How to Install and Configure Access Control for Local E-mail

Afaria 7 SP2+
## Contents

**Introduction** .................................................................................................................. 1
   - Access Control Overview ................................................................................. 1
   - Prerequisites ............................................................................................... 1
   - Devices Supported ..................................................................................... 1

**Installing Access Control for Local E-mail** ................................................................. 3
   - Access Control Components ...................................................................... 3
   - ISAPI Filter Components ......................................................................... 4
   - Installing Access Control Components on a Single Machine ............................. 5
   - Installing Access Control Components on Multiple Machines ......................... 8
     - Installing the Filter and the Data Handler Proxy Service .............................. 9
     - Installing the Data Handler Only .......................................................... 12
   - Afaria Filter Files ..................................................................................... 15

**Configuring Afaria for Access Control** ..................................................................... 19
   - Configuring the Afaria Filter Listener .................................................... 19
   - Configuring Relay Server for Access Control ....................................... 20
   - Configuring Exchange ActiveSync for iOS Devices ............................... 21
   - Editing the Registry to Create Extra Logs .............................................. 22
   - Required Variables While Creating/Editing an iOS or Android Enrollment Policy .................................................. 22
   - Examples for Using Substitution Variables When Creating/Editing an Android or iOS Configuration Policy .................................................................................. 23
   - Required E-Mail Formats for Android Devices .................................... 25
   - Client Configuration Examples .................................................................. 26
     - Configuring Android Native Email Client for Exchange ActiveSync (Microsoft Active Directory Authentication) .................................................. 26
Introduction

This document describes how to install and configure the Access Control for E-mail component, including managing access control in a local e-mail environment and configuring access control policies.

Access Control Overview

The Access Control for E-mail component adds a layer of protection to your enterprise e-mail platforms by filtering mobile device synchronization requests according to your access control policies.

Access control discards any synchronization requests that do not meet the policies you defined on the Afaria server and saved to the Afaria database. Access control policies include the list of known devices, their associated policies, and any defined policies for unknown devices.

There are two implementations for Access Control for E-mail:

- Hosted e-mail – e-mail services are hosted by a third-party and are available to users from the Internet without any e-mail servers or related Afaria components inside the enterprise network or DMZ. The Afaria server communicates with Exchange 365 to update device status.
- Local e-mail – e-mail server and related Afaria components are installed within the enterprise network and/or the DMZ.

Prerequisites

Install Afaria 7 SP2 including the Access Control for E-mail component. Install Afaria 7 SP2 Hotfix 26 on top of Afaria 7 SP2 Hotfix 14.

Devices Supported

Access Control for E-mail is supported only for Android, iOS, Windows Mobile Professional, and Windows Mobile Standard devices; it is not supported for BlackBerry and Windows Phone 8 devices.

Introduction
Installing Access Control for Local E-mail

The local e-mail implementation of access control means that the e-mail server and related Afaria components are installed within the enterprise network and the DMZ. Set up Access Control by installing and configuring the Afaria components.

Access Control Components

Access control uses a filter, Data Handler services, and the Afaria filter listener. You can install access control components on a single machine behind the corporate firewall. You can also install some components in the DMZ and some components behind the firewall.

- **Afaria access control filter** – includes the Internet Server Application Programming Interface (ISAPI) filter and Data Handler services
  - **Filter** – accepts inbound synchronization requests from mobile clients and passes details from incoming requests to the Data Handler which determines whether to allow or block the incoming request
    
    The filter must reside on the server that accepts inbound client requests on the Certificate Authority Server (CAS). For greater security, install the filter on a proxy server located in your DMZ.
  
  - **Data Handler services** – includes:
    - **HttpsClient** – a PowerShell component that queries the Afaria server at defined intervals to obtain updated details about the device
    - **Pipeserver** – a C# multithreaded component that decides whether to allow or block the incoming request by parsing data from the device list

    Data Handler services must reside on a server that can initiate a connection to either the Afaria server or its optional relay server proxy and the filter host. For greater security, install it on a separate server within your enterprise firewall, as it requests user and device data from the Afaria environment.

- **Afaria filter listener** – resides on the Afaria server. When requested by the PowerShell service (HttpsClient), the listener queries the Afaria database to obtain an updated access control policy list and forwards it to the PowerShell service.

  **Note:** The Afaria server service starts the Afaria filter listener.
ISAPI Filter Components

ISAPI filter components include:

- **Filter (XSISAPI.dll)** – XSISAPI.dll is either on the IIS or ISA box and watches the ActiveSync traffic as it comes through on the way to the Exchange CAS.

- **Data Handler Proxy (XSISAPIReversePipe.exe)** – XSISAPIReversePipe connects to PipeServer and sends incoming request details to get the device state. Based on data available in Device.xml, PipeServer returns the “Allowed” or “Not Allowed” flag to XSISAPIReversePipe.

- **Data Handler** – includes:
  
  - **Httpsclient.ps1** – This script contains two areas of functionality. First, the script contacts the Afaria server and requests, based on the e-mail domain, the lists of devices, and their respective Allow/Block status, for that domain. Second, the script specifies how to handle an "unknown" device attempting to conduct an ActiveSync session.
  
  - **PipeServer.exe** – The XSISAPI.dll talks to the PipeServer using a named pipe. XSISAPI.dll sends to the PipeServer the following information, which is collected from the connection headers sent by a device contacting the Exchange CAS:
    
    - Device ActiveSync ID (ASID)
    - Users email account, USER
    - Device Type, TYPE

    The label at the end of each item matches how it is logged in the XSISAPIPipe_Log. The PipeServer attempts to match these three items to a record in the Devices.xml file. PipeServer looks for the ASID and tries to match the GUID value from Devices.xml. The e-mail account is matched against the ExchangeID data in Devices.xml.

    Finally, the device type is also considered. Device type is determined by the device manufacturer and can actually be anything.

    When the PipeServer sends a response code, it uses the following response values to tell XSISAPI.dll how to handle the pending connection:

    - 0 - Device is known but is not permitted to get email
    - 1 - Device is known and is permitted to get email
    - 2 - Device is not known and is not permitted to get email
    - 3 - Device is not known, add to the new device list and allow to get email
    - 4 - Device is not known, add to the new device list but do not permit to get email
• **Afaria Filter Listener** (*XSISAPIServer.exe*) – resides on the Afaria server. *XSISAPIServer.exe* extracts the list of devices that the ISAPI filter should, or should not, allow to sync with the Exchange server.

### Installing Access Control Components on a Single Machine

You can install access control components on one server behind the corporate firewall.

If all the components are installed on a single machine behind the corporate firewall, you can select the **Filter and data handler** option while running the Access Control for Email installation program on the IIS/ISA machine behind the firewall.

**Figure 1: Components on a single IIS/ISA machine behind the corporate firewall**

If all the components are installed on multiple IIS machines behind the corporate firewall and load balancer, you can select the **Filter and data handler** option while running the Access Control for Email installation program on each IIS/ISA machine.
1. To install the Access Control filter, run the setup program (`setup.exe`) as administrator to launch the Afaria 7 Setup wizard.
2. From the first screen of the wizard, click **Install**.
3. From the second screen, click **Additional Installations and Resources**.
4. From the third screen, click **Install Access Control for Email**.

   The wizard prompts you to choose the appropriate version of the filter for your operating system. Click **32-bit (x86)** or **64-bit (x64)** as required.

   The setup wizard launches the Afaria 7 ISAPI Filter Setup wizard.

5. Click **Next**.
6. Select **Filter and data handler** and click **Next**.
7. From the Blocking Option screen, do the following and then click Next:
   a) Select **Allow all traffic but Microsoft-Active-Sync** to allow all traffic to the email server except from handheld devices.
   b) Select an ISAPI installation method - **Install ISAPI filter for IIS Server** or **Install ISAPI for ISA Server**.

   **Note:** The ISAPI filter does not affect Outlook Web Access (OWA).

8. From the Server Settings screen, enter the following and click Next:
   • URL of the Afaria server
   • Relay Server (RS) Prefix
   • Relay Server (RS) Farm ID

9. From the Ready to Start Installation screen, click Install.
   The filter (XSISAPI.dll) and data handler (httpsclient.ps1 and PipeServer.exe) components are installed on one server behind the firewall.

---

**Installing Access Control Components on Multiple Machines**

When installing access control components on multiple machines, you can install the Filter and Data Handler Proxy service (Query Forwarder) on an IIS or ISA box in the DMZ. You can
then install the data handler (Query Processor) on one or more CAS boxes behind an enterprise firewall.

Installing the Filter and the Data Handler Proxy Service

If an IIS or ISA machine is located in the DMZ and rest of the servers are hidden behind the inner firewall, you can select the Filter and Data Handler Proxy Service option while running the Access Control for Email installation program. It installs XSISAPI.dll and XSISAPIReversePipe.exe on an IIS/ISA server.

The Access Control List process flow is described below:

1. A mobile device submits an ActiveSync request.
2. The filter (XSISAPI.dll) intercepts the request and forwards it to the data handler proxy (XSISAPIReversePipe.exe).
3. The data handler proxy connects to the PipeServer and sends incoming request details to get back the device state. Based on data available in Device.xml, the PipeServer returns either the “Allowed” or "Not Allowed” flag to the data handler proxy.
4. The Data handler (HTTPSClient) requests Device.xml from the Afaria filter listener. It also uploads the newDevices.xml file to the Afaria filter listener in case ActiveSync ID is not available for the device.

Figure 3: Components on the ISA Server in the DMZ and on multiple CAS behind the corporate firewall

Perform the following steps to install the filter and data handler proxy service on an IIS/ISA box in the DMZ:

Note: Run the procedure on each IIS/ISA box.

1. To install the Access Control filter, run the setup program (setup.exe) as administrator to launch the Afaria 7 Setup wizard.
2. From the first screen of the wizard, click **Install**.

3. From the second screen, click **Additional Installations and Resources**.

4. From the third screen, click **Install Access Control for Email**.

   The wizard prompts you to choose the appropriate version of the filter for your operating system. Select **32-bit (x86)** or **64-bit (x64)** as required.

   The setup wizard launches the Afaria ISAPI Filter Setup wizard.
5. Click Next.

6. Select Filter and data handler proxy service and click Next.
7. From the Proxy Settings screen, type the Hostname and Port for the Powershell proxy server and click Next.

8. From the Blocking Option screen, Do the following and then click Next:
   a) Select Allow all traffic but Microsoft-Active-Sync to allow all traffic to the email server except from handheld devices.
   b) Select an ISAPI installation method - Install ISAPI filter for IIS Server or Install ISAPI for ISA Server.

9. From the Ready to Start Installation screen, click Install.
   The filter and data handler proxy (XSISAPI.dll and XSISAPIReversePipe.exe) components are installed on an IIS or ISA box in the DMZ.

### Installing the Data Handler Only

After installing the filter and data handler proxy service on an IIS or IAS box in the DMZ, you can install the data handler on a CAS behind the firewall.

**Note:** If there are multiple CAS servers, run the procedure below on each CAS.

1. To install the Access Control filter, run the setup program (setup.exe) as administrator to launch the Afaria 7 Setup wizard.
2. From the first screen of the wizard, click **Install**.

3. From the second screen, click **Additional Installations and Resources**.

4. From the third screen, click **Install Access Control for Email**.

   The wizard prompts you to choose the appropriate version of the filter for your operating system. Select **32-bit (x86)** or **64-bit (x64)** as required.

   The setup wizard launches the Afaria ISAPI Filter Setup wizard.
5. Click Next.

6. Select Data handler only and click Next.
7. From the Proxy Settings screen, type the Hostname and Port for the Powershell proxy server and click Next.

8. From the Server Settings screen, enter the following and click Next:
   - URL of the Afaria server
   - Relay Server (RS) Prefix
   - Relay Server (RS) Farm ID

9. From the Ready to Start Installation screen, click Install.
   The data handler (httpsclient.ps1 and PipeServer.exe) files are installed on the CAS box behind the enterprise firewall.

Afaria Filter Files

This section lists the files installed with the Afaria filter or generated during access control operations.

Files Installed with the PowerShell Service Component
If you are using the 32-bit version of the PowerShell component, the files are installed in C:\WINDOWS\system32\inetsrv.

If you are using the 64-bit version of the PowerShell component, the files are installed in C:\Windows\SysWOW64\inetsrv.

Installing the PowerShell service component of the Afaria filter adds these files:
Installing Access Control for Local E-mail

- AfariaISAPIFilterUninstall.ini
- AfariaIsapiSetup.exe
- XSISAPIReversePipe.exe
- XSSrvAny.exe
- PipeServer.ps1
- HTTPSClient.ps1

Files Installed with the ISAPI Filter Component
Installing the ISAPI filter component of the Afaria filter adds these files in C:\WINDOWS\system32\inetsrv:

- AfariaISAPIFilterUninstall.ini
- AfariaISAPIFilter.exe
- XSISAPI.dll
- XSISAPIReversePipe.exe
- XSSrvAny.exe

If you installed both components of the Afaria filter on the Exchange Server's IIS Server, the files are added to IIS_InstallDir and IIS_InstallDir\bin.

Files Generated During Access Control operations
Executable XSSrvAny.exe launches PipeServer.ps1 and HTTPSClient.ps1. In turn, each of these create an event in the Windows Application Event log. The entries indicate the start action and its log file location. Consider this example event log entry:

XSISAPI PowerShell HTTPS Client was successfully started. Logfile is C:\Documents and Settings\Default User\Application Data\XSISAPI\XSISAPIHTTPS_Log.txt.

Afaria filter operations use and generate the following files on your IIS Server. The path for the files is described in the PiPServer.ps1 and HTTPSClient.ps1 start-up Windows Application Event log entries.

- `<ApplicationDataPath>\XSISAPI\ Devices.xml` - the list of Afaria Exchange access control clients known and managed by Afaria synchronization policies. This file is created by the Afaria server at the request of the PipeServer and is transferred to the PipeServer via HTTP