BlackBerry AtHoc

FAX Installation and Configuration Guide

Last Published: July 2019

Contents

Overview

This guide describes the steps to install and configure the Twilio Fax plug-in for BlackBerry AtHoc NDS. The Twilio Fax plug-in for BlackBerry AtHoc is a plug-in of NDS, which is a dedicated server that processes and delivers alert messages from the NDS host services (plug-ins). For more information about NDS and its prerequisites, see the BlackBerry AtHoc NDS Installation and Upgrade Guide.

Twilio account requirements

You require a Twilio for Enterprise account configured with the following settings:

- SSL certificate validation must be enabled.
- Public Key Client Validation must be enforced.
- Your Twilio account must have the necessary permission to upload the BlackBerry AtHoc public key to the Twilio console and to create the private key that is used to sign requests. This must be performed by an administrator user of your Twilio account.

Administration account requirements

Before you install, make sure that the user account that you use meets the following criteria:

- The administrator user that installs NDS and the plug-ins should have the same Windows administration user account as the BlackBerry AtHoc user account. The BlackBerry AtHoc application and NDS are run on IIS, and the IIS USR or NETWORK SERVICE group needs access to the AtHocENS folder.

  Note: Additionally, the services might need DLLs to be either GACed, located in a folder with access permission, or copied to the folder or /bin folder of the program.
- This user needs to be an administrator account in Microsoft SQL Server:
  - The SA account must be a system administrator.
  - NGAD can be public in Server Roles.
  - NGAD becomes the owner of the database during the NDS installation.

    Note: This can conflict with using Windows authentication, where the Database Owner (dbo) is supposed to be the Windows service account.The Administrator user, IIS user, and Network service user need EDIT access to AtHocENS folders

Software requirements

To install the Twilio Fax plug-in, you must have the following software installed in your environment:

- Windows Server 2012 or Windows Server 2016
- Microsoft SQL Server Standard 2008 R2 or Microsoft SQL Server 2012 with the SQL Server Agent Service configured as “Automatic Start”
- Microsoft System CLR Types for Microsoft SQL Server 2012.
- Internet Information Services (IIS) Role Service.
- Microsoft .NET Framework Version 4.7.2.
- Microsoft Management Framework 3.0: (PowerShell x64 bit, 3.0 Support).
- External IPs on your app server

- IIS extension enabled for Microsoft ASP.NET
- BlackBerry AtHoc release 7.6 and later when installing the application server in combination mode. Combination mode is used when the AtHoc Management System is installed on the application server with NDS.

Hardware and firmware requirements

To install the Twilio Fax plug-in, your environment must meet the following hardware requirements:

- A minimum of Dual-Core Dual CPUs (2 Dual-Core CPUs such as Xeon 51xx family, Xeon E53xx family or X53xx family) 2 GHz or higher
- One database server core for each of the two application server cores
- **Recommended**: Dual, redundant Intel NICs and power supplies.
- If using Broadcom NICs
  1. Make sure that the latest drivers are installed.
  2. Disable the TCP Chimney feature. See http://support.microsoft.com/kb/951037 for more information.
- Disk space for storage on a RAID 5, RAID 0+1, or RAID 10 configured disk system.The exact allocation of disks depends on the hardware configuration.

Important: These requirements are for a small-scale installation. For a large-scale installation, contact BlackBerry AtHoc support for assistance.

Set up your Windows server to support the Fax plug-in installation

Before you install the Fax plug-in, you must configure the following setting on the Windows server that the Fax plug-in will be installed on:

1. Open **Server Manager** > **Dashboard**.
2. In the top right corner, click **Manage**.
3. Select **Add Roles and Features**.
4. Click **Next**
5. Select the server where installation will be performed.
6. Click **Next**.
7. On the **Server Roles** tab, perform the following tasks:
   a) Expand **Web Server (IIS)**.
   b) Expand **Application Development**.
   c) Select **Application Initialization**.
8. Click **Next**.
9. On the **Server Roles** tab, perform the following tasks:
   a) Expand **Web Server (IIS)**.
   b) Expand **Security**.
   c) Select **Basic Authentication**.
10. Click **Next**.
11. Click **Install** to install the selected components.

Installing the NDS platform

Before you install the Twilio Fax plug-in, you must install the NDS platform. For information about how to install NDS, see BlackBerry AtHoc NDS Installation.

Note: When NDS is installed, an additional service used for fax delivery called PDF Service is also installed. When the pop-up message appears to install the PDF Service, make sure that you select Yes to install this service.

Configure the PDF service

Before you begin:

- Install the NDS platform

1. Open **IIS Manager**.
2. In the left panel, click **Application Pools**.
3. In the list of application pools, click **AtHoc.NDS.PDFService**.
4. In **Advanced settings**, set the following values:
   a) In the **General** section, set the **Start Mode** value to **AlwaysRunning**.
   b) In the **Process Model** section, set the **Idle Time-out (minutes)** value to **0**.
   c) In the **Process Model** section, set the **Maximum Worker Processes** value to **1**.
   d) In the **Recycling** section, set the **Regular Time Interval (minutes)** value to **1440**.
5. In the left panel, click **Sites**.
6. Expand **Default Web Site**.
7. Right-click **PDFService** and select **Manage Application**.
8. Select **Advanced Settings**.
9. Set the **Preload Enabled** value to **True**.

Copy the FAX plug-in to the NDS server

To be able to install the Fax plug-in software, you must copy the Fax-plug-in software to the NDS sever:

1. To download the software, navigate to `\\fsg2002sjc-i05.athoc.com\Released - GA \I2\HostedFax\2.9.20`.
2. Copy the `AtHoc.Plugin_Fax.zip` file to the NDS Server.
3. Right-click the zip file and click **Unblock** to unblock the zip file.
4. Unzip the package into the NDSplug-in folder located at `C:\Program Files (x86)\AtHocENS \DeliveryServer\Plugin`.
5. Restart IIS.

Enable basic authentication in the PDF Service and the R service

1. In **Computer Management** > **System Tools** > **Local Users and Groups**, create the following:
   - A new user group called **FaxUser**
   - A new user called **faxplugin** and select **Password never expires**. Do not use URL specific special characters (@/%^#) in the username and password.
2. In **Local Users and Groups**, click **Users**.
3. On the **Users Properties** screen, in the **Members** list, click **faxplugin**.
4. Click **Remove**.

   You must remove the **faxplugin** user from **Local Users and Groups** because user groups have access to multiple directories on the computer. By default, new users are attached to the users group.
5. Click **OK**.
6. In the **Local Users and Groups** folder, select **FaxUser** from the list.
7. In the **FaxUsers Properties** dialog box, complete the following tasks:
   a) In the **Select this object type** field, enter `Users or Built-in security principals`.
   b) In the **From this location** field, enter `ODC-NDS-DEV1`.
   c) In the **Enter the object names to select**field, enter `ODC-NDS-DEV1\faxplugin`.
8. Click **OK**.
9. Click **Add**.
10. Click **Apply**.
11. In **IIS Manager**, go to **Sites** > **Default Web Site** > **PDFService**.
12. In the **Authentication** section, enable **Basic Authentication** and disable **Anonymous Authentication**.
13. Repeat steps 11 and 12 for R services to enable basic authentication and disable anonymous authentication.
14. Add the following HTTP configuration parameters to the **nds.plugins.fax** configuration file:
```
<ndsHTTPAuthEnabled>true</ndsHTTPAuthEnabled><!-- HTTP Basic Auth Username/ Password of NDS IIS (R & PDF service). --><ndsHTTPUsername>faxplugin</ ndsHTTPUsername><ndsHTTPPassword>Test1234*</ndsHTTPPassword
```
   For more information about Fax plug-in configuration parameters, see Update configuration parameters.
15. Restart the **IIS** and **AthocDeliveryService** services.

Test basic authentication

1. Open **IIS** and right-click **PDFService**.
2. In the **Manage Application** section, select **Browser**.

   Note: The PDF Service should open in a browser showing a username and password dialog box. If you do not see the the username and password dialog box, basic authentication has not been enabled correctly for the PDF Service. If you cannot see the dialog box, follow the steps in Enable basic authentication in the PDF Service and the R service.
3. Enter your username and password.
4. Click **OK**. A 404 error will be displayed due to the additional security on the website.
5. Repeat steps 1 to 3 for R services.

Public key authentication

This section describes the additional setup and configuration steps required to activate public key authentication requests from NDS to Twilio.

Prerequisites for public key authentication

To activate public key authentication requests from NDS to Twilio, you must perform the following tasks:

- The Twilio master account or subaccounts that are used to send faxes must have **Public Key Client Validation** enforced.

  Note: This feature requires the Twilio Enterprise Plan. Contact Twilio sales if you do not have this feature enabled.

  To check if the public key client validation is enforced, log in to the Twilio site at https://www.twilio.com/login.

  - To enforce public key validation for the Master account

    1. Log in to the Twilio site at https://www.twilio.com/login.
    2. In the top right, click  .
    3. Click **Settings**.
    4. Select **ENFORCED** under **Public Key Client Validation**.
  - To enforce public key validation for subaccounts

    1. In the master account, in the top right corner, click  .
    2. Select **Subaccounts**.
    3. Beside the name of a subaccount, click **View subaccount**.
    4. Select **ENFORCED** under **Public Key Client Validation**.
- To allow webhook status callbacks and PDF requests from Twilio to NDS, SSL Certificate Validation must be enabled for the Twilio master account and subaccounts.
- You must have a .pfx certificate file that has both private and public keys.

Import certificate(.pfx) to NDS

You can use NDS Console to Import Certificate (.pfx) file to NDS.

1. Start the NDS Console.
2. Click the **Utilities** tab.
3. In the **Import System Certificate** section, click **Load File** and browse to your certificate.
4. Name your certificate **FaxCert**.
5. Click **Load**.
6. Enter your password. After the certificate is imported, the FaxCert.pfx certificate is displayed under `nds.certificate.repository` in NDS configuration.
7. Add the following account configuration code in `nds.plugins.fax.accountConfig` for the account to be used for publishing fax alerts.

nds.plugins.fax.accountConfig

```
<orgId>0</orgId> <hashAlgorithm>SHA256</hashAlgorithm>
  <systemCertName>FaxCert</systemCertName>
 </certSigningInfo></AccountConfig>
```

Note: The `systemCertName` must match the certificate name provided during import.

Extract the public key from the .pfx file

You must extract the public kiey from the .pfx file so that it can be uploaded to Twilio. You can use the OpenSSL tool to extract the public key from the `.pfx` file.

Before you begin:

- OpenSSL must be installed on your computer and NOT on the NDS server.

1. Open a command prompt
2. Type `cd D:\openssl\openssl-0.9.8h-1-bin\bin` to navigate to the `bin` directory. If you installed OpenSSL in a different path, provide that path.
3. Execute the following two OpenSSL commands to extract public key from `.pfx` file.

   It is assumed that the .pfx certificate is located at `D:/SSLCertificate/mycert.pfx`. If your certificate file name and path are different, replace the path and file name in the bolded text with the path and file name that you have used.

   ```
   #(extract keypair from mycert.pfx)
    openssl pkcs12 -in D:/SSLCertificate/mycert.pfx  -nocerts -nodes -out   D:/
   SSLCertificate/keypair.key
   ```

   A `public_key.pem` file is created in the same location. This `public_key.pem` file will be required in the next step.

Submit the NDS public key to Twilio

Before you begin:

- Extract the public key from the .pfx file

1. Log in to your Twilio account.
2. Select the Twilio account that you want to generate signing keys for. It can be the Twilio master account or any one of the subaccounts.
3. Verify that you have selected the required Twilio account. The account that is currently selected is displayed in the breadcrumbs at the top of the screen.
4. In the left panel, click **All Products & Services**.
5. In the left panel, scroll down and click **Runtime**.
6. On the **Runtime Overview** page, click **Credentials**.
7. On the **Credentials** page, click **Create new Credential**.
8. Enter following values in the **New Credential** form:
   a) In the **Type** drop-down list, select **Public Key**.
   b) In the **Friendly Name** field, type `NDS`.

c) In the **Public Key** field, copy the contents of the public_key.pem file that you generated using the OpenSSL tool. To copy the contents, open the public_key.pem file in Notepad and copy the contents. To prevent the authentication from failing, the entire contents of public_key.pem file must be copied and should not be modified.

9. Click **Create**.
10. On the **Confirmation** page, copy the **SID**.
11. Click **Done**.
12. Add the SID to the <ndsPublicKeySID> parameter in NDS Fax configuration as shown in this example:<ndsPublicKeySID>CR7fe078b7d4ee7c8fbad0d1bb9f90c5d1</ndsPublicKySID>

Generate a signing key in Twilio

Before you begin: Submit the NDS public key to Twilio

1. Log in to the Twilio account to be used for public key authentication.
2. In the left panel, click **All Products & Services**.
3. In the left panel, scroll down and click **Runtime**.
4. On the **Runtime Overview** page, click **API keys**.
5. Click **Create new API Key**.
6. In the **Friendly Name** field, enter a friendly name for the API key.
7. In the **Key Type** drop-down list, select **Standard**.
8. Click **Create API Key**.
9. Click **Submit**. The signing key and secret are displayed.
10. Update the signing key SID and secret in the following NDS parameters for the Fax plug-in. For information about updating parameters, see Update configuration parameters.

```
<twilioSigningKey>SKbb2509a2188d0d8200f3a6e1ec8bc034</twilioSigningKey>
<twilioSigningSecret>pj7Pc7ie5aA36N17ykynLhw2pvA7b7uI</twilioSigningSecret
```

11. Select **Got it**
12. Click **Done**.
13. On the **Signing Key Public Authentication** page, click **Cancel**.
    The signing key is displayed on the signing key listing page.

Update configuration parameters

To configure your environment, you can update the following `nds.plugin.fax` parameters. The AthocDeliveryService and IIS must be restarted after you make any updates to these parameters.

Parameter	Steps
twilioFromNumber	1. Log in to Twilio at https://www.twilio.com/login. 2. Select an account. 3. In the left panel, click **All Products & Services**. 4. Select **Phone Numbers** and select **Verified Caller IDs**. 5. Click + and enter the country and phone number. 6. To verify this number as the From Number, receive a call or text. 7. Enter the verified number in the configuration with the country code.
responseUrl	Replace "https://www.myndsserver.com/R/" with your server name.
pdfUrl	Replace "https://www.myndsserver.com/PDFService" with your server name.
ndsHTTPAuthEnabled	For information about this setting, see Enable basic authentication in the PDF Service and the R service.
twilioAccountSID	To find the account SID, do the following: 1. Log in to Twilio at https://www.twilio.com/login. 2. Select the account. 3. In the console dashboard that opens, note the ACCOUNT SID.
twilioAuthCode	To find the auth code, do the following: 1. Log in to Twilio at https://www.twilio.com/login. 2. Select the account to be used. 3. In the console dashboard that opens, note AUTH TOKEN.
twilioSigningKey	Enter your Twilio signing key, signing secret, and the public key. For information about getting keys, see Generate a signing key in Twilio.
twilioSigningSecret	
ndsPublicKeySID	
ndsHTTPUsername	For information about this setting, see Enable basic authentication in the PDF Service and the R service.
ndsHTTPPassword	For nformation about this this setting, see Enable basic authentication in the PDF Service and the R service.

The following is an example showing the parameters described above:

```
<FaxConfig xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">    <requestsPerSec>50</requestsPerSec>
```

```
  <maxTasksPerExecution>200</maxTasksPerExecution> <maxBacklog>1000</
maxBacklog> <minBatchSize>10</minBatchSize> <taskTimeout>600</taskTimeout>
 <configKey>FaxPlugIn</configKey> <selfTestInterval>30</selfTestInterval>   <!--
 Provide validated From number for the Twilio account.  --><twilioFromNumber>
+15555552530</twilioFromNumber>   <!-- For following 2 URLS provide the
 correct hostname in the URL --><responseUrl>https://myndsserver.com/
R/</responseUrl>  <pdfUrl>https://myndsserver.com/PDFService</pdfUrl>
   <!-- This zoom level of the PDF generated for fax.  Keep it's value
 as 1 ( default value) --> <pdfZoomLevel>1</pdfZoomLevel>   <!-- If
 this is set to true,  HTTP Basic Auth will be used for all incoming
 requests (Webhook status callbacks, PDF requests) to NDS from Twilio -->
 <ndsHTTPAuthEnabled>true</ndsHTTPAuthEnabled>     <encryptCredential>false</
encryptCredential>   <!-- Parameters given below will be encrypted by
 AtHocDeliveryService on first run if encryptCredential is set to false -->
  <!-- SID of Twilio Account & its auth code to be used for fax submision --
>  <twilioAccountSID>ACb8959fec31218c7ad37ad4f094a55538</twilioAccountSID>
   <!-- Twilio Authcode is not used for public key authentication. It is
 used for validating X-Twilio-Signatures of incoming status call backs & PDF
 requests from Twilio --><twilioAuthCode>88c6b6a4d006ff41f031b088dbc492a2</
twilioAuthCode><!-- Twilio Signing key (i.e, API Key) & its  secret -->
  <twilioSigningKey>SKbb2509a2188d0d8200f3a6e1ec8bc034</twilioSigningKey>
  <twilioSigningSecret>pj7Pc7ie5aA36N17ykynLhw2pvA7b7uI</twilioSigningSecret>
  <!-- SID of NDS Public key. This SID is provided by Twilio, after we upload NDS
 public key to Twilio--> <ndsPublicKeySID>CR7fe078b7d4ee7c8fbad0d1bb9f90c5d1</
ndsPublicKeySID>     <!-- HTTP Basic Auth Username/Password of NDS IIS
 (R & PDF service). --> <ndsHTTPUsername>faxplugin</ndsHTTPUsername>
 <ndsHTTPPassword>Test1234*</ndsHTTPPassword> </FaxConfig>
```

OpenSSL in Microsoft Windows

This section outlines how to install OpenSSL and verify it to extract the public key from our `.pfx` certificate file.

Install OpenSSL in Microsoft Windows

Before you begin:

- Verify that you are using one the following operating systems: Windows 2000, XP, Vista, or 7; Windows Server 2003 or 2008 2000/ XP / 2003 / Vista / 2008 / 7

1. Download OpenSSL from http://gnuwin32.sourceforge.net/packages/openssl.htm.
2. Click the .zip file for the Binaries option.
3. Extract the downloaded .zip file to `D:/openssl/`. The folder structure after extraction will be: `D:\openssl \openssl-0.9.8h-1-bin`

   Note: If drive D is not available, use `C:/openssl` or any other available drive on your computer.

   The version of OpenSSL may be different depending on the version that is available when you perform the installation.

Verify the OpenSSL installation

1. Open a Windows command prompt as an administrator
2. Type `cd D:\openssl\openssl-0.9.8h-1-bin\bin` to navigate to the location where you extracted the `openssl` zip file. If you did not install the file in this location, update the path to the correct location.
3. Type `openssl` in the command prompt and press **Enter** to execute OpenSSL.
4. In the `openssl` prompt, type `help` and press **Enter** in the `openssl` prompt. If OpenSSL was installed successfully, you, you should see the help for OpenSSL.
5. Type `quit` and press **Enter** to exit.

BlackBerry AtHoc customer portal

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

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

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

Legal notice

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

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

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

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

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

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

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

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada