BlackBerry AtHoc

Cisco IP Phone Blast NDS Installation Guide

Last Published: May 2020

2.9.7

Contents

Overview..... 5

Verify installation prerequisites..... 6

System requirements..... 6
Supported phone models..... 7
Before you begin..... 7
Create a working folder..... 7

Install and configure the IP Phone Blast on AtHoc NDS..... 8

Install the IP Phone Blast on NDS..... 8
Configure the Blast system..... 9
Install TTS on a new NDS server..... 11
System generated certificates..... 12
SSL private key validation..... 12

Upload certificates to CUCM..... 13

Upload CA certificate..... 13
Upload App certificate..... 13
Upload phone certificate..... 13

Using fully qualified domain names 15

FQDN between blast notifier and CUCM..... 15
FQDN between blast notifier and Cisco phones..... 15
Possible conflicts..... 16

Copy Tomcat certificate to NDS..... 17

Download a Tomcat certificate from CUCM..... 17
Import the Tomcat certificate to the Windows Certificate store..... 17

Update CUCM authentication URLs..... 18

Configure NDS for Cisco IP phones..... 19

Obtain the Blast plug-in..... 19
Add the ucmIpPhone key to the NDS server..... 19
Configure the database server..... 19

Set up the Windows server..... 21

Windows Roles and Features Error.....23

Verify the NDS installation.....24

Errors.....24

Supported Cisco IP phones.....26

BlackBerry AtHoc Customer Support Portal.....29

Legal notice.....30

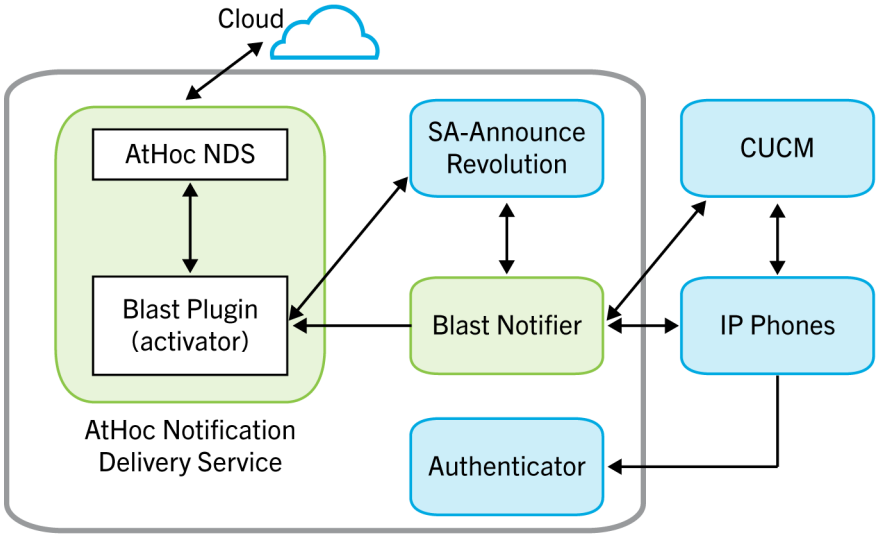
Overview

The `BlastSystemSetup.exe` is an installation and configuration utility comprised of a collection of SA-Announce Revolution modules that integrate with BlackBerry AtHoc NDS to provide alert notifications to Cisco IP Phones. The utility installs all of the required Blast System modules and prompts the administrator to input configuration data. This includes SSL certificate creation, storage, and binding on the host system.

The following modules are included:

- SA-Announce Revolution version 1.1.0.5 or later release. Notification broker.
- Blast Activator (NDS plug-in) version 1.1.0.5 or later release. Receives notification activation events from NDS and passes them to Revolution for dispersal.
- Blast Notifier version 1.1.0.5 or later release - Delivers content to Cisco IP phones. Provides feedback to the Activator, which provides it to NDS.
- Authenticator version 1.1.0.5 or later release - Authenticates Cisco IP phone requests.

The Blast System supports SSL on all communication interfaces.



Caveats

CUCM Extension Mobility is not supported by the Blast System.

For information about how to set up NDS for Avaya IP Phone Blast, see the *BlackBerry AtHoc Avaya IP Phone Blast NDS Installation Guide*.

For information about how to set up IP Phone Blast in BlackBerry AtHoc, see the *BlackBerry AtHoc IP Phone Gateway Setup and Operation Guide for Avaya and Cisco IP Phone Blast*.

Verify installation prerequisites

The following sections describes the system requirements that are necessary for installing and configuring AtHoc Blast System on the AtHoc Notification Delivery Server (NDS).

