AtHoc SDK pool |
|---|----------------|-------------------------------|----------------|
| Generate recycle event log entry | | | |
| Application pool configuration changed | False | False | False |
| Isapi reported unhealthy | False | False | False |
| Manual recycle | False | False | False |
| Private memory limit exceeded | True | True | True |
| Regular time interval | True | True | True |
| Request limit exceeded | False | False | False |
| Specific time | False | False | False |
| Virtual memory limit exceeded | True | True | True |
| Private memory limit (KB) | 1800000 | 1800000 | 1800000 |
| Regular time interval (minutes) | 0 | 0 | 0 |
| Request limit | 0 | 0 | 0 |

Table 1g: Generate Recycle Event Log Entry, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|---|-------------------------|--------------------|---------------------------------|
| Generate recycle event log entry | | | |
| Application pool configuration changed | False | False | False |
| Isapi reported unhealthy | False | False | False |
| Manual recycle | False | False | False |
| Private memory limit exceeded | True | True | True |
| Regular time interval | True | True | True |
| Request limit exceeded | False | False | False |

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|---|-------------------------|--------------------|---------------------------------|
| Generate recycle event log entry | | | |
| Specific time | False | False | False |
| Virtual memory limit exceeded | True | True | True |
| Private memory limit (KB) | 1800000 | 1800000 | 1800000 |
| Regular time interval (minutes) | 0 | 0 | 0 |
| Request limit | 0 | 0 | 0 |

Table 1h: Specific times, part 1

| | AtHoc auth services .NET core pool | AtHoc D911 pool | AtHoc default pool | AtHoc desktop integrated pool | AtHoc desktop pool |
|---------------------------|------------------------------------|-----------------|--------------------|-------------------------------|--------------------|
| Specific times | | | | | |
| [0] | 01:38:00 | 01:33:00 | 01:34:00 | 01:34:00 | 01:36:00 |
| Virtual memory limit (KB) | 0 | 0 | 0 | 0 | 0 |

Table 1h: Specific times, part 2

| | AtHoc IWS pool | AtHoc management system pool | AtHoc SDK pool |
|---------------------------|----------------|------------------------------|----------------|
| Specific times | | | |
| [0] | 01:36:00 | 01:33:00 | 01:35:00 |
| Virtual Memory Limit (KB) | 0 | 0 | 0 |

Table 1h: Specific times, part 3

| | AtHoc Self Service pool | AtHoc web API pool | AtHoc web API v2 .NET core pool |
|---------------------------|-------------------------|--------------------|---------------------------------|
| Specific times | | | |
| [0] | 01:33:00 | 01:35:00 | 01:38:00 |
| Virtual Memory Limit (KB) | 0 | 0 | 0 |

Table 2: Application Pool - Web application associations for the AtHoc website - Enterprise configuration

| Web application | Associated application pool |
|--------------------|------------------------------------|
| api\ v1 | AtHoc WebAPI pool |
| api\ v2 | AtHoc WebAPI v2 .NET core pool |
| ast | AtHoc default pool |
| athoc-cdn | AtHoc IWS pool |
| athoc-iws | AtHoc IWS pool |
| AuthServices\ Auth | AtHoc auth services .NET core pool |
| CascadeAlertAgent | AtHoc default pool |
| client | AtHoc management system pool |
| config | AtHoc desktop integrated pool |
| csi | AtHoc desktop integrated pool |
| D911Server | AtHoc D911 pool |
| Data | AtHoc default pool |
| DataExport | AtHoc default pool |
| EasyConnect | AtHoc default pool |
| EmailResponse | AtHoc Self Service pool |
| Graphics | AtHoc default pool |
| Monitor | AtHoc default pool |
| Redirector | AtHoc default pool |
| SelfService | AtHoc Self Service pool |

| Web application | Associated application pool |
|-----------------|-------------------------------|
| sdk | AtHoc SDK pool |
| sps | AtHoc desktop integrated pool |
| sso | AtHoc default pool |
| Syndication | AtHoc Syndication pool |
| TwitterConfig | AtHoc default pool |
| wis | AtHoc desktop pool |

Table 3: AtHoc services application pool configuration

Table 3: AtHoc services application pool configuration, part 1

| | AtHoc alert coordinator pool | AtHoc delivery coordinator pool | AtHoc tracking processor pool | AtHoc regular scheduler pool | AtHoc advanced scheduler pool |
|----------------------------|------------------------------|---------------------------------|-------------------------------|------------------------------|-------------------------------|
| General | | | | | |
| .NET framework version | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 |
| Enable 32-bit applications | True | True | True | True | True |
| Managed pipeline mode | Integrated | Integrated | Integrated | Integrated | Integrated |
| Queue length | 1000 | 1000 | 1000 | 1000 | 1000 |
| Start automatically | AlwaysRunning | AlwaysRunning | AlwaysRunning | AlwaysRunning | AlwaysRunning |
| CPU | | | | | |
| Limit | 0 | 0 | 0 | 0 | 0 |
| Limit action | NoAction | NoAction | NoAction | NoAction | NoAction |
| Limit interval (minutes) | 5 | 5 | 5 | 5 | 5 |
| Processor affinity enabled | False | False | False | False | False |

| | AtHoc alert coordinator pool | AtHoc delivery coordinator pool | AtHoc tracking processor pool | AtHoc regular scheduler pool | AtHoc advanced scheduler pool |
|--------------------------------------|------------------------------|---------------------------------|-------------------------------|------------------------------|-------------------------------|
| Processor affinity mask | 4294967295 | 4294967295 | 4294967295 | 4294967295 | 4294967295 |
| Process model | | | | | |
| Identity ¹ | – | – | – | – | – |
| Idle time-out (minutes) | 0 | 0 | 0 | 0 | 0 |
| Load user profile | True | True | True | True | True |
| Maximum worker processes | 1 | 1 | 1 | 1 | 1 |
| Ping enabled | True | True | True | True | True |
| Ping maximum response time (seconds) | 90 | 90 | 90 | 90 | 90 |
| Ping period (seconds) | 30 | 30 | 30 | 30 | 30 |
| Shutdown time limit (seconds) | 90 | 90 | 90 | 90 | 90 |
| Startup time limit (seconds) | 90 | 90 | 90 | 90 | 90 |
| Process orphaning | | | | | |
| Enabled | False | False | False | False | False |
| Executable | – | – | – | – | – |
| Executable parameters | – | – | – | – | – |
| Rapid-fail protection | | | | | |
| "Service Unavailable" response type | HttpLevel | HttpLevel | HttpLevel | HttpLevel | HttpLevel |
| Enabled | False | False | False | False | False |

| | AtHoc alert coordinator pool | AtHoc delivery coordinator pool | AtHoc tracking processor pool | AtHoc regular scheduler pool | AtHoc advanced scheduler pool |
|--|------------------------------|---------------------------------|-------------------------------|------------------------------|-------------------------------|
| Failure interval (minutes) | 5 | 5 | 5 | 5 | 5 |
| Max failures | 5 | 5 | 5 | 5 | 5 |
| Shutdown executable | – | – | – | – | – |
| Shutdown executable parameters | – | – | – | – | – |
| Recycling | | | | | |
| Disable overlapped recycle | True | True | True | True | True |
| Disable recycling for configuration change | False | False | False | False | False |
| Generate recycle event log entry | | | | | |
| Application pool configuration changed | False | False | False | False | False |
| Isapi reported unhealthy | False | False | False | False | False |
| Manual recycle | False | False | False | False | False |
| Private memory limit exceeded | True | True | True | True | True |
| Regular time interval | True | True | True | True | True |
| Request limit exceeded | False | False | False | False | False |
| Specific time | False | False | False | False | False |
| Virtual memory limit exceeded | True | True | True | True | True |

| | AtHoc alert coordinator pool | AtHoc delivery coordinator pool | AtHoc tracking processor pool | AtHoc regular scheduler pool | AtHoc advanced scheduler pool |
|---------------------------------|------------------------------|---------------------------------|-------------------------------|------------------------------|-------------------------------|
| Private memory limit (KB) | 800000 | 800000 | 800000 | 800000 | 800000 |
| Regular time interval (minutes) | 0 | 0 | 0 | 0 | 0 |
| Request limit | 0 | 0 | 0 | 0 | 0 |
| Specific times | | | | | |
| [0] | 04:30:00 | 04:30:00 | 04:30:00 | 04:30:00 | 04:30:00 |
| Virtual memory limit (KB) | 0 | 0 | 0 | 0 | 0 |

¹ ApplicationPoolIdentity

Table 3: AtHoc services application pool configuration, part 2

| | AtHoc PSS polling agent pool | AtHoc tracking summary coordinator pool | AtHoc batch coordinator pool | AtHoc user termination coordinator pool |
|----------------------------|------------------------------|---|------------------------------|---|
| General | | | | |
| .NET framework version | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 | v4.7.2 and v6.0.10 |
| Enable 32-bit applications | True | True | True | True |
| Managed pipeline mode | Integrated | Integrated | Integrated | Integrated |
| Queue length | 1000 | 1000 | 1000 | 1000 |
| Start automatically | AlwaysRunning | AlwaysRunning | AlwaysRunning | AlwaysRunning |
| CPU | | | | |
| Limit | 0 | 0 | 0 | 0 |
| Limit action | NoAction | NoAction | NoAction | NoAction |
| Limit interval (minutes) | 5 | 5 | 5 | 5 |

| | AtHoc PSS polling agent pool | AtHoc tracking summary coordinator pool | AtHoc batch coordinator pool | AtHoc user termination coordinator pool |
|--|---------------------------------|---|---------------------------------|---|
| Processor affinity Enabled | False | False | False | False |
| Processor affinity mask | 4294967295 | 4294967295 | 4294967295 | 4294967295 |
| Process model | | | | |
| Identity ¹ | – | – | – | – |
| Idle time-out (minutes) | 0 | 0 | 0 | 0 |
| Load user profile | True | True | True | True |
| Maximum worker processes | 1 | 1 | 1 | 1 |
| Ping enabled | True | True | True | True |
| Ping maximum response time (seconds) | 90 | 90 | 90 | 90 |
| Ping period (seconds) | 30 | 30 | 30 | 30 |
| Shutdown time limit (seconds) | 90 | 90 | 90 | 90 |
| Startup time limit (seconds) | 90 | 90 | 90 | 90 |
| Process orphaning | | | | |
| Enabled | False | False | False | False |
| Executable | – | – | – | – |
| Executable parameters | – | – | – | – |
| Rapid-fail protection | | | | |
| "Service Unavailable" response type | HttpLevel | HttpLevel | HttpLevel | HttpLevel |

| | AtHoc PSS polling agent pool | AtHoc tracking summary coordinator pool | AtHoc batch coordinator pool | AtHoc user termination coordinator pool |
|--|---------------------------------|---|---------------------------------|---|
| Enabled | False | False | False | False |
| Failure interval (minutes) | 5 | 5 | 5 | 5 |
| Max failures | 5 | 5 | 5 | 5 |
| Shutdown executable | – | – | – | – |
| Shutdown executable Parameters | – | – | – | – |
| Recycling | | | | |
| Disable overlapped recycle | True | True | True | True |
| Disable recycling for configuration change | False | False | False | False |
| Generate recycle event log entry | | | | |
| Application pool configuration changed | False | False | False | False |
| Isapi reported unhealthy | False | False | False | False |
| Manual recycle | False | False | False | False |
| Private memory limit Exceeded | True | True | True | True |
| Regular time interval | True | True | True | True |
| Request limit exceeded | False | False | False | False |
| Specific time | False | False | False | False |
| Virtual memory limit exceeded | True | True | True | True |

| | AtHoc PSS polling agent pool | AtHoc tracking summary coordinator pool | AtHoc batch coordinator pool | AtHoc user termination coordinator pool |
|---------------------------------|------------------------------|---|------------------------------|---|
| Private memory limit (KB) | 800000 | 800000 | 800000 | 800000 |
| Regular time interval (minutes) | 0 | 0 | 0 | 0 |
| Request limit | 0 | 0 | 0 | 0 |
| Specific times | | | | |
| [0] | 04:30:00 | 04:30:00 | 04:30:00 | 04:30:00 |
| Virtual memory limit (KB) | 0 | 0 | 0 | 0 |

Table 4: Application pools - web application association for AtHoc services web site

| Web application | Associated application pool |
|------------------------------|---|
| Advanced scheduler | AtHoc advanced scheduler pool |
| Alert coordinator | AtHoc alert coordinator pool |
| Batch coordinator | AtHoc batch coordinator pool |
| Delivery coordinator | AtHoc delivery coordinator pool |
| PSS polling agent | AtHoc PSS polling agent pool |
| Regular scheduler | AtHoc regular scheduler pool |
| Tracking processor | AtHoc tracking processor pool |
| Tracking summary coordinator | AtHoc tracking summary coordinator pool |

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 |

| Handler name | Path | Description |
|---|----------|----------------------------|
| 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 v4.7.2 (x64) and v6.0.10 (x64) in the Allowed category. |
| | Default web site | Ensure the default web site points to the <AtHocENS \wwwroot> folder. |

| ✓ | Item | Description |
|---|---------------------|---|
| | Virtual directories | <p>The AtHoc website must contain the following virtual directories:</p> <ul style="list-style-type: none"> • Data: Points to <AtHocENS>\CommonSiteData\AtHocData • Graphics: Points to <AtHocENS>\CommonSiteData\Graphics |
| | Web applications | <p>The AtHoc website must contain the following Web applications:</p> <ul style="list-style-type: none"> • api <ul style="list-style-type: none"> • v1 • v2 • ast • athoc-cdn • athoc-iws • AuthServices - Auth • CascadeAlertAgent • client • config • csi • D911Server • Data • DataExport • EasyConnect • EmailResponse • errorpages • Graphics • gw • help • icons • images • include • monitor • redirector • sdk • selfservice • sps • sso • syndication • temp • twitterconfig • user • wis |

| ✓ | Item | Description |
|---|---------------------------|--|
| | ASP.NET version | All Web applications must point to the ASP.Net 4.7.2 and 6.0.10 versions. IIS 7: this is set in the Basic or Advanced settings of each Application Pool. |
| | Application pools | <p>The following application pools are created during the application server installation and must be present:</p> <ul style="list-style-type: none"> • DefaultAppPool • AtHoc Advanced Scheduler Pool • AtHoc Alert Coordinator Pool • AtHoc Auth Services .Net Core pool • AtHoc Batch Coordinator Pool • AtHoc D911 Pool • AtHoc Default Pool • AtHoc Delivery Coordinator Pool • AtHoc Desktop Integrated Pool • AtHoc Desktop Pool • AtHoc IWS Pool • AtHoc Management System Pool • AtHoc PSS Polling Agent Pool • AtHoc Regular Scheduler Pool • AtHoc SDK Pool • AtHoc Self Service Pool • AtHoc Syndication Pool • AtHoc Tracking Processor Pool • AtHoc Tracking Summary Coordinator Pool • AtHoc User Termination Coordinator Pool • AtHoc WebAPI Pool • AtHoc WebAPI v2 .Net Core Pool |
| | Integrated Weather Alerts | Verify that the internal routing from the application server to the domain name (https://api.weather.gov/alerts/active) is functioning correctly over HTTP. |
| | MIME types | <p>Verify that the following MIME types exist:</p> <ul style="list-style-type: none"> • .mp4, video/mp4 • .webm, video/webm • .woff, application/x-wor |

| ✓ | Item | Description |
|---|------------------|--|
| | AtHoc services | <ul style="list-style-type: none"> • Advanced Scheduler • Alert Coordinator • Batch Coordinator • Delivery Coordinator • PSS Polling Agent • Regular Scheduler • Tracking Processor • Tracking Summary Coordinator • User Termination Coordinator |
| | Response headers | <p>There are six response headers for Default Web Site:</p> <ul style="list-style-type: none"> • 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. |

(Optional) Enable the TLS 1.2 protocol

BlackBerry AtHoc is fully TLS 1.2 compliant. If needed, TLS 1.2 can be enabled for inbound and outbound network connections on both the application and database servers.

Application server changes

After TLS 1.2 is enabled and enforced for inbound and outbound network connections on all AtHoc application servers, complete the following tasks on each application server:

1. Copy the registry script `AtHoc_AppServer_Win2016_TLS1.2.reg` (for Windows Server 2016) or `AtHoc_AppServer_Win2019_TLS1.2.reg` (for Windows Server 2019 with cumulative updates) available under the `PostUpgrade\TLS1.2` folder to a local folder on the application server and double click to run it. It is important that the correct registry script based on AtHoc application server OS version (Microsoft Server 2016 or 2019) is run, to make necessary registry entries only after enabling and enforcing TLS 1.2 on the application server.
2. Reboot the application server.

Database server changes

Microsoft SQL Server 2016 and 2019 (with cumulative updates) support TLS 1.2 out-of-the-box and no further update is needed. If you have Microsoft SQL Server 2014 installed, go to the following URL to install and update your software to support TLS 1.2:

<https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server>

Verify the database connection encryption state. Run the following SQL as a system administrator to view the SQL connections state. The encrypt_option column should display TRUE for all records:

```
select encrypt_option, count(*) FROM sys.dm_exec_connections group by
encrypt_option
go
SELECT * FROM sys.dm_exec_connections order by connect_time desc
go
```

(Optional) Configure the application server for Windows authentication

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. Modify the anonymous user identity to use the new logon.
4. Change the OleDbConnectionString. Change "User Id=ngad;Password=@THOC123;" to "Integrated Security=SSPI;".

For more information, see [Configure AtHoc database operations to use Windows authentication](#) in the "Advanced Server configuration" section.

(Optional) Configure client certificates on the application server

These steps 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**.

The Certificate snap-ins dialog opens.
 - c. Select **Computer account** and click **Next**.
 - d. Select **Local Computer**.
 - 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.

Note: Wizard notes

- The certificate that you import must 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 the following note after the **Valid from** field: You have a private key that corresponds to this certificate.

7. Repeat this process for each application server.

When you configure the AtHoc 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 smart card 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.

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** option under client certificates. Use the recommendations for each folder, provided in the table below.
4. Click **Apply**.

The following table provides a reference for client certificate settings for 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 | Ignore |
| ast | Require |
| athoc-cdn | Require |
| athoc-iws | Require |
| AuthConfig | Ignore |
| CascadeAlertAgent | Require |
| client ¹ | Require |

| Application or virtual directory | SSL client certificates |
|--|---|
| config ² | Ignore if you have desktop clients deployed. Require if not. |
| csi ² | Ignore if you have desktop clients deployed. Require if not. |
| D911Server | Require |
| Data | Require |
| DataExport | Require |
| Default Web Site | Require |
| EasyConnect | Require |
| EmailResponse | Require |
| Help | Require |
| Graphics ² | Ignore if you have desktop clients deployed. Require if not. |
| Gw | Require |
| Icons | Require |
| Images | Require |
| Include | Require |
| Integrated Weather Alerts ³ | Require |
| monitor | Ignore if your web server monitoring solution will not work with client certificates. Require if it does. |
| Redirector | Require |
| sdk | Ignore if your custom code integration does not support client certificates. Require if it does. |
| SelfService | Require |
| Self Service/AuthWin | Require |
| sps ² | Ignore if you have desktop clients deployed. Require if not. |
| Sso | Require |

| Application or virtual directory | SSL client certificates |
|----------------------------------|---|
| Syndication | Require if your IIM devices have client certificates installed, or If no IIM devices are deployed. Ignore if not. |
| TwitterConfig | Require |
| User | 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. You should disable this monitor in this configuration.
2. If `config`, `csi`, `Graphics`, and `sps` 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.
 - 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 certificates for cloud delivery services

Certificates to access cloud delivery services such as TAS, email, and SMS are automatically installed as part of the BlackBerry AtHoc installation.

If you need to reinstall these certificates, complete the following steps for each BlackBerry AtHoc application server:

1. Go to the following URL: <https://www.digicert.com/digicert-root-certificates.htm>.
2. Locate and download the following certificate files to the application server and rename the extension to `.CER`:
 - DigiCert
 - DigiCert SHA2 Secure Server CA
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.
6. Select **Computer account** and click **Next**.
7. Select **Local computer**.
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.
12. Click **Next** and click **Browse**.
13. Navigate to where you saved the certificates.

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

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

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

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 customer support.
2. Configure BlackBerry AtHoc security settings.
3. Restart IIS.

Gather information from the customer

If the organization using an access card requires a format not supported by BlackBerry AtHoc, you must 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 BlackBerry AtHoc with the examples.

For example:

```
Subject: DC=edu, DC=athoc, O=internal, OU=people,  
OID.0.9.2342.19200300.100.1.1=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=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 that 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 automatic login for the BlackBerry AtHoc management system, update the Security Policy settings.

Note: You must be in the system setup organization (3) to update this setting.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click .
3. In the **System Setup** section, click **Security Policy**.
4. On the **Security Policy** window, in the **Smart Card Authentication** section, select the Smart Card Login **Enabled** option.
5. Save your changes.
6. Log out and attempt to log back in using a smart 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**.

(Optional) Enable FIPS on each application server

Federal Information Processing Standards (FIPS) requires an HTTPS environment.

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. Restart the server.

(Optional) System Archive account requirement

Note: This task is required only for new installations that use System Archive.

In order for the System Archive function to work, the AtHoc services application pool identities need a domain service account with **sysadmin** access on the 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 sysadmin server role.

The backup folder path must also exist on the Microsoft SQL Server and the application pool identities must have write access to that folder. The backup folder path is defined in the System Setup (3) organization in 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 [\(Optional\) Configure client certificates on the application server](#).

1. As a sysadmin, log in to the database server instance.
2. Give sysadmin permissions to the following user: `domain\"<app-server-name>$`.
3. Map the DEFAULT DATABASE to "ngaddata".
4. As a sysadmin, log in to the **SQL Server Management Studio**.
5. Open **Object Explorer**.
6. Click `server_instance_name` > **Security** > **Logins**.
7. Right-click **Logins** and then select **New Login**.
8. On the folder defined in GLB_CONFIG_TAB for [key_name]"DB_ARCHIVE_LOCATION", give full permissions to the [NTAUTHORITY\SYSTEM] login and sysadmin permissions to the database server instance.
9. On the application server, open the registry.
10. Edit the OleDbConnectionString value to add the following string at the end: **Trusted_Connection=True**.
11. As an administrator, at the command prompt, run the **IISRESET** command to restart IIS.

Configure .NET framework to use a web proxy

1. Open Notepad as administrator and open the following files:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config
```

2. Search for <system.net>. If <system.net> is not found, add the following text as the second line from the end (</configuration>) and substitute the proxy address as appropriate for the environment:

```
<system.net>
  <defaultProxy>
    <proxy autoDetect="false" bypassonlocal="true"
    proxyaddress="http://proxy_host:8080" />
  </defaultProxy>
</system.net>
```

3. Save and close the file.
4. Open Notepad as an administrator and open the following files:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\web.config
```

5. Search for <system.net>. If <system.net> is not found, add the following text as the second line from the end (</configuration>) and substitute the proxy address as appropriate for the environment:

```
<system.net>
  <defaultProxy>
    <proxy autoDetect="false" bypassonlocal="true"
    proxyaddress="http://proxy_host:8080" />
  </defaultProxy>
</system.net>
```

6. Save and close the file.
7. Open up a command prompt as an administrator and run the following command, substituting the proxy address as appropriate for the environment:

```
C:\Windows\syswow64\netsh.exe winhttp set proxy http://proxy_host:8080 bypass-
list="*.customernetwork.com"
```

Note: The bypass-list argument is optional, but it can be used to allow BlackBerry AtHoc to poll itself (health monitors) without going through the proxy.

8. Execute the following command to verify the proxy setting:

```
C:\Windows\syswow64\netsh.exe winhttp show proxy
```

9. Issue the following commands to restart the BlackBerry AtHoc application:

```
iisreset /stop
iisreset /start
```

(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
```

(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.

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. You can configure these load balancers or proxy servers to trap these errors and redirect to the friendlier messages instead. The error pages are available on the application server at the following path:
AtHocENS\wwwroot\errorpages.

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

Note: The server where you host your error pages should be different than the AtHoc server where you are running the AtHoc applications.

To host the folder, administrators copy the folder and make it publicly available from their web server. For example, if you hosted these pages directly under the root folder of the web server, the error pages can then be accessed using the following URLs, 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 AtHoc server, you 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.

Advanced server configuration

The following topics describe advanced server configuration tasks.

Migrate a preinstalled server

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

Stop services

Stop IIS.

Application server changes

1. Uninstall and reinstall 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 Time Zone and Homepage URL.

Migrate to an enterprise hierarchy

After you upgrade to this release, you can migrate to a 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.

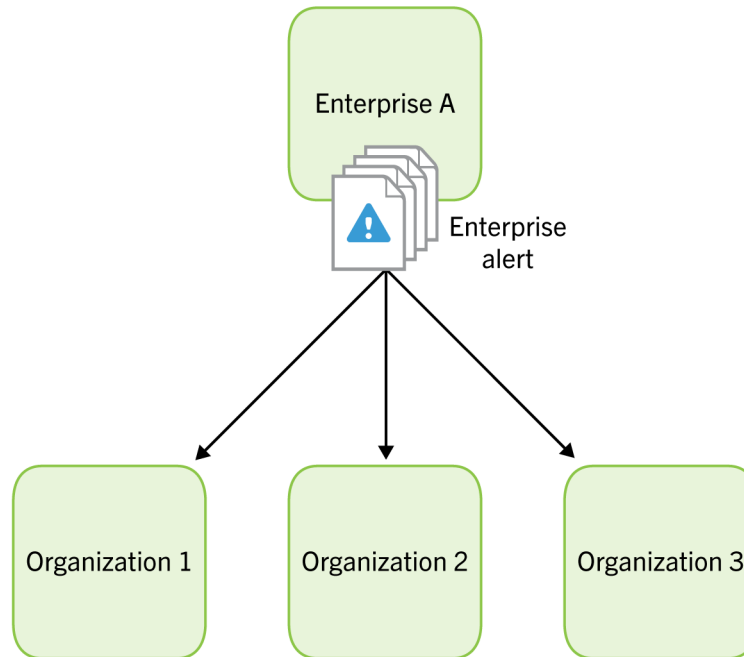
Plan the enterprise hierarchy

Important: Plan your hierarchy before you use the Enterprise Migrator 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 suborganization.

In BlackBerry AtHoc enterprise organization, there are three levels:

- The top level is System Setup. The system administrator role manages the system by logging into the System Setup (3) 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 suborganizations. The administrator can create enterprise-level attributes and folders for the enterprise organization that is inherited by its children.



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

Using the Enterprise Migrator tool, you will choose one organization that acts as the enterprise organization, and the rest that are members (suborganizations.) System Setup is the default and top-level organization. An enterprise organization inherits from System Setup and a suborganization 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 suborganizations. The suborganization 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 suborganization 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 suborganizations, but not edited. Content created at the suborganization level cannot be seen at the enterprise or system levels.

Best practices

- Rename user attributes with the name "Organization". BlackBerry AtHoc provides an enterprise user attribute with this name.
- Plan the promotion of attributes and alert folders:
 - Use enterprise attributes and alert folders is 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 suborganizations should stay at the suborganization level.
- Create end users and operators for suborganizations at the suborganization level, not the enterprise level.
- You can see all users from suborganizations 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 suborganization.)
- 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 tool

The Enterprise Migrator tool is provided with the installation package. You can use this tool to specify the relationship between parent and child organizations.

1. Log in to the BlackBerry AtHoc server and change to the following directory: `.. \AtHocENS\ServerObjects\Tools`.
2. Locate the following executable file: `EAMigrator`.
3. Right-click the file and select **Run as Administrator**.

The Enterprise Migrator opens.

Migrate organizations to the enterprise

Run the Enterprise Migrator tool to create or modify an enterprise hierarchy, and to promote attributes and alert folders from suborganizations to the enterprise or system level.

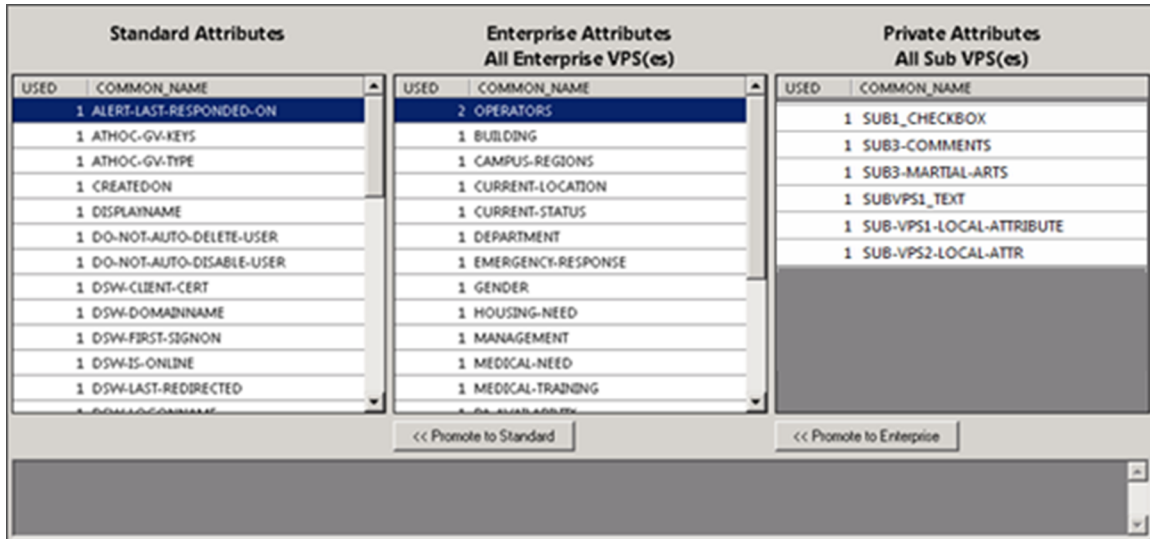
1. Plan your hierarchy before you use the tool. After you save your changes, you cannot change them.
2. The list of organizations shows all standalone organizations, except for basic organizations. If an organization is missing, it likely has an incorrect database type.
3. In the first column of the Enterprise Migrator, drag and drop any organization under another organization to specify the enterprise and suborganization levels.
4. Verify your structure before you save your changes. After your changes are saved, they cannot be undone.
5. Click **Save Structure**.

Promote user attributes and alert folders

During migration, you specify at which level the custom attributes and alert folders are defined: at the system, enterprise, or suborganization level. If only a small group of users in a suborganization 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, complete the following steps:

1. Open the Enterprise Migrator tool and click **User Attributes**.
2. Determine how many instances there are of an attribute at the suborganization 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 suborganizations within that enterprise.
3. Select the attribute name.
4. Verify that you want to promote the attribute. You cannot undo this step.



- Click **Promote to Enterprise** or **Promote to System** to move them up to a higher level.

Promote an attribute from suborganization to Enterprise if the entire enterprise needs to use the attribute. Keep the attribute in a suborganization if you want to restrict access to a single 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 suborganization level because its members have joined a lunchtime league.

- Click **Alert Folders**.

- 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 suborganization to enterprise if the entire enterprise needs to receive alerts from that alert folder. Keep the alert folder like `ExecutiveSafety` at suborganization if you want to restrict access to operators and users that have a need to know.

- Save your changes.

You have completed the reorganization.

What's next?

Grant permissions to the enterprise administrator for access to the suborganizations.

- Restart IIS after you have made the structure or content changes.
- Log in to the enterprise organization as an administrator.
- Create a user and grant this user the enterprise administrator role.
- Change to each suborganization 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, see [Appendix B: Organization duplicator object management](#).

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.
5. Select the organizations to be duplicated. The Status column indicates whether the organization is ready to copy.
6. Do one of the following:
 - Click **Copy to Target** to copy the organizations to a new system.
 - Click **New on Source** to create a new organization on the source system.
 - Click **Duplicate on Source** to copy an organization on the same system.

The message log indicates whether the duplication was successful.

Create organizations on the source server

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

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**.

You cannot select an organization administrator using the tool. The message log shows whether the new organization has been created.

Duplicate organizations on the source server

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

1. Click **Duplicate on Source**.
2. Enter the organization name and the number of copies of the organization that you want to create.

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 administrator role to do the initial set up. To access the Users menu, use the advanced operator manager role 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 the advanced operator manager role to provide access distribution lists.
- **Basic Organization roles:** If operators from other organizations need permission for a Basic organization, use the advanced operator manager role to configure permissions. Grant either the basic administrator or basic operator roles. If you choose other roles, you might 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 is the Windows domain name of the application server.
- Domain Account Name is the name of the Windows domain account.
- DomainAccountPassword is the password of the Windows domain account.

The script makes the following updates:

- Creates a Windows domain account as a login and a new "AtHoc" database server role in the SQL server. The Windows domain account is created as a member of AtHoc server role.

Database access is granted to the AtHoc server role instead of giving direct access to the Windows domain account. This login is given ownership to all AtHoc databases.

If for any reason a database restore is performed manually and the Windows domain account user account is missing, it can be created by running the ATH_CREATE_USERS SQL stored procedure in the msdb database. To return to SQL authentication by using ngad login, use the ATH_CREATE_USERS stored procedure.

Contact BlackBerry AtHoc customer support for information about using this stored procedure.

- 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 CPUs continue to function normally. Processor affinity is used in conjunction with the processor affinity mask setting to specify CPUs.

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 the `affinity.vbs` file to reflect the number of cores available.

The value for `SMPProcessorAffinityMask` must be entered as hexadecimal.

3. Complete any of the following tasks:

- a. Specify specific cores to use: 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. For example, eight cores in binary would be represented as 11111111.
- b. Specify to use only the first four cores. For example, all cores in the same chip for a quad-core): Select 00001111 or 11110000 (if dual-quad.)
- c. Specify to use every other core:
 1. Enter **10101010** (or **01010101**) in a Windows scientific calculator in binary data (Bin) and click **Hex** to see the equivalent value in hexadecimal (&AA or &55.)
 2. Stop IIS and run the `affinity.vbs` file in a 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 uploading very large .csv or audio files.

1. In **IIS Manager**, click 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.

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

Database recovery setting

If the recovery model for the SQL databases is set to Full, the transaction log files must be backed up before they become full. Otherwise, all operations on the database will stop and the system will freeze. It is very important to understand the backup strategy for the site and configure these settings carefully. Consult with your database administrator before you make any changes to the recovery model.

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

IIS 10.0 Security Technology Implementation Guide

The following sections describe the server and application tasks that you can complete to achieve IIS 10.0 STIG compliance in your BlackBerry AtHoc system.

Server STIG

This section describes the tasks you need to complete to ensure your servers comply with the IIS 10.0 STIG.

IIST-SV-000102: Enable enhanced logging

Enhanced logging for the IIS 10.0 web server must be enabled and must capture all user and web server events.

To check compliance with IIST-SV-000102, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Click **Select Fields** and verify that at least one of the following fields are selected:
 - Date
 - Time
 - Client IP Address
 - User Name
 - Method
 - URI Query
 - Protocol Status
 - Referrer

If no options are selected, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Select the following fields: **Date**, **Time**, **Client IP Address**, **User Name**, **Method**, **URI Query**, **Protocol Status**, and **Referrer**.
6. In the **Actions** pane, click **Apply**.

IIST-SV-000103: Enable log file and Event Tracing for windows

Both the log file and Event Tracing for Windows (ETW) for the IIS 10.0 web server must be enabled.ts.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web 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 **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 10.0 Manager.
2. Click the IIS 10.0 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**.

IIST-SV-000110: Produce log records

The IIS 10.0 web server must produce log records that contain sufficient information to establish the outcome (success or failure) of IIS 10.0 web server events.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, verify that **Request Header >> Connection** and **Request Header >> Warning** are selected.

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

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, select the following fields:
 - **Source Type > Request Header**
 - **Source > Connection**
7. Click **OK**.
8. Click **Source Type > Response Header**.
9. Click **Source > Warning**.
10. Click **OK**.
11. In the **Actions** pane, click **Apply**.

IIST-SV-000111: Produce log records

The IIS 10.0 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 IIST-SV-000111, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured 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 **Request Header >> Authorization** and **Response Header >> Content-Type** are selected.

If any of the standard or custom fields are not selected, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, select **User Agent**, **User Name**, and **Referrer**.
7. Under **Custom Fields**, select the following fields:
 - **Source Type > Request Header**
 - **Source > Authorization**
8. Click **OK**.
9. Click **Source > Content-Type**
10. Click **Source Type > Response Header**.
11. Click **OK**.
12. In the **Actions** pane, click **Apply**.

IIST-SV-000115: Protect log information

The log information from the IIS 10.0 web server must be protected from unauthorized modification or deletion.

To check compliance with IIST-SV-000115, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Click **Browse** and then navigate to the directory where the log files are stored.
5. Right-click the log file directory and select **Properties**.
6. Click the **Security** tab.
7. Verify the log file access is restricted to **System - Full Control** and **Administrators - Full Control**.

If the log file restrictions are not set to **System - Full Control** and **Administrators - Full Control**, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Click **Browse** and then navigate to the directory where the log files are stored.
5. Right-click the log file directory and select **Properties**.
6. Click the **Security** tab.
7. Set the log file permissions to **System - Full Control** and **Administrators - Full Control**.
8. Click **OK**.
9. In the **Actions** pane, click **Apply**.

IIST-SV-000117: Do not perform user management

The IIS 10.0 web server must not perform user management for hosted applications.

To check compliance with IIST-SV-000117, complete the following steps:

1. Verify with the System Administrator (SA) if the IIS 10.0 web server is hosting an application.
2. If the IIS 10.0 web server is hosting an application, verify with the SA that they can provide supporting documentation about how the application's user management is accomplished outside of the IIS 10.0 web server.

If the web server is hosting an application and the SA cannot provide the supporting documentation, your server is not compliant.

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

1. Reconfigure any hosted applications on the IIS 10.0 web server to perform user management outside the IIS 10.0 web server.
2. Document how the hosted application user management is accomplished.

IIST-SV-000118: Contain only necessary functions

The IIS 10.0 web server must contain only functions that are necessary for operation.

To check compliance with IIST-SV-000118, complete the following steps:

1. Click **Start**.
2. Open the **Control Panel**.
3. Click **Programs**.
4. Click **Programs and Features**.
5. Review the installed programs.

If any programs are installed that are not required for the IIS 10.0 web services, your server is not compliant. If additional software is needed, supporting documentation must be signed by the Information Systems Security Officer (ISSO.)

If your server is not compliant, remove all unapproved programs and roles from the production IIS 10.0 web server.

IIST-SV-000119: Must not be both a website server and a proxy server

The IIS 10.0 web server must not be both a website server and a proxy server.

To check compliance with IIST-SV-000119, complete the following steps:

1. Open the IIS 10.0 Manager.
2. In the **Connections** pane, select the IIS 10.0 web server.
3. Under **IIS installed features**, verify if **Application Request Routing Cache** is present. If this setting is not present, your server is compliant.
4. If the **Application Request Routing Cache** is present, double-click the icon.
5. In the **Actions** pane, under **Proxy**, click **Server Proxy Settings....**
6. In the **Application Request Routing** window, verify if the **Enable proxy** option is selected.

If the **Enable proxy** option is selected, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. In the **Connections** pane, select the IIS 10.0 web server.
3. Under **IIS installed features** double-click the **Application Request Routing Cache** icon.
4. In the **Actions** pane, under **Proxy**, click **Server Proxy Settings....**
5. In the **Application Request Routing** window, deselect the **Enable proxy** option.
6. In the **Actions** pane, click **Apply**.

IIST-SV-000120: Remove code samples, example applications, and tutorials

All IIS 10.0 web server sample code, example applications, and tutorials must be removed from a production IIS 10.0 server.

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

1. Navigate to the following folders:
 - intepub\
 - Program Files\Common Files\System\msadc
 - Program Files (x86)\Common Files\System\msadc
2. Check if the folder or sub-folders contain any executable sample code, example applications, or tutorials which are not explicitly used by a production website.

If the folder or sub-folders contain any executable sample code, example applications, or tutorials which 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 which are not explicitly used by a production website.

IIST-SV-000121: Delete accounts created by uninstalled features

Accounts created by uninstalled features such as tools and utilities must be deleted from the IIS 10.0 server.

To check compliance with IIST-SV-000121, complete the following steps:

1. Open the IIS 10.0 Manager.
2. On the **Apps** menu, under **Administrative Tools**, click **Computer Management**.
3. In the left pane, expand **Local Users and Groups**.
4. Click **Users**.
5. Review the local users listed in the middle pane.

If any local accounts are present that were created by uninstalled features or are not used, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. On the **Apps** menu, under **Administrative Tools**, click **Computer Management**.
3. In the left pane, expand **Local Users and Groups**.
4. Click **Users**.
5. Delete any local accounts that were created by uninstalled features or are not used.

IIST-SV-000123: Remove unnecessary features, utilities, plug-ins, and modules

The IIS 10.0 web server must be reviewed on a regular basis to remove any Operating System features, utility programs, plug-ins, and modules not necessary for operation.

To check compliance with IIST-SV-000123, complete the following steps:

1. Consult with the System Administrator and review all installed IIS 10.0 and Operating System features.
2. Determine if any features installed are no longer necessary for operation.

If any Operating System features are installed, your server is not compliant.

If your server is not compliant, remove all utility programs, Operating System features, or modules that are not necessary for web server operation.

IIST-SV-000124: Disable MIMEs that invoke OS shell programs

The IIS 10.0 web server must have Multipurpose Internet Mail Extensions (MIME) that invoke OS shell programs disabled.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. Under **Application**, verify that the list of MIME types for OS shell program extensions that have been removed includes, at a minimum, the following extensions:
 - .exe
 - .dll
 - .com
 - .bat
 - .csh

If any 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 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. From the list of extensions under "Application", remove MIME types for OS shell program extensions, to include at a minimum, the following extensions:
 - .exe
 - .dll
 - .com
 - .bat
 - .csh
6. In the **Actions** pane, click **Apply**.

IIST-SV-000125: Disable WebDAV

The IIS 10.0 web server must have Web Distributed Authoring and Versioning (WebDAV) disabled.

To check compliance with IIST-SV-000125, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. In the **Cells** section, review the list of features.

If the **WebDAV Authoring Rules** icon exists, your server is not compliant.

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

1. Access Server Manager on the IIS 10.0 web server.
2. Click the IIS 10.0 web server name.
3. Click **Manage**.
4. Click **Add Roles and Features**.

5. On the **Before you begin** dialog, click **Next**.
6. On the **Installation Type** dialog, click **Role-based or feature-based installation**.
7. Click **Next**.
8. On the **Server Selection** dialog, click the IIS 10.0 web server.
9. From the **Windows Features** dialog, navigate to **World Wide Web Services > Common HTTP Features**.
10. Deselect **WebDAV Publishing**.
11. Click **Next** to remove the WebDAV Publishing feature from the IIS 10.0 web server.

IIST-SV-000130: Limit installed Java software

Java software installed on a production IIS 10.0 web server must be limited to .class files and the Java Virtual Machine.

To check compliance with IIST-SV-000130, search the system for files with either .java or .jsp extensions.

If files with .java or .jsp extensions are found, your server is not compliant.

If your server is not compliant, remove all files from the web server with both .java or .jsp extensions.

IIST-SV-000131: Limit access to only administrative accounts

IIS 10.0 web server accounts that access the directory tree, the shell, or other operating system functions and utilities must only be administrative accounts.

To check compliance with IIST-SV-000131, complete the following steps:

1. Obtain a list of the user accounts with access to the system, including all local and domain accounts.
2. Review the privileges to the web server for each account.
3. Verify with the System Administrator or the ISSO that all privileged accounts are mission essential and documented.
4. Verify with the System Administrator or the ISSO that all non-administrator access to shell scripts and operating system functions are mission essential and documented.

If undocumented privileged accounts are found, your server is not compliant.

If undocumented non-administrator access to shell scripts and operating system functions are found, your server is not compliant.

Note: If your IIS 10 installation supports Microsoft Exchange and is not otherwise hosting any content, this requirement is not applicable.

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

1. Ensure that non-administrators are not allowed access to the directory tree, the shell, or other operating system functions and utilities.
2. Ensure that all non-administrator access to shell scripts and operating system functions is mission essential and documented.

IIST-SV-000134: Use cookies to track session state

The IIS 10.0 web server must use cookies to track session state.

To check compliance with IIST-SV-000134, do one of the following:

- 1. Open the IIS 10.0 Manager.
 2. Click the IIS 10.0 web server name.
 3. Under **ASP.Net**, double-click the **Session State** icon.
 4. Under **Cookie Settings**, verify that the **Use Cookies** option is selected in the **Mode** drop-down list.

If the **Use Cookies** option is not selected, your server is not compliant.

- 1. Click the site name.
 2. In the **Management** section, click **Configuration Editor**.
 3. On the configuration editor, from the **Section:** drop-down list, locate **system.web/sessionState**.
 4. Verify that **cookieless** is set to **UseCookies**.

If the **cookieless** option is not set to **UseCookies**, your server is not compliant.

Note: If your IIS 10.0 server/site is used only for system-to-system maintenance, does not allow users to connect to an interface, and is restricted to specific system IPs, this is not applicable.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **ASP.Net**, double-click the **Session State** icon.
4. Under **Cookie Settings**, select **Use Cookies** from the **Mode** drop-down list.
5. In the **Actions** pane, click **Apply**.

IIST-SV-000135: Accept only system-generated session identifiers

The IIS 10.0 web server must accept only system-generated session identifiers.

To check compliance with IIST-SV-000135, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **ASP.NET** section, select **Session State**.
4. Under **Cookie Settings**, verify that the **Use Cookies** option is selected from the **Mode:** drop-down list.
5. Under **Time-out (in minutes)**, verify that **20 minutes or less** is selected.

If the **Use Cookies** option is selected, and **Time-out (in minutes)** is not set to **20 minutes or less**, your server is not compliant.

Note: If your IIS 10.0 server/site is used only for system-to-system maintenance, does not allow users to connect to the interface, and is restricted to specific system IPs, this is not applicable.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **ASP.NET** section, click **Session State**.
4. In the **Actions** pane, click **Apply**.
5. Under **Cookie Settings**, select the **Use Cookies** option from the **Mode:** drop-down list.
6. Under **Time-out (in minutes)**, click **20 minutes or less**.

IIST-SV-000138: Disable directory browsing

Directory Browsing on the IIS 10.0 web server must be disabled.

To check compliance with IIST-SV-000138, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Directory Browsing** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.
5. In the **Actions** panel, verify that **Directory Browsing** is disabled.

If **Directory Browsing** is enabled, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Directory Browsing** icon.
4. In the **Actions** pane, click **Disabled**.

IIST-SV-000139: Index only web content

The IIS 10.0 web server Indexing must only index web content.

To check compliance with IIST-SV-000139, complete the following steps:

1. Access the IIS 10.0 web server.
2. Access an administrator command prompt and type **regedit <enter>** to access the server's registry.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex\Catalogs\. If this key exists, then indexing is enabled. If the key does not exist, this check is not applicable.
4. Review the catalog keys to determine if directories other than web document directories are being indexed.

If directories other than web document directories are being indexed, your server is not compliant.

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

1. Run MMC.
2. Add the **Indexing Service** snap-in.
3. Edit the indexed directories to include only web document directories.

IIST-SV-000140: Modify warning and error messages

Warning and error messages displayed to clients must be modified to minimize the identity of the IIS 10.0 web server, patches, loaded modules, and directory paths.

To check compliance with IIST-SV-000140, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Error Pages** icon.
4. Click any error message.
5. In the **Actions** pane, click **Edit Feature Setting**.

If the feature setting is not set to **Detailed errors for local requests and custom error pages for remote requests**, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Error Pages** icon.
4. Click any error message.
5. In the **Actions** pane, set **Feature Setting** to **Detailed errors for local requests and custom error pages for remote requests**.

IIST-SV-000141: Follow access policy

Remote access to the IIS 10.0 web server must follow access policy or work with enterprise tools designed to enforce policy requirements.

If web administration is performed at the console, this check is not applicable.

If web administration is performed remotely, to check compliance with IIST-SV-000141, verify that the following conditions are met:

- If administration of the server is performed remotely, it is only performed securely by System Administrators.
- If website administration or web application administration has been delegated, those users are documented and approved by the ISSO.
- Remote administration is in compliance with any requirements contained within the Windows Server STIGs and any applicable Network STIGs.
- Remote administration of any kind is restricted to documented and authorized personnel.
- All users performing remote administration are authenticated.
- All remote sessions are encrypted and use FIPS 140-2-approved protocols. FIPS 140-2-approved TLS versions include TLS V1.2 or greater.

Review with site management how remote administration is configured on the website, if applicable. If remote management meets the criteria listed above, your server is compliant. If remote management is used and does not meet the criteria listed above, your server is not compliant.

If your server is not compliant, ensure that the web server administration is only performed over a secure path.

IIST-SV-000142: Restrict inbound connections

The IIS 10.0 web server must restrict inbound connections from non-secure zones.

Note: This requirement applies to the Web Management Service. If the Web Management Service is not installed, this requirement is not applicable.

To check compliance with IIST-SV-000142, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **Management**, double-click **Management Service**.
4. If **Enable remote connections** is not selected, this requirement is not applicable. If **Enable remote connections** is selected, review the entries under **IP Address Restrictions**.
5. Verify that only known, secure IP ranges are configured as **Allow**.

If **IP Address Restrictions** are not configured, or IP ranges that are configured as **Allow** are not restrictive enough to prevent connections from non-secure zones, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.5 web server name.
3. Under **Management**, double-click **Management Service**.
4. In the **Actions** pane, stop the Web Management Service.
5. Configure only known, secure IP ranges as **Allow**.
6. In the **Actions** pane, click **Apply**.
7. In the **Actions** pane, restart the Web Management Service.

IIST-SV-000144: Conform to minimum file permission requirements

IIS 10.0 web server system files must conform to minimum file permission requirements.

To check compliance with IIST-SV-000144, complete the following steps:

1. Open Explorer and navigate to the **inetpub** directory.
2. Right-click **inetpub** and select **Properties**.

3. Click the **Logging** icon.
4. Click the **Security** tab.
5. Verify the permissions for the following users:
 - System: Full control
 - Administrators: Full control
 - TrustedInstaller: Full control
 - ALL APPLICATION PACKAGES (built-in security group): Read and execute
 - ALL RESTRICTED APPLICATION PACKAGES (built-in security group): Read and execute
 - Users: Read and execute, list folder contents
 - CREATOR OWNER: Full Control, Subfolders and files only

If the permissions for the users listed above are less restrictive, your server is not compliant.

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

1. Open Explorer and navigate to the **inetpub** directory.
2. Right-click **inetpub** and select **Properties**.
3. Click the **Security** tab.
4. Set the following permissions:
 - System: Full control
 - Administrators: Full control
 - TrustedInstaller: Full control
 - ALL APPLICATION PACKAGES (built-in security group): Read and execute
 - ALL RESTRICTED APPLICATION PACKAGES (built-in security group): Read and execute
 - Users: Read and execute, list folder contents
 - CREATOR OWNER: Special permissions to subkeys

IIST-SV-000145: Allocate sufficient log record storage capacity

The IIS 10.0 web server must use a logging mechanism configured to allocate log record storage capacity large enough to accommodate the logging requirements of the IIS 10.0 web server.

To check compliance with IIST-SV-000145, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. In the **Logging** dialog, verify the **Directory**: that W3C logging is written to.
5. Confirm with the System Administrator that the designated log path is of sufficient size to maintain the logging.
6. Under **Log File Rollover**, verify that **Do not create new log files** is not selected.
7. Verify that a schedule is configured to roll over log files on a regular basis.
8. Verify with the System Administrator that there is a documented process for moving the log files off of the IIS 10.0 web server to another logging device.

If the designated logging path device is not large enough to maintain all log files, and there is not a schedule to roll over files on a regular basis, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.

4. In the **Logging** dialog, designate a log path to a location able to house the logs.
5. Under **Log File Rollover**, deselect the **Do not create new log files** option.
6. Configure a schedule to roll over log files on a regular basis.

IIST-SV-000147: Restrict access to web administration tools

Access to web administration tools must be restricted to the web manager and the web manager's designees.

To check compliance with IIST-SV-000147, complete the following steps:

1. Right-click **InetMgr.exe**, and then click **Context > Properties**.
2. Click the **Security** tab.
3. Review the groups and user names.
4. Compare the local documentation authorizing specific users against the users observed when reviewing the groups and users.

The following accounts may have full control privileges:

- TrustedInstaller
- Web Managers
- Web Manager designees
- CREATOR OWNER: Full Control, Subfolders and files only

The following accounts may have read and execute or read permissions:

- Non Web Manager Administrators
- ALL APPLICATION PACKAGES (built-in security group)
- ALL RESTRICTED APPLICATION PACKAGES (built-in security group)
- SYSTEM
- Users

Specific users may have read and execute and read permissions.

If any other access is observed, your server is not compliant.

If your server is not compliant, restrict access to the web administration tool to only the web manager and the web manager's designees.

IIST-SV-000149: Disable IPP

The Internet Printing Protocol (IPP) must be disabled on the IIS 10.0 web server.

If the Print Services role and the Internet Printing role are not installed, this check is not applicable.

To check compliance with IIST-SV-000149, complete the following steps:

1. Navigate to the following directory: %windir%\web\printers. Take note if the directory exists.
2. Click **Start > Administrative Tools**, and then click **Server Manager**.
3. Expand the **roles** node.
4. Right-click **Print Services**, and then click **Remove Roles Services**.

If the %windir%\web\printers folder exists, your server is not compliant. If the Internet Printing option is enabled, your server is not compliant.

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

1. Click **Start > Administrative Tools**, and then click **Server Manager**.
2. Expand the **roles** node.
3. Right-click **Print Services**, and then click **Remove Roles Services**.

4. Deselect the the **Internet Printing** option.
5. Click **Next**.
6. Click **Remove**.

IIST-SV-000152: Use TLS to send session IDs

IIS 10.0 web server session IDs must be sent to the client using TLS.

To check compliance with IIST-SV-000152, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **Management** section, double-click the **Configuration Editor** icon.
4. From the **Section:** drop-down list, select **system.webServer/asp**.
5. Expand the **session** section.
6. Verify that **keepSessionIdSecure** is set to **True**.

If **keepSessionIdSecure** is not set to True, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **Management** section, double-click the **Configuration Editor** icon.
4. From the **Section:** drop-down list, select **system.webServer/asp**.
5. Expand the **session** section.
6. Select **True** for **keepSessionIdSecure**.
7. In the **Actions** pane, click **Apply**.

IIST-SV-000153: Use TLS to maintain confidentiality

An IIS 10.0 web server must maintain the confidentiality of controlled information during transmission through the use of an approved Transport Layer Security (TLS) version.

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

1. Access the IIS 10.0 web server.
2. Access an administrator command prompt and type **regedit <enter>** to access the server's registry.
3. Navigate to: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server.
4. Verify that **DisabledByDefault** has a REG_DWORD value of **0**.
5. Navigate to the following paths and verify that **DisabledByDefault** has a REG_DWORD value of **1** and **Enabled** has a REG_DWORD value **0**:
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server

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

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

1. Access the IIS 10.0 web server.
2. Access an administrator command prompt and type **regedit <enter>** to access the server's registry.
3. Navigate to: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server.

4. Configure **DisabledByDefault** to have a REG_DWORD value of **0**.
5. Navigate to the following paths and configure **DisabledByDefault** to have a REG_DWORD value of **1** and **Enabled** to have a REG_DWORD value **0**:
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server

IIST-SV-000154: Use approved TLS version

The IIS 10.0 web server must maintain the confidentiality of controlled information during transmission through the use of an approved Transport Layer Security (TLS) version.

To check compliance with IIST-SV-000154, review the web server documentation and deployed configuration to determine which version of TLS is being used.

If the TLS version is not TLS 1.2 or higher, according to NIST SP 800-52, or if non-FIPS-approved algorithms are enabled, your server is not compliant.

If your server is not compliant, configure the web server to use an approved TLS version according to NIST SP 800-52 and disable all non-approved versions.

IIST-SV-000156: Assign passwords

All accounts installed with the IIS 10.0 web server software and tools must have passwords assigned and default passwords changed.

To check compliance with IIST-SV-000156, complete the following steps:

1. Access the IIS 10.0 web server.
2. Access the **Apps** menu.
3. Under **Administrative Tools**, click **Computer Management**.
4. In the left pane, expand **Local Users and Groups**.
5. Click **Users**.
6. Review the local users displayed in the middle pane.
7. If any local accounts are present and used by IIS 10.0, verify with your System Administrator that the default passwords have been changed.

If passwords have not been changed from the default, your server is not compliant.

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

1. Access the IIS 10.0 web server.
2. Access the **Apps** menu.
3. Under **Administrative Tools**, click **Computer Management**.
4. In the left pane, expand **Local Users and Groups**.
5. Click **Users**.
6. Change the password for any local accounts displayed that are used by IIS 10.0.
7. Verify with your System Administrator that the default passwords have been changed.

IIST-SV-000158: Remove unspecified file extensions

Unspecified file extensions on a production IIS 10.0 web server must be removed.

To check compliance with IIST-SV-000158, complete the following steps:

1. Open the IIS 10.0 Manager.

2. Click the IIS 10.0 web server name.
3. Double-click the **ISAPI and CGI restrictions** icon.
4. Click **Edit Feature Settings**.
5. Verify that **Allow unspecified CGI modules** and **Allow unspecified ISAPI modules** are not selected.

If **Allow unspecified CGI modules** or **Allow unspecified ISAPI modules** is selected, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **ISAPI and CGI restrictions** icon.
4. Click **Edit Feature Settings**.
5. Deselect **Allow unspecified CGI modules** and **Allow unspecified ISAPI modules**.
6. Click **OK**.

IIST-SV-000159: Configure a global authorization rule

The IIS 10.0 web server must have a global authorization rule configured to restrict access.

To check compliance with IIST-SV-000159, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **.NET Authorization Rules** icon.

If any groups other than **Administrators** are listed, your server is not compliant.

If ASP.NET is not installed, this is not applicable. If the server is hosting Microsoft SharePoint, this is not applicable. If the server is hosting WSUS, this is not applicable.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Authorization Rules** icon.
4. Remove all groups other than **Administrators**.

IIST-SV-000200: Configure the Max Connections setting

The IIS 10.0 website's MaxConnections setting must be configured to limit the number of allowed simultaneous session requests.

To check compliance with IIST-SV-000200, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **Management** section, click **Configuration Editor**.
4. From the **Section:** drop-down list at the top of the configuration editor, locate **system.applicationHost/sites**.
5. Expand **siteDefaults**.
6. Expand **limits**.
7. Review the results and verify that the value of the **maxconnections** parameter is greater than zero.

If the **maxconnections** parameter value is zero, your server is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.

3. In the **Management** section, click **Configuration Editor**.
4. From the **Section:** drop-down list at the top of the configuration editor, locate **system.applicationHost/sites**.
5. Expand **siteDefaults**.
6. Expand **limits**.
7. Set the **maxconnections** parameter to a value greater than zero.

IIST-SV-000205: Enable HSTS

The IIS 10.0 web server must enable HTTP Strict Transport Security (HSTS.)

To check compliance with IIST-SV-000205, complete the following steps:

1. Access the IIS 10.0 web server.
2. Open IIS Manager.
3. Click the IIS 10.0 web server name.
4. Under **Management**, open **Configuration Editor**.
5. For the **Section**, navigate to **system.applicationHost/sites**.
6. Expand **siteDefaults** and **HSTS**.

Your server is not compliant if:

- **enabled** is not set to **True**.
- **includeSubDomains** is not set to **True**.
- **max-age** is not set to a value greater than 0.
- **redirectHttpToHttps** is not set to **True**.

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

1. Log in to the Configuration Editor in the IIS Manager or Powershell.
2. Enable **HSTS**.
3. Set **includeSubDomains** to **True**.
4. Set **max-age** to a value greater than 0.
5. Set **redirectHttpToHttps** to **True**.

IIST-SV-000160: Require authentication for an SMTP relay

An IIS server configured to be an SMTP relay must require authentication.

To check compliance with IIST-SV-000160, interview your System Administrator about the role of the IIS 10.0 web server.

If the IIS 10.0 web server is running SMTP relay services, have the SA provide supporting documentation about how the server is hardened. A DoD-issued certificate, and specific allowed IP address should be configured.

If the IIS web server is not running SMTP relay services, this is not applicable.

If the IIS web server running SMTP relay services without TLS enabled, your server is not compliant.

If your server is not compliant, configure the relay server with a specific allowed IP address from the same network as the relay and implement TLS.

Application STIG

This section describes the tasks you need to complete to ensure your application complies with the IIS 10.0 STIG.

IIST-SI-000201: Enable session state

The IIS 10.0 website session state must be enabled.

To check compliance with IIST-SI-000201, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Session State Mode Settings**, verify that the **In Process** mode is selected.

If the **Session State Mode Settings** mode is not set to **In Process** selected, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, select **Session State**.
4. Under **Session State Mode Settings**, select **In Process** mode.
5. In the **Actions** pane, click **Apply**.

IIST-SI-000202: Configure session state cookie settings

The IIS 10.0 website session state cookie settings must be configured to Use Cookies mode.

To check compliance with IIST-SI-000202, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Cookie Settings**, verify that the **Use Cookies** mode is selected from the **Mode:** drop-down list.

If the **Use Cookies** mode is selected, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, select **Session State**.
4. Under **Cookie Settings**, select **Use Cookies** from the **Mode:** drop-down list.
5. In the **Actions** pane, click **Apply**.

IIST-SI-000206: Enable the log file and ETW

Both the log file and Event Tracing for Windows (ETW) for each IIS 10.0 website must be enabled.

To check compliance with IIST-SI-000206, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website 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 **Both log file and ETW event** option is not selected, your application is not compliant.

Note: "Microsoft-IIS-Logging/logs" must be enabled before configuring this setting.

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

1. Open the IIS 10.0 Manager.
2. Click the site 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**.

IIST-SI-000210: Produce log records containing sufficient information

The IIS 10.0 website 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 IIST-SI-000210, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that the **Format:** option is configured to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, verify that the following fields are configured:
 - Request Header >> Authorization
 - Response Header >> Content-Type

If either **Request Header >> Authorization** or **Response Header >> Content-Type** is not selected, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, configure **Format:** under **Log File** to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, select **Request Header >> Authorization** and **Response Header >> Content-Type**.
7. Click **OK**.
8. In the **Actions** pane, click **Apply**.

IIST-SI-000214: Disable MIMEs that invoke OS shell programs

The IIS 10.0 website must have Multipurpose Internet Mail Extensions (MIME) that invoke OS shell programs disabled.

To check compliance with IIST-SI-000214, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. From the list of extensions under **Application**, verify that MIME types for OS shell program extensions have been removed, to include at a minimum, the following extensions:
 - .exe

- .dll
- .com
- .bat
- .csh

If any 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 10.0 Manager.
2. Click the IIS 10.0 site.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. From the list of extensions under **Application**, remove MIME types for OS shell program extensions to include, at a minimum, the following extensions:
 - .exe
 - .dll
 - .com
 - .bat
 - .csh
6. In the **Actions** pane, click **Apply**.

IIST-SI-000216: Set resource mappings

The IIS 10.0 website must have resource mappings set to disable the serving of certain file types. For request filtering, the ISSO must document and approve all scripts the website allows (white list) and denies (black list.) The white list and black list are compared to the request filtering in IIS 10.0. Request filtering at the site level takes precedence over request filtering at the server level.

To check compliance with IIST-SI-000216, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **Request Filtering > File Name Extensions Tab**.

If any script file extensions from the black list are not denied, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **Request Filtering > File Name Extensions Tab > Deny File Name Extension**.
4. Add any script file extensions listed on the black list that are not listed.
5. In the **Actions** pane, click **Apply**.

IIST-SI-000217: Disable WebDAV

The IIS 10.0 website must have Web Distributed Authoring and Versioning (WebDAV) disabled.

To check compliance with IIST-SI-000217, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 website.
3. Review the features listed under the **IIS** section.

If the **WebDAV Authoring Rules** icon is present, your application is not compliant.

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

1. Access **Server Manager** on the IIS 10.0 website.
2. Click **Local Server**.
3. Click **Manage**.
4. Click **Add Roles and Features**.
5. In the **Before you begin** dialog, click **Next**.
6. In the **Installation Type** dialog, click **Role-based or feature-based installation**.
7. Click **Next**.
8. On the **Server Selection** dialog, select the IIS 10.0 web server.
9. On the **Windows Features** dialog, navigate to **World Wide Web Services > Common HTTP Features**.
10. Deselect **WebDAV Publishing**.
11. Click **Next**.
12. In the **Actions** pane, click **Apply**.

IIST-SI-000221: Restrict anonymous access accounts

Anonymous IIS 10.0 website access accounts must be restricted.

To check compliance with IIST-SI-000221, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click **Authentication**.
4. If Anonymous Access is disabled, this is not applicable. If Anonymous Access is enabled, click **Anonymous Authentication**.
5. In the **Actions** pane, click **Edit**.
6. If the **Specific user** option is selected and an ID is specified in the adjacent control box, this is the ID being used for anonymous access. Take note of the account name.
7. Check privileged groups that may allow the anonymous account inappropriate membership:
 - a. On the computer, open **Server Manager**.
 - b. Expand **Configuration**.
 - c. Expand **Local Users and Groups**.
 - d. Click **Groups**.
 - e. Review members of the following privileged groups:
 - Administrators
 - Backup Operators
 - Certificate Services (of any designation)
 - Distributed COM Users
 - Event Log Readers
 - Network Configuration Operators
 - Performance Log Users
 - Performance Monitor Users
 - Power Users
 - Print Operators
 - Remote Desktop Users
 - Replicator
 - f. Double-click each group and review its members.

If the IUSR account or any account noted above used for anonymous access is a member of any group with privileged access, your application is not compliant.

If your application is not compliant, remove the Anonymous Access account from all privileged accounts and all privileged groups.

IIST-SI-000223: Generate unique session identifiers

The IIS 10.0 website must generate unique session identifiers that cannot be reliably reproduced.

To check compliance with IIST-SI-000223, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Session State** mode settings, verify that the **In Process** mode is selected.

If the **In Process** mode is not selected, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Session State** mode settings, select the **In Process** mode.

IIST-SI-000224: Separate document directory and system files

The IIS 10.0 website document directory must be in a separate partition from the IIS 10.0 websites system files.

To check compliance with IIST-SI-000224, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. In the **Actions** pane, click **Advanced Settings**.
4. Review the Physical Path.

If the **Path** is on the same partition as the OS, your application is not compliant.

Note: If this IIS 10.0 installation supports Microsoft Exchange, and is not otherwise hosting any content, this requirement is not applicable.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. In the **Actions** pane, click **Advanced Settings**.
4. Change the Physical Path to the new partition and directory location.

IIST-SI-000225: Limit the maxURL

The IIS 10.0 website must be configured to limit the maxURL.

To check compliance with IIST-SI-000225, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.

3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **maxUrl** value is not set to 4096 or less, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Set the **maxUrl** value to 4096 or less.

IIST-SI-000226: Limit the size of web requests

The IIS 10.0 website must be configured to limit the size of web requests.

To check compliance with IIST-SI-000226, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **maxAllowedContentLength** value is not explicitly set to "30000000" or less, or a length documented and approved by the ISSO, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Set the **maxAllowedContentLength** value to "30000000" or less.

IIST-SI-000227: Configure the Maximum Query String limit

The IIS 10.0 website's Maximum Query String limit must be configured.

To check compliance with IIST-SI-000227, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **Maximum Query String** value is not set to "2048" or less, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Set the **Maximum Query String** value to 2048 or less.

IIST-SI-000228: Prohibit non-ASCII characters in URLs

Non-ASCII characters in URLs must be prohibited by any IIS 10.0 website.

To check compliance with IIST-SI-000228, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

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

Note: If this IIS 10.0 installation supports Microsoft Exchange, and is not otherwise hosting any content, this requirement is not applicable.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

Deselect the **Allow high-bit characters** option.

IIST-SI-000229: Prohibit double encoded URL requests

Double encoded URL requests must be prohibited by any IIS 10.0 website.

To check compliance with IIST-SI-000229, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **Allow double escaping** option is selected, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Deselect the **Allow double escaping** option.

IIST-SI-000231: Disable directory browsing

Directory Browsing on the IIS 10.0 website must be disabled.

To check compliance with IIST-SI-000231, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Double-click the **Directory Browsing** icon. If Directory Browsing is not installed, this is not applicable.
4. In the **Actions** pane, verify that **Directory Browsing** is **Disabled**.

If the **Directory Browsing** option is not Disabled, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Directory Browsing** icon.
4. In the **Actions** pane, click **Disabled**.

IIST-SI-000233: Modify warning and error messages

Warning and error messages displayed to clients must be modified to minimize the identity of the IIS 10.0 website, patches, loaded modules, and directory paths.

To check compliance with IIST-SI-000233, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Error Pages** icon.
4. Click each error message and then click **Edit Feature** in the **Actions** pane.

If any error message is not set to **Detailed errors for local requests and custom error pages for remote requests**, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Error Pages** icon.
4. Click each error message and then click **Edit Feature** in the **Actions** pane.
5. Set each error message to **Detailed errors for local requests and custom error pages for remote requests**.

IIST-SI-000234: Disable debugging and trace information

Debugging and trace information used to diagnose the IIS 10.0 website must be disabled.

Note: If the ".NET feature" is not installed, this check is not applicable.

To check compliance with IIST-SI-000234, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **.NET Compilation**.
4. Scroll down to the **Behavior** section and verify that the value for **Debug** is set to **False**.

If the **Debug** option is not set to **False**, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **.NET Compilation**.
4. Scroll down to the **Behavior** section and set the value for **Debug** to **False**.

IIST-SI-000238: Use a logging mechanism

The IIS 10.0 website must use a logging mechanism configured to allocate log record storage capacity large enough to accommodate the logging requirements of the IIS 10.0 website.

To check compliance with IIST-SI-000238, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. In the **Logging** dialog, determine the **Directory**: that **W3C** logging is being written to.
5. Confirm with your System Administrator that the designated log path is of sufficient size to maintain the logging.
6. Under **Log File Rollover**, verify that **Do not create new log files** is not selected.
7. Verify that a schedule is configured to roll over log files on a regular basis.
8. Consult with your System Administrator to determine if there is a documented process for moving the log files off of the IIS 10.0 web server to another logging device.

If the designated logging path device is not of sufficient space to maintain all log files and there is not a schedule to rollover files on a regular basis, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **IIS**, double-click the **Logging** icon.
4. If necessary, in the **Logging** configuration box, designate a log path to a location able to house the logs.
5. Under **Log File Rollover**, deselect the **Do not create new log files** setting.

IIST-SI-000244: Use TLS to send session IDs

IIS 10.0 website session IDs must be sent to the client using TLS.

To check compliance with IIST-SI-000244, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **Management**, double-click the **Configuration Editor** icon.
4. From the **Section**: drop-down list, select **system.webServer/asp**.
5. Expand the **Session** section.
6. Verify if **keepSessionIdSecure** is set to **True**.

If **keepSessionIdSecure** option is not set to **True**, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **Management**, double-click the **Configuration Editor** icon.
4. From the **Section**: drop-down list, select **system.webServer/asp**.
5. Expand the **Session** section.
6. Select **True** for the **keepSessionIdSecure** setting.
7. In the **Actions** pane, click **Apply**.

IIST-SI-000255: Set an application pool recycle time

The application pool for each IIS 10.0 website must have a recycle time explicitly set.

To check compliance with IIST-SI-000255, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
 - a. Click **Application Pools**.
 - b. Highlight an Application Pool.
 - c. In the **Action** pane, click **Advanced Settings**.
 - d. Scroll down to the **Recycling** section.
 - e. Expand the **Generate Recycle Event Log Entry** section.
 - f. Verify that **Regular time interval** and **Specific time** are set to **True**.

If both the **Regular time interval** and **Specific time** options are not set to **True**, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
 - a. Click **Application Pools**.
 - b. Highlight an Application Pool.
 - c. In the **Action** pane, click **Advanced Settings**.
 - d. Scroll down to the **Recycling** section.
 - e. Expand the **Generate Recycle Event Log Entry** section.
 - f. Set the **Regular time interval** and **Specific time** options to **True**.

IIST-SI-000257: Enable application pool pinging monitor

The application pools pinging monitor for each IIS 10.0 website must be enabled.

To check compliance with IIST-SI-000257, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
 - a. Click **Application Pools**.
 - b. Highlight an Application Pool.
 - c. In the **Action** pane, click **Advanced Settings**.
 - d. Scroll down to the **Process Model** section.
 - e. Verify that the value for **Ping Enabled** is set to **True**.

If the value for **Ping Enabled** option is not set to **True**, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
 - a. Click **Application Pools**.
 - b. Highlight an Application Pool.
 - c. In the **Action** pane, click **Advanced Settings**.
 - d. Scroll down to the **Process Model** section.

- e. Set the value for **Ping Enabled** to **True**.
- f. Click **OK**.

IIST-SI-000259: Enable application pool rapid fail protection settings

The application pool rapid fail protection settings for each IIS 10.0 website must be managed.

Note: If the IIS Application Pool hosts Microsoft SharePoint, this is not applicable.

To check compliance with IIST-SI-000259, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click **Application Pools**.
3. Complete the following steps for each Application Pool:
 - a. Click **Application Pools**.
 - b. Highlight an Application Pool.
 - c. In the **Action** pane, click **Advanced Settings**.
 - d. Scroll down to the **Rapid Fail Protection** section.
 - e. Verify that the value for **Failure Interval** is set to **5**.

If the **Failure Interval** option is not set to **5**, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Click **Application Pools**.
3. Complete the following steps for each Application Pool:
 - a. Click **Application Pools**.
 - b. Highlight an Application Pool.
 - c. In the **Action** pane, click **Advanced Settings**.
 - d. Scroll down to the **Rapid Fail Protection** section.
 - e. Set the value for **Failure Interval** to **5**.
 - f. Click **OK**.

IIST-SI-000261: Keep interactive scripts in unique and designated folders

Interactive scripts on the IIS 10.0 web server must be located in unique and designated folders.

To check compliance with IIST-SI-000261, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Determine whether scripts are used on the web server for the target website. Common file extensions include, but are not limited to: .cgi, .pl, .vbs, .class, .c, .php, and .asp.
2. All interactive programs must be placed in unique designated folders based on CGI or ASP script type. For modular and third-party applications, it is permissible to have script files in multiple folders.
3. Open the IIS 10.0 Manager.
4. Click the website name.
5. Click **Explore**.
6. Search for the listed script extensions. Each script type must be in a unique designated folder.

If scripts are not segregated from web content and in their own unique folders, your application is not compliant.

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

1. Open the IIS 10.0 Manager.

2. Click the website name.
3. Click **Explore**.
4. Search for the listed script extensions.
5. Move each script type to a unique designated folder.
6. Set the following permissions for the script folders:
 - Administrators: FULL
 - TrustedInstaller: FULL
 - SYSTEM: FULL
 - ApplicationPoolId: READ
 - Custom Service Account: READ
 - Users: READ
 - ALL APPLICATION PACKAGES: READ

IIST-SI-000262: Add restrictive access controls for interactive scripts

Interactive scripts on the IIS 10.0 web server must have restrictive access controls.

To check compliance with IIST-SI-000262, complete the following steps for each site hosted on the IIS 8.5 web server:

1. Determine whether scripts are used on the web server for the subject website. Common file extensions include, but are not limited to: .cgi, .pl, .vb, .class, .c, .php, and .asp. If the website does not utilize CGI, this finding is not applicable. All interactive programs must have restrictive permissions.
2. Open the IIS 10.0 Manager.
3. Right-click the website name and click **Explore**.
4. Search for the listed script extensions.
5. Review the permissions of the CGI scripts.
6. Verify that only the following permissions, or more restrictive permissions, are assigned:
 - Administrators: FULL
 - Web Administrators: FULL
 - TrustedInstaller: FULL
 - ALL APPLICATION PACKAGES: Read
 - ALL RESTRICTED APPLICATION PACKAGES: Read
 - SYSTEM: FULL
 - ApplicationPoolId: READ
 - Custom Service Account: READ
 - Users: READ

If the permissions are less, your application is not compliant.

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

1. Open the IIS 10.0 Manager.
2. Right-click the website name and click **Explore**.
3. Search for the listed script extensions.
4. Set the following permissions, or more restrictive permissions, for the CGI scripts:
 - Administrators: FULL
 - Web Administrators: FULL
 - TrustedInstaller: FULL
 - ALL APPLICATION PACKAGES: Read
 - ALL RESTRICTED APPLICATION PACKAGES: Read

- SYSTEM: FULL
- ApplicationPoolId: READ
- Custom Service Account: READ
- Users: READ

IIST-SI-000263: Remove backup interactive scripts

Backup interactive scripts on the IIS 10.0 server must be removed.

To check compliance with IIST-SI-000263 complete the following steps for each site hosted on the IIS 10.0 web server:

1. Determine whether scripts are used on the web server for the subject website. Common file extensions include, but are not limited to: .cgi, .pl, .vb, .class, .c, .php, .asp, and .aspx. The scope of this requirement is to analyze only within the web server content directories, not the entire underlying operating system. If the website does not utilize CGI, this finding is not applicable.
2. Open the IIS 10.0 Manager.
3. Right-click the website name and click **Explore**.
4. Search for the listed script extensions.
5. Search for the following files: *.bak, *.old, *.temp, *.tmp, *.backup, or "copy of..."

If files with these extensions are found, your application is not compliant.

If your application is not compliant, remove the backup files from the production web server.

IIST-SI-000264: Display the required DoD banner page

The required DoD banner page must be displayed to authenticated users accessing a DoD private website.

Note: This requirement is only applicable for private DoD websites.

If a banner is required, the following banner page must be in place:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests, not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

OR

If your system cannot meet the character limits to store this amount of text in the banner, the following is another option for the warning banner: "I've read & consent to terms in IS user agreem't."

Note: While DoDI 8500.01 does not contain a copy of the banner to be used, it does point to the RMF Knowledge Service for a copy of the required text. It is also noted that the banner is to be displayed only once when the individual enters the site and not for each page.

If the access-controlled website does not display this banner page before entry, your application is not compliant.

If your application is not compliant, configure a DoD private website to display the required DoD banner page when authentication is required for user access.

IIS 8.5 Security Technology Implementation Guide

The following sections describe the server and application tasks that you can complete to achieve IIS 8.5 STIG compliance in your BlackBerry AtHoc system.

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

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
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:
 - 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:
 - Request Header >> User-Agent
 - Request Header >> Authorization
 - Response Header >> Content-Type
8. Click **OK**.
9. In the **Actions** pane, 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 1.2\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 1.2\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 during transmission

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: Sufficient website log records to establish identity

The IIS 8.5 website 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 website 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-SI-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.


Verifying BlackBerry AtHoc is operational

After you complete a new installation 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.

Basic BlackBerry AtHoc test procedures

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


Log in

| ✓ | Description | Expected result |
|---|--|--|
| | Open a browser, and navigate to the Management System application. To do this, navigate to the <AtHoc-ENS-URL>. For example, <code>https://alerts.company.com</code> (if SSL is used). | The login page displays. |
| | Log in as an administrator. | The BlackBerry AtHoc management system home page displays. |
| | In the navigation bar, click  . | — |

Connect a client



| ✓ | Description | Expected result |
|---|--|--|
| | Install a desktop software client, as described in the <i>BlackBerry AtHoc Desktop App Installation and Administration Guide</i> . | The desktop software is installed on the user's computer and the user appears in the User manager. |

Custom attributes

| ✓ | Description | Expected result |
|---|---|-----------------|
| | Open the BlackBerry AtHoc management system. In the navigation bar, click  . | — |
| | Click Users > User Attributes . On the User Attributes page, click New . | — |
| | Create a multi-select picklist attribute whose Attribute Name is Test . | — |
| | Assign two pick-list values to the Test attribute: T1 and T2 . | — |

| ✓ | Description | Expected result |
|---|--|---|
| | Click Save to create the pick list attribute. | A pick list attribute named Test is created. |
| | 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

| ✓ | Description | Expected result |
|---|--|---|
| | In the navigation bar, click  . | The Settings page opens. |
| | From the Settings page, in the Users section, click User Attributes . | The User Attributes screen opens. |
| | On the User Attributes screen, select the attribute that is of the Type Path . | The Organizational Hierarchy settings page opens. |
| | In the Values section, add or delete a node. | — |
| | Click Save . | A Success message is displayed. |
| | In the navigation bar, click  . | The Settings page opens. |
| | From the Settings page, in the Users section, click Distribution List Folders . | The Distribution List Folders screen opens. |
| | On the Distribution List Folders screen, add or delete a node. | — |
| | Click Save . | A success message is displayed. |

Distribution lists

| ✓ | Description | Expected result |
|---|---|--|
| | In the navigation bar, click Users . Click Distribution Lists . | — |
| | 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 or export users

| ✓ | Description | Expected result |
|---|---|--|
| | In the navigation bar, click the Users > Users . | The Users page opens. |
| | Click More Actions > Import > Users . | — |
| | 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 computer. 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 in all required fields. | — |
| | Save the file with the name <code>test.csv</code> . | — |
| | Return to the management system and continue from the Import User File page. | — |
| | Select the import CSV file: <ol style="list-style-type: none"> 1. Click Browse. 2. In the file selection dialog, navigate to and select the <code>test.csv</code> file. 3. Right-click and select Open with to confirm the selection of the file. 4. Click Open. 5. Click Import. | The Import User Progress window opens and all users are successfully processed. The Last import field displays 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 <i>OK</i> and each user has a unique user ID. |
| | Compare the Users list with the import CSV file. To open the CSV file: <ol style="list-style-type: none"> 1. From the Users page, click More > Actions > Import > Users. 2. 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, click Users > Users . | 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

| ✓ | Description | Expected result |
|---|---|--|
| | In the navigation bar, click Alert > Alert Templates . | The Alert Templates page opens. |
| | Click New . | The New Alert Template screen opens. |
| | Create an alert template named SC1 . | — |
| | For the new template: <ol style="list-style-type: none"> 1. Select Available for Quick Publish. 2. Add the title and body. 3. Add a response option. 4. Target one or more users. 5. Select delivery to the following device: Desktop popup. 6. Check spelling. | — |
| | Save the alert template. | An alert template named SC1 is created. |

Alert publishing

| ✓ | Description | Expected result |
|---|--|---|
| | In the navigation bar, click Alerts > New Alert . | The Select from Alert Templates page opens. |
| | Publish an alert template: <ol style="list-style-type: none"> 1. Select the SC1 alert template and click Edit. 2. In the Target Users section, click review the users in the Targeting Summary. 3. Click Review and Publish. 4. 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 template activation. |
| | Wait up to two minutes for the alert to arrive on the users desktop. After you receive the pop-up, click Acknowledge and Close . | The desktop pop-up displays and an audio alert plays (if speakers are connected and audio is enabled). Upon acknowledgment, the pop-up must disappear. |


Self Service

| ✓ | Description | Expected result |
|---|--|---|
| | <p>From the user's computer, right-click the AtHoc desktop software system tray icon (🔊) and select Access Self Service.</p> <p>For Mac users, left-click to open the status item menu.</p> | <p>A new browser window displays the Self Service Inbox which contains the newly published alert (but only if the user authentication is set to Auto\Windows authentication.)</p> <p>(Mac) The Safari browser is launched for any service selected from the status item menu.</p> |
| | Navigate through the other Self Service tabs and verify that the displayed information is correct. | The published alert appears in the list with a Live status. |

Alert tracking reports

| ✓ | Description | Expected result |
|---|---|---|
| | In the navigation bar, click Alert > Sent Alerts . | 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. | <p>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.</p> <p>You can also see a drop-down list of detail reports.</p> |
| | Click Export > Export Full Report . Note that you must have Excel 2003 or higher installed on your computer to open the report. | <p>You are asked to open the .csv file. The Detailed Alert tracking report must open and display the alert details and track information.</p> <p>You can see the users who received and acknowledged the alert.</p> |

Audio files

| ✓ | Description | Expected result |
|---|--|--|
| | In the navigation bar, click  . | — |
| | In the Basic section, click Audio Files . | The Audio Files page opens. |
| | Click New . | The New Audio File dialog opens. |
| | Enter an audio name and upload a .wav file that is larger than 1 MB but not more than 2 MB. | <p>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.</p> |

| ✓ | Description | Expected result |
|---|--|-----------------------------|
| | After selecting the file to be uploaded, click Save . | # Return to Audio Files. |

Error logs

| ✓ | Description | Expected result |
|---|---|---|
| | 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 | 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, and 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: None

Message: The installation stops because the following prerequisites are missing on the server. Install these components first: <List of Missing Prerequisites>

Cause: The listed prerequisites are not installed.

Resolution: Install the missing prerequisites.

Error code: 2147217900

Message: No additional message

Cause: During a new installation, the `ngad` user password does not meet Microsoft SQL Server password requirements.

Resolution: Do not use the default password for `ngad`. Enter a custom password that meets the strong password requirement of Microsoft SQL Server.

Error code: 2147217900

Message: The operating system returned the error "5(Access is denied." while attempting to "restoreContainer::ValidateTargetForCreation" on <path>."

Cause: Microsoft SQL Server service account does not have permission to create files.

Resolution: Change the service account to "Local System account."

Error code: 2147217900

Message: No additional message

Cause: The transaction log for database NGADDATA is full.

Resolution: Shrink the NGADDATA database and back up the transaction log.

Error code: 2147217900

Message: No additional message

Cause: The Application server logon account did not have a logon on the Database server, or did not have a Microsoft SQL Server logon with system administrator rights.

Resolution: Grant the correct permissions or switch to an account that has the correct permissions.

Error code: 2147217900

Message: 3a CreateUsers Error running ATH_CREATE_USERS sp: error -2147217900, exec dbo.ATH_DROP_USERS @dropLogin = 1

Cause: Microsoft 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.

Resolution: Do not use the default password for ngad. Enter a custom password that meets the strong password requirement of Microsoft SQL Server.

Error code: 2147319779

Message: Library not registered

Cause: `sccrun.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.

Resolution: Register the 32-bit version of `sccrun.dll`.

Error code: 2147467259

Message: Unspecified error

Cause: 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.

Resolution: Make sure that the Microsoft SQL Server service is running or call BlackBerry AtHoc customer support.

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 tables describe objects that are duplicated to the organization on the target server.

| |
|---|
| Feature: Server configuration |
| Objects: <ul style="list-style-type: none">• Cascading systems• Images• Gateways and devices• Health monitors (Actions only, not Global Health Monitors.) |
| Duplicates across servers: <ul style="list-style-type: none">• Super enterprise/enterprise (from SRC/SRC)• Enterprise/sub (from SRC/SRC)• Basic (from SRC) |
| Feature: System Setup (Organization 3) |
| Objects: <ul style="list-style-type: none">• Attributes• Channels |
| Duplicates across servers: <ul style="list-style-type: none">• Super enterprise/enterprise (from SRC/SRC)• Enterprise/sub (from SRC/SRC)• Basic (from SRC) |
| Feature: Standard Organization Configuration |
| Objects: <ul style="list-style-type: none">• Provider configuration• 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: Standard Organization Configuration

Duplicates across servers:

- Super enterprise/enterprise (from SRC/SRC)
- Enterprise/sub (from SRC/SRC)
- Basic (from SRC)

Feature: Custom organization configuration

Objects:

- Attributes
- Channels
- Audio
- Templates
- Mass devices
- Custom DLs (Except static list user membership [see Users].)
- Alert templates (Except targeting of individual users [see Users].)
- Reports
- Schedules

Duplicates across servers:

- Super enterprise/enterprise (from SRC/SRC)
- Enterprise/sub (from SRC/SRC)
- Basic (from SRC)

Feature: Custom organization configuration

Objects:

- Operator permissions
- Users, their DL memberships, and targeting (Organization users, Static DL user membership, alert templates individual user targeting)

Not duplicated across servers:

- Super enterprise/enterprise (from SRC/SRC)
- Enterprise/sub (from SRC/SRC)
- Basic (from SRC)

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

Feature: Server configuration

Objects:

- Cascading systems
- Images
- Gateways and devices
- Health monitors (Actions only, not Global Health Monitors.)

Not created on the same server

- Super enterprise (from System Setup 3)
- Enterprise (from 5)
- Sub (from ENT)
- Basic (from 6)

Not duplicated on the same server:

- Super enterprise (from SRC)
- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: System setup (Organization 3)

Objects:

- Attributes
- Channels

Not created on the same server:

- Super enterprise (from System Setup 3)
- Enterprise (from 5)
- Sub (from ENT)
- Basic (from 6)

Not duplicated on the same server:

- Super enterprise (from SRC)
- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: Standard organization configuration

Objects:

- Provider configuration
- 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

Created on the same server:

- Super enterprise (from System Setup 3)
- Enterprise (from 5)
- Sub (from ENT)
- Basic (from 6)

Duplicated on the same server:

- Super enterprise (from SRC)
- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: Custom organization configuration

Objects:

- Attributes
- Channels
- Audio
- Templates
- Mass devices
- Custom DLs (Except static list user membership [see Users].)
- Alert templates
- Reports

Feature: Custom organization configuration

Created on the same server:

- Super enterprise (from System Setup 3)
- Enterprise (from 5)
- Basic (from 6)

Not created on the same server: Sub (from ENT)

Duplicated on the same server:

- Super enterprise (from SRC)
- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: Custom organization configuration

Objects: Users, their DL memberships and targeting (Organization users, static DL user membership, alert templates, individual user targeting)

Not created on the same server:

- Super enterprise (from System Setup 3)
- Enterprise (from 5)
- Sub (from ENT)
- Basic (from 6)

Not duplicated on the same server:

- Super enterprise (from SRC)
- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

BlackBerry AtHoc Customer Support Portal

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

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

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

Documentation feedback

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

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

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

Legal notice

©2023 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

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

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

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

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

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

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

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

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

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

Published in Canada