System requirements

System requirement	Description
AtHoc NDS v2.9.7	If necessary, upgrade NDS before proceeding.
Windows Server 2016	Supported Windows Server. **Note:** A number of Windows roles and features are required. These are automatically configured by the Blast System utility.
Microsoft SQL Server	Microsoft SQL Server 2016
Microsoft .NET Framework 4.7.2	**Windows 2016:** This server comes with Microsoft .NET Framework 4.7 installed. If you have not upgraded to Microsoft .NET Framework 4.7.2, the Blast System attempts to install it. **Note:** If an Internet connection is not available, the utility aborts the Blast System installation. You must then manually install .Microsoft .NET Framework. Download the Microsoft .NET Framework 4.7.2 full installer at: https://dotnet.microsoft.com/download/dotnet-framework/net472.
Server	106.6 MB free space for installation, 8 GB memory, and 2 CPU cores. Single multicast IP address to endpoints for the text-to-speech functionality. This IP address is provided by your IT department.
Microsoft VS++2010SP1x86 Redistributable	Required and automatically installed by the install utility if internet access is available. **Note:** If an internet connection is not available, the utility aborts the Blast System installation. You must then manually install Microsoft VS. Download <VC++2010SP1x86_Redistributable>.
CUCM v 8.x, 9.x, 10.x, 11.x	CUCM 8 or later is required for security features.
Default Ports	Cisco phone registration and communication with SA Revolution occurs on port 8008. Cisco phone communication port 80. Ports are configurable.
Default Protocols	RTP and HTTP
Voice Streaming	RTP through via multicast over UDP

Supported phone models

All models that support IP phone services support Blast Notifier in non–secure mode. Only phones that support the Security by Default feature are supported in secure mode.

To get a list of the devices that support a particular feature using CUCM Reporting, perform the following steps:

1. In the Cisco Unified Reporting main window,
2. Click **System Reports**.
3. Click the **Unified CM Phone** feature and generate the report.
4. From the **Feature** list, select **IP Phone Services** or **Security by Default**.
5. Click **Submit**.

For a list of Cisco supported phones, see Supported Cisco IP phones.

Before you begin

- If your Windows server does not have Internet access, and does not have Microsoft .NET 4.7.2, then click Microsoft .NET 4.7.2 full installer to download Microsoft .NET and manually install it before running the AtHoc Blast System utility.
- If Windows server does not have Microsoft VS++2010SP1x86, then click><VC++ +2010SP1x86_Redistributable> to download the redistributable VS and manually install it before running the AtHoc Blast utility.
- Ensure AtHocENS is installed prior to installing the AtHoc Blast System. The AtHocENS must be located at:

  <DRIVE>:\Program Files (x86)\AtHocENS\Installation

  The Blast System installation fails if AtHocENS is located somewhere else.
- You will need the following data to input into the Blast System configuration user interface that automatically launches after installation:
  - IP address of the server where the Blast System is being installed
  - Port number if not using the default 8008 port
- Place the Blast System executable file and the SA-Announce Revolution license file that you obtained from AtHoc Sales in a working folder on the server on which the AtHoc Blast System will be installed.
- Place the BlastConfiguration folder that you obtained from AtHoc sales in a folder on your local computer. This folder contains the BlastConfiguration.bat and BlastConfiguration.sql files.
- You will need the following information before you configure the database server:
  - The database server name.
  - The SA user password.
  - The name of the ngdelivery database.

Create a working folder

During the installation and configuration process, you will need to access files and export files from one system into a local directory. To make it easier to do this, before you begin any of the installation and configuration tasks, you should create a working folder on your local drive and add the following files to it:

- `CiscoBlastSystemSetup.exe`: Contact the BlackBerry AtHoc Build and Release group for this file.
- The `SA-AnnounceRevolution.license` file.
- The BlastConfiguration folder: Contact the BlackBerry AtHoc Build and Release group for this file.

Install and configure the IP Phone Blast on AtHoc NDS

This section describes how to install and configure the IP Phone Blast on the AtHoc Notification Delivery Server (NDS).

Install the IP Phone Blast on NDS

Important: Before you begin, verify that you are running on NDS. Installation will be unsuccessful if AtHoc NDS is not located at: <Drive>:\Program Files (x86)\AtHocENS\Installation.

The Blast System utility is a wizard that installs all three BlackBerry AtHoc modules.

1. Go to the working folder where you placed the `CiscoBlastSystemSetup.exe` file.
2. Right-click the `CiscoBlastSystemSetup.exe` file and select **Run as administrator**.
3. On the **User Account Control** pop-up screen, click **Yes**. The Blast System Installer opens.
4. On the **Welcome** screen, click **Next**. The Blast system software requirements appear on the screen
5. Click **Next**.
6. Verify the following information before continuing with the installation:

Screen	Action
Information	• If the server meets all the listed requirements, click **Next**. • If the server is running AtHoc NDS 2.9.7 but does not have Microsoft .NET 4.7.2 and VS++2010SP1x86 and has an internet connection, click **Next**. • If the server is running AtHoc NDS 2.9.7 but does not have Microsoft .NET 4.7.2 and VS++2010SP1x86 and does not have an internet connection, click **Cancel**. You must manually install Microsoft .NET 4.7.2 and VS++2010SP1x86, and then run the Blast System utility again. **Note:** The utility checks for the specific versions. If they are not found, the installation does continue and displays an error message. Install the appropriate program versions and then run the Blast System utility again.

7. Select **I have read and accept the license terms**.
8. Click **Install**. The installation process begins.
9. In the **Select Destination Location** screen, enter a selected destination location using the following format:

```
<DRIVE:>:\Program Files (x86)\Syn-Apps\CiscoBlastSystemSetup
```

   Note: The AtHoc NDS must be located at: <Drive>:\Program Files (x86)\AtHocENS\Installation.

   First installation only: Blast System updates target the existing installation folder designated here.
10. Click **Next**.
11. In the **Environment Requirements** screen, select the check box beside each item. Installation does not continue until all check boxes are selected.

    Note: You are required to select the check boxes only once. The system considers the state of the check boxes from the original installation whenever the system runs updates.
12. Click **Next**.

13. Click **Install**.
14. In the **Completing the BlastSystemSetup Setup Wizard** screen, select **Launch BlastSystemSetup Configuration**.
15. Click **Finish**. By default, the Blast System utility automatically launches the Blast System Configuration interface after the installation is finished.

The `CiscoBlastSystemSetup.exe` extracts the installers needed to set up the Windows roles and features and installs the Blast System modules. However, these installers do not run until you provide the necessary data in the `CiscoBlastSystemSetup` configuration interface.

Configure the Blast system

If you have not selected the **Launch CiscoBlastSystemSetup Configuration** check box on the last installation screen, navigate to the folder `<DRIVE>:\Program Files (x86)\Syn-Apps\BlastSystem\Setup\Configuration`, right-click the `CiscoBlastSystemConfig.exe` file and run as administrator.

1. On the User **Account Control** pop-up screen, click **Yes**.
2. On the **Blast System Configuration** screen, complete the following fields:

Field	Description
Blast System Settings: *These Settings apply to the entire Blast system.*	
IP	Displays the default IP Address of the server on which the Blast System is installed. If this server has multiple IP addresses and if you want to use a different one, enter the IP address manually.
Port	Enter the port number as desired. The default port is 8008. Because IP Phone callbacks are directed to this port, the certificate chain must be uploaded to CUCM. For detailed information about uploading the certificates to CUCM, see Upload certificates to CUCM.
License File	Click **Browse**, and then navigate to the AtHoc SA-Announce Revolution license located in the working folder. The Blast Setup utility copies the file to `<DRIVE>:\Program Files (x86)\AtHoc\SAAnnouncesRevolution`. **Note:** To update the license file in the future, copy it over the existing file.
SSL Settings: *Security– related settings.*	
SSL Enabled	Select the **SSL Enabled** check box to secure all communication. SSL certificates are automatically created. If the Port specified in settings is already bound to an interface then configuration will fail. For more information about validating the SSL Key, see SSL private key validation.

Field	Description
Private Key	Enter a password that will be used with the private key of the SSL certificate chain. This field is displayed only when SSL Enabled is checked. **User Supplied Certificates:** Enter the private key that was used when generating the certificates. **System Generated Certificates**: Enter a password to use with the private key of the SSL certificates. **Note:** If you are configuring SSL for the first time, you will need the private key or password (whichever you enter here) later when prompted to validate the certificates. If you are reconfiguring Blast, the SSL Key field must be filled with any value to continue with the configuration.
Trust Phones	Select the **Trust Phones** check box. Trust Phones employs a trust all certificates method when checked. This trust only applies to the initial POST leg from the Blast Notifier to the phones in the notification. Select the check box if phone certificates are not installed on the Blast application server.
CA Certificate	If you are using self-signed certificates generated by the Blast System, leave this field blank. If you are using certificates from an authorized certificate of authority, browse and select the certificate.
App Certificate	If you are using self-signed certificates generated by the Blast System, leave this field blank. If you are using certificates from an authorized certificate of authority, browse and select the certificate.
CUCM Settings: *Settings that apply to the notifier for CUCM access.*	
CUCM IP Address	Enter the **CUCM IP Address**. IP Address of the CUCM server that the notifier must connect to, to discover the devices and other CUCM objects it needs to be aware of.
CUCM User	Enter the username you created in the Create a UCM User and UCM Roles section of this guide. The user can be a CUCM user or a CUCM application user with AXL access permissions, used to gather CUCM data for the IP phone devices. User account needs proper roles for this access. **Note:** This setting is encrypted in the registry and cannot be changed manually. Run the Blast System Configuration program to change it.

Field	Description
CUCM Password	Enter the password you created for the new user. **Note:** This setting is encrypted in the registry and cannot be changed manually. Run the Blast System Configuration program to change it.
CUCM Version	Change the version if required. Only the first two version identifiers are used. For example, 10.5, though others can be entered.

3. When you finish entering the values in each of the fields, click **Configuration** in the top right corner of the screen.

   A pop-up notification screen with instructions to complete additional configuration steps is displayed.

   The first part of the notification refers to the CUCM authentication process, which will take place after testing of the authentication service. Complete the CUCM Authentication configuration regardless of whether SSL is enabled.

   The second part of the notification refers to the certificates that you will upload later after they are generated. At the end the installation process, you will delete the certificates from the installation folder. For more information about the deletion process, see NDS configuration for Cisco IP phones.

   Cisco IP phones cannot receive Blast commands until the CUCM enterprise parameters for the authentication URL (secure and non-secure) have been changed to the authentication URL provided by the notice. Restart the phones to acquire the new setting.

   Cisco IP phones cannot receive Blast commands until the CUCM enterprise parameters for the authentication URL (secure and non-secure) have been changed to the authentication URL provided by the notice. Restart the Phones to acquire the new setting.
4. In the **Notice** window, click **OK**. The system configuration begins. The individual module installers run one by one and the configuration settings are applied across the module settings files to create a contiguous integration.

   CUCM settings are not validated at this stage. The Blast Notifier `log.txt` file must be checked to determine if there is any issue with the current settings.

   When the installation process reaches the SSL certificate creation stage, three pop-up screens will appear in succession.
5. On the **Create Private Key Password** screen, in the **Password** and **Confirm Password** fields, enter the password that you created for the private key.
6. Click **OK**.
7. On the **Enter Private Key Password** screen for the **Subject** key, enter the password that you created for the private key.
8. Click **OK**.
9. On the **Enter Private Key Password** screen for the **Issuer Signature** key, enter the password that you created for the private key.
10. Click **OK**.
11. On the **Configuration Completed Successfully**, click **OK**.

Install TTS on a new NDS server

1. Contact ReadSpeaker at support@readspeaker.com and request a TTS license. Approval is needed from the ReadSpeaker account manager.

2. If the TTS license provided by your account manager at ReadSpeaker did not include a verification.txt file, contact ReadSpeaker and request it.
3. Add the verification.txt file to your local system at: C:\VW\VTSvc\verify.
4. After your have finished completing the other configuration tasks described in this guide, send a test alert and verify that the text from the alert title and body is converted to an audio file and can play on a Cisco IP Phone device.

System generated certificates

The Blast System configuration attempts to perform the following actions:

- Automatically create the required certificates if user-generated certs have been selected.
- Copy the certificates to the appropriate certificate stores on the local host.
- Bind the certificate chain to the selected IP Address and Port.

The configuration process never unbinds an in-use port. The process notifies that the port is in use by something other than our certificate. Use the delete binding function to delete an existing binding and free the port for configuration or change the port. For more information, see Set up the Windows server.

The following certificates and private key are generated and stored in:

`c:\Program Files (x86)\Syn-Apps\SAAnnounceRevolution\Configuration\Certificates`

Note: `SynAppsAuth.cer` is the App certificate.

SSL private key validation

Note: This section only applies when **SSL Enabled** is selected.

You must validate the SSL Private Key if you are:

- Performing the SSL configuration for the first time.
- Reconfiguring SSL and the certificates, and the private key no longer exists in the certificate directory.

You are presented with three validation windows, enter the password as follows:

- If you have created a password for system-generated certificates and have left the CA and App Certificate fields blank, enter the password you entered on the Blast System Configuration screen. Enter the same password in all three validation windows.
- If you selected user-generated certificates for the CA and App certificates, enter the private key you used to generate the certifications in the Private Key field on the Blast System Configuration screen. Enter that same Private Key in all three validation windows.

Upload certificates to CUCM

This section describes how to upload the generated CA and App certificates from NDS to CUCM. After the Blast System configuration, you must upload the certificates to CUCM . The Blast Server must trust the CUCM certificates. If SSL is enabled and the CA and App Certificate fields are left blank to allow system-generated certificates, an additional notice is displayed with the location of the certificates you can upload them to CUCM.

Upload CA certificate

1. Open **CUCM**.
2. Select **Cisco Unified OS Administration** from the navigation drop-down list.
3. Click **Security > Certificate Management**.
4. Click **Upload Certificate/Certificate chain**.
5. From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
6. Optionally, enter a descriptive name. Do not use spaces in this field.
7. Click **Choose File** and navigate to **SynAppsAuthCA.cer**.
8. Click **Upload**.
9. To apply the certification changes to the phones, restart the Cisco Tomcat service from the CUCM host command line interface: `utils service restart Cisco Tomcat`.

   Note: You must have Cisco administrator permissions.

Upload App certificate

1. Open **CUCM**.
2. Select **Cisco Unified OS Administration** from the navigation drop-down menu.
3. Click **Security > Certificate Management**.
4. Click **Upload Certificate/Certificate chain**.
5. From the **Certificate Purpose** drop-down list, select **Phone-trust**.
6. Optionally, enter a descriptive name. Do not use spaces in this field
7. Click **Choose File** and navigate to **SynAppsAuthCA.cer**.
8. Click **Upload**.
9. Reboot the phones.

Important: Do not reboot the Cisco Tomcat service again.

Upload phone certificate

Do not perform these steps if you have selected **Trust Phones** in the Blast System Configuration screen. If you did not select **Trust Phones**, the CUCM Phone Certificate Authority must be downloaded from CUCM and imported to the Blast application server.

1. Open **CUCM**.
2. From the navigation drop-down list, select **Cisco Unified OS Administration**.
3. Click **Security > Certificate Management**.
4. Search for the CAPF certificate where **Certificate begins with CAPF**.
5. Click **Find**.

6. Click **CAPF Common Name**. The Certificate Details window should show the file name "CAPF.pem".
7. Click **Download.PEM**.
8. Import the CAPF.pem file to the application server's local computer- Trusted Root CA's certificate store.

Using fully qualified domain names

If your environment requires fully qualified domain names (FQDNs) in your Blast System environment, complete these additional tasks after you have completed the Blast System installation, configuration, and SSL setup.

FQDN between blast notifier and CUCM

1. Create a DNS entry for CUCM.
2. Edit the config properties in: `c:\Program Files (x86)\Syn-Apps\BlastNotifier\BlastNotifier.exe.config`:
   - Change `CUCMIP` to the FQDN of CUCM.
   - Set `UseSSL` to `True`.
3. Save the file and restart Blast Notifier.

FQDN between blast notifier and Cisco phones

1. Open the **Authenticator.exe.config** file.
2. Change **SecurePort** to an unused port of your choose.
3. Save the file.

   Note: The default port value is 8008. Standard practice is to use a 4-digit port number that ends in 443, for example 8443.
4. Open the **BlastNotifier.exe.config** file.
5. Change **AppServerURL** to use the server's FQDN.
6. Save the file.
7. Request a CA-signed certificate for the new port. Use a Certificate Authority of your choice and install the certificate.
8. Open the CA-signed certificate. Click the **Details** tab. Scroll down to the bottom of the **Details** window and click **Thumbprint**.

   You can use this value to bind the certificate to the new port.
9. Bind the CA-signed certificate to the new port (for the URLs) using the `netsh` command.

   ```
   netsh http add sslcert ipport=0.0.0.0:<Port> certhash=<Thumbprint>
    appid={00112233-4455-6677-8899-AABBCCDDEEFF}
   ```

   where `<Port>` is the `SecurePort` defined in the `Authenticator.exe.config` file.

   Note: This must be a free port as you are binding to all available interfaces in this case.

   where `<Thumbprint>` is the Thumbprint from the Details tab of the CA-signed cert. Remove all spaces.

   Important: If a binding already exists for this port it must first be removed using the following command: `netsh http delete sslcert ipport=0.0.0.0:<Port>`

   Warning: Do not bind this certificate to that port using the IIS control panel. This will cause the other bindings of NDS with port 443 to fail. You must use `netsh` instead of IIS. Leave the existing binding to the system-generated certificate in place.
10. To upload the CA certificate, click **CUCM OS Administration** > **Certificate Management** > **Upload Certificate/ Certificate chain** and from the **certificate purpose** drop-down list, select **Phone-trust**.

Possible conflicts

- Certificate already in use: This error occurs when binding already exists for this port. Remove the certificate using the following command: `netsh http delete sslcert ipport=0.0.0.0:<Port>`
- Failed to bind certificate chain to port: If this error occurs, you need to run the set up as an administrator.

Copy Tomcat certificate to NDS

To copy the Tomcat certificate from CUCM to NDS, complete the following tasks:

1. Download a Tomcat certificate from CUCM.
2. Import the Tomcat certificate to the Windows Certificate store.

Download a Tomcat certificate from CUCM

1. Open **CUCM**.
2. Select **Cisco Unified OS Administration** from the navigation drop-down menu.
3. Click **Security** > **Certificate Management**.
4. Search for the tomcat certificate where **Certificate begins with tomcat**.
5. Click **Find**.
6. Click the Tomcat **Common Name** link. The **Certificate Details** window should show tomcat.pem in the **File Name** field.
7. Click **Download.PEM** file.

Import the Tomcat certificate to the Windows Certificate store

1. Open Windows search and type **mmc**.
2. Click **Yes** to allow changes.
3. Click **File** > **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** window, select **Certificates** from the available snap-ins.
5. Click **Add**.
6. In the **Certificates snap-ins** window:
   - Select **Computer account**.
   - Click **Next**.
   - Click **Finish**.
7. In the **Add or Remove Snap-ins** window, click **OK**.
8. Expand the **Trusted Root Certification Authorities** folder.
9. Right-click the **Certificates** folder and select **All Tasks** > **Import**.
10. Go through the **Certificate Import Wizard** screens to import the tomcat.pem certificate you downloaded from CUCM.

Update CUCM authentication URLs

1. Open **CUCM Administration**.
2. Click **System** > **Enterprise Parameters**.
3. For **Phone URL Parameters**, set:
   - **URL Authentication** to *http://<IP>:<Port>/<UrlPath>/Authenticate*

     Note: This URL must be a Fully Qualified Domain Name(FQDN).
   - **Secured Authentication URL** to *http(s)://<IP>:<Port>/<UrlPath>/Authenticate*
4. Click **Save**.
5. Click **Apply Config** to update the authentication URL on all phones.

When using a non-secure mode, the **Secured Authentication URL** must be set to **HTTP** and not **HTTPS**. For the basic testing purpose, the authentication URLs can also be overridden on a phone using the device settings for each phone in question.

Configure NDS for Cisco IP phones

Complete the following tasks to configure NDS for Cisco IP phones:

- Obtain the Blast plug-in.
- Add the ucmIpPhone key to the NDS server.
- Configure the database server.

Obtain the Blast plug-in

After you install the Synaps software, the BlastPlugin folder is created in: `C:\Program Files (x86)\AtHocENS\DeliveryServer\Plugins\BlastPlugin`.

Note: If the AtHocENS folder is present in a different location, navigate to the **BlastPlugin** folder in the **Plugins** directory and copy the entire folder to: `<Drive>:\AtHocENS\DeliveryServer\Plugins`.

Add the ucmIpPhone key to the NDS server

1. Open the NDS console.
2. Go to the **Management** tab.
3. Select **Configuration**.
4. Click **New Configuration**.
5. In the **New Key** field, add the **nds.plugin.ucmIpPhone** key.
6. Add the following configuration in the **Value** field:

```
<nds.plugin.ucmIpPhone>
    <supportedDevices>
        <device type="ucmIpPhone"
        enabled="true" secondsTimeout="0"
        requiredInilizations="None"
        maxTasksPerInit="10000"
        maxTasksPerExecution="10000"
        maxTasksCanProcess="10000" />
    </supportedDevices>
</nds.plugin.ucmIpPhone>
```

7. Click **Save**.
8. Close the NDSconsole.
9. Open the NDS console. The ucmIpPhone device is displayed in the supported devices list.
10. Go to the **Testing** tab to verify that the ucmIpPhone device is displayed in the **Supported Devices** section.

Configure the database server

Before you begin:

- You will need the following information before you configure the database server:
  - The database server name.
  - The SA user password.
  - The name of the ngdelivery database.

- Place the BlastConfiguration folder that you obtained from AtHoc sales in a folder on your local computer. This folder contains the `BlastConfiguration.bat` and `BlastConfiguration.sql` files.

1. Open the **BlastConfiguration** folder on your local system.
2. Right-click the `BlastConfiguration.bat` file. Click **Edit** and open the file using Notepad.
3. Add the database server instance name, ngdelivery database server name, and the SA user password to the `BlastConfiguration.bat` file as shown in the following example:

```
@echo off
@echo Configuring the Blast Plugin
rem update the database information in the below statement. Remove the <> from
 <value> and add the respective values.
for %%G in (*.sql) dosqlcmd -S <DatabaseServerInstanceName> -d
 <NGDeliveryDBName> -U sa -P "<SAUserPassword>" -i "&&G"
PAUSED
```

4. Save and close the `BlastConfiguration.bat` file.
5. Open the `BlastConfiguration.sql` file.
6. Verify that the @deviceType value is '**ucmIpPhone**'.

```
DECLARE @deviceType NVARCHAR(50)
SELECT @deviceType='ucmIpPhone'
IF NOT EXISTS (SELECT * FROM NGDeliveryAccount.dbo.DatacenterSiteDetail
.
.
.
```

When you log in to the database server, there is a **ucmIpPhone** entry in the **deviceType** column in the **ngdeliveryaccount** > **DatacenterSiteDetail** table.

Set up the Windows server

This section is for reference only and is not a part of Blast System configuration. The Blast System configuration program automatically performs these steps on a machine where the selected port is free of bindings.

If you have to perform these steps manually, then run the Blast System configuration program from a command prompt, as an administrator. When applicable, use makecert / netsh to install the certificate chain on the server hosting the application.

Configuration	Command and description

Create Root Authority Cert	`makecert -n "CN=SynAppsAuthCA" -cy authority -a sha256 -sv "SynAppsAuthCA.pvk" -r "SynAppsAuthCA.cer"`
	
	Requires that the `makecert.exe` file is included with the Authenticator installation at:
	
	`C:\Program Files (x86)Syn-Apps\Authenticator\Certificates\makecert.exe.`
	
	Set a password and use the same password in both pop-ups.
	
	Results are in the same directory as makecert.

Store Root Cert	1. Execute **MMC** (**Start** > **Find: MMC**). 2. Add the **Certificates snap-in** (for Local Computer, not the default Current User.) 3. Navigate to **TrustedRoot Certification Authorities**, right–click, and select **All Tasks** > **Import**. 4. Browse to the previously created SynAppsAuthCA.cer and import it.
Create Application Cert	`makecert -n "CN=<IP>" -ic "SynAppsAuthCA.cer" -iv "SynAppsAuthCA.pvk" -a sha256 -sky exchange -pe -sr localmachine -ss my "SynAppsAuth.cer"` Replace the <IP> with the IP settings value used in the BlastNotifier configuration file. This is the IP address of the interface we are to bind to on the local machine. Enter the password from the first makecert step.

Configuration	Command and description
Store Application Cert	1. Execute **MMC** (**Start** >**Find: MMC**). 2. Add the **Certificates snap-in** (for Local Computer, not the default 'Current User'). 3. Navigate to **Personal**, right–click and select **All Tasks** > **Import**. 4. Browse to the previously created SynAppsAuth.cer and import it.

Bind Cert	`netsh http add sslcert ipport=0.0.0.0:<Port> certhash=<Thumbprint> appid={00112233-4455-6677-8899-AABBCCDDEEFF}`
	
	where `<Port>` is the Port as set in the BlastNotifier configuration file. This should be a free port as we are binding to all available interfaces in this case.
	
	where `<Thumbprint>` is the thumbprint from the details panel of the `SynAppsAuth.cer` (double-click it in the MMC view). Remove all spaces.
	
	If a binding already exists for this port it must first be removed using the following command:
	
	`netsh http delete sslcert ipport=0.0.0.0:<Port>`

Verify Proper Operation	1. Open the URL in a browser on the application server. This is the only place the certificate authority is trusted. `http(s) //<IP>:<Port>/<UrlPath>/Authenticate?UserId=<userName>&Password=<password>` Example: `https://10.0.0.100:6443/Authenticator/Authenticate?UserId=SynApps&Password=SynApps` 2. Verify that there are no security warnings when in secure mode. 3. Verify that the browser body shows 'AUTHORIZED'. **Note:** This test generally applies to the Authenticator module only. For other modules, test the functionality as normal.

Windows Roles and Features Error

Some Microsoft Windows 2016 users may encounter a Windows pop-up error while installing the Cisco Blast Configuration Utility.

```
Warning – Dependencies failed to install:
Windows Roles and Features.
This is likely due to lack of internet access, please enable internet access and
 re-run installer or install the required components manually.
```

Note: This will not affect the functionality of the Cisco Blast system or NDS.

Click **OK**.

Verify the NDS installation

1. Check the `SAAnnounceLog.txt` file in the **SAAnnounceRevolution** folder to see that Revolution is receiving heartbeats from both the Activator plug-in and the Notifier. This ensures that there is a connection between all Blast components. Each module heartbeats every 30 seconds as displayed in the following example:

```
12 Apr 2017 23:40:14  DEBUG  [4]  SAAnnounceRevolution.NotifierRegistrar.AddNotifier  [(null)]
: Received HeartBeat from Notifier: BlastNotifier at 192.168.1.50:8006
12 Apr 2017 23:40:23  DEBUG  [4]  SAAnnounceRevolution.ActivatorRegistrar.AddActivator
[(null)] : Received HeartBeat from Activator: AtHoc.NDS.Plugin.Blast at 192.168.1.50:8006
12 Apr 2017 23:40:44  DEBUG  [4]  SAAnnounceRevolution.NotifierRegistrar.AddNotifier  [(null)]
: Received HeartBeat from Notifier: BlastNotifier at 192.168.1.50:8006
12 Apr 2017 23:40:53  DEBUG  [4]  SAAnnounceRevolution.ActivatorRegistrar.AddActivator
[(null)] : Received HeartBeat from Activator: AtHoc.NDS.Plugin.Blast at 192.168.1.50:8006
12 Apr 2017 23:41:14  DEBUG  [4]  SAAnnounceRevolution.NotifierRegistrar.AddNotifier  [(null)]
: Received HeartBeat from Notifier: BlastNotifier at 192.168.1.50:8006
12 Apr 2017 23:41:23  DEBUG  [4]  SAAnnounceRevolution.ActivatorRegistrar.AddActivator
[(null)] : Received HeartBeat from Activator: AtHoc.NDS.Plugin.Blast at 192.168.1.50:8006
```

2. Verify the connection between the Notifier and Call Manager by checking the `PhoneCacheLog.txt` file in the **Blast Notifier** folder.
3. Verify the Call Manager by checking the `PhoneCacheLog.txt` file in the **Blast Notifier** folder.
4. The Blast Notifier queries the connected Call Manager for all phones that are registered with it. A successful connection between Notifier and Call Manager results in a list of all the devices that are registered in the Call Manager, as displayed in the following log entries:

```
************************************  4/13/2017 4:54:19 PM
****************************************
13 Apr 2017 16:54:19  INFO   [5]  RIS.RISAdapter.GetDevices  : Sending RIS Request for 14 /
200max devices:
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP2C3F38C81EA9
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP0013C4285C91
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEPB000B4BA32E2
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP44D3CA71894E
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP00146A743DCD
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP001E7AC46E9B
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEPB000B4BA32EE
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP001121FFECD4
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP001469A9557E
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP2C3ECF87EF5C
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP649EF3B17420
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP001EF7C26202
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEPA40CC3959B95
13 Apr 2017 16:54:19  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Name: SEP7081050C384A
13 Apr 2017 16:54:20  INFO   [5]  RIS.RISAdapter.GetDevices  : Received RIS Response for 1
devices.
13 Apr 2017 16:54:20  DEBUG  [5]  RIS.RISAdapter.GetDevices  : RIS Response for CUCM node:
192.168.20.254, num devices: 1.
13 Apr 2017 16:54:20  DEBUG  [5]  RIS.RISAdapter.GetDevices  : Device Name: SEP7081050C384A,
Status: UnRegistered, IP: 192.168.20.50, DN: 1543-UnRegistered
13 Apr 2017 16:54:20  DEBUG  [5]  AXL_new.PhoneCache.Update  : PhoneCache UPDATE Finished...
13 Apr 2017 16:54:20  INFO   [5]  AXL_new.PhoneCache.Update  : 1 phones in the cache
13 Apr 2017 16:54:20  INFO   [5]  BlastNotifier.DataAccess.<.ctor>b__9_0  : cache update
complete... converting phones
13 Apr 2017 16:54:20  DEBUG  [5]  BlastNotifier.DataAccess.<.ctor>b__9_0  : 1 phones converted
```

Errors

Errors displayed in the log file should provide some indication of what the problem is and where to start looking to fix the errors. The following are example errors and troubleshooting steps:

1. In the following error, the endpoint failed to receive the notification because “there was no endpoint listening” at the address specified. To troubleshoot this error, start by ensuring that the Notifier is communicating with Revolution and Call Manager. Then verify that the endpoint is listed as Registered and was pulled in by the Notifier. From there troubleshooting might get more specific based on the answers to those questions.

```
23 Mar 2017 17:57:10 ERROR [17]
 SAAnnounceRevolution.NotificationHandlerBlast.CheckFor75PercentResponse
```

```
 [(null)] : Failed to obtain ActivationResult from BlastNotifier Notifier
 System.ServiceModel.EndpointNotFoundException: There was no endpoint listening
 at http://192.168.10.101:8008/SAAnnounceSDK/BlastNotifier/SAAnnounceSDK
 that could accept the message. This is often caused by an incorrect address
 or SOAP action. See InnerException, if present, for more details. ---
> System.Net.WebException: Unable to connect to the remote server --->
 System.Net.Sockets.SocketException: A connection attempt failed because
 the connected party did not properly respond after a period of time, or
 established connection failed because connected host has failed to respond
 192.168.10.101:8008.
```

2. The Notifier is currently inactive. If you check the SAAnnounceLog.txt file in this scenario, you cannot see a heartbeat from BlastNotifier to Revolution, meaning they are not communicating. To troubleshoot this error, start by getting the Notifier to communicate with Revolution.

```
23 Mar 2017 18:19:05 WARN [8]
 SAAnnounceRevolution.NotificationHandler.SendCommandToken [(null)] : Could
 not send notification to notifier: BlastNotifier because the Notifier is NOT
 active.
```

Supported Cisco IP phones

The following tables list supported Cisco IP phones.

Cisco DX phone models	XML	IMG
Cisco DX 650	✓	✓
Cisco DX 70	✓	✓
Cisco DX 80	✓	✓

Cisco IP phone models	XML	IMG
Cisco IP Communicator	✓	✓
Cisco 6921	✓	
Cisco 6941	✓	
Cisco 6945	✓	
Cisco 9691	✓	
Cisco 7821	✓	
Cisco 7841	✓	
Cisco 7861	✓	
Cisco 7911	✓	
Cisco 7912	✓	
Cisco 7920	✓	✓
Cisco 7921G	✓	✓
Cisco 7925	✓	✓
Cisco 7926	✓	✓
Cisco 7931	✓	
Cisco 7937 Conference Station	✓	
Cisco 7940	✓	

Cisco IP phone models	XML	IMG
Cisco 7941	✓	✓
Cisco 7941G-GE	✓	✓
Cisco 7942	✓	✓
Cisco 7945	✓	✓
Cisco 7960	✓	
Cisco 7961	✓	✓
Cisco 7961G-GE	✓	✓
Cisco 7962	✓	✓
Cisco 7965	✓	✓
Cisco 7970	✓	✓
Cisco 7971	✓	✓
Cisco 7975	✓	✓
Cisco 8811	✓	✓
Cisco 8831	✓	✓
Cisco 8841	✓	
Cisco 8845	✓	✓
Cisco 8865	✓	✓
Cisco 8851	✓	
Cisco 8861	✓	
Cisco 8941	✓	✓
Cisco 8945	✓	✓
Cisco 8961	✓	✓
Cisco 9951	✓	✓

Cisco IP phone models	XML	IMG
Cisco 9971	✔	✔

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

The BlackBerry AtHoc Customer Support Portal also provides support via computer-based training, operator checklists, best practice resources, reference manuals, and user 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
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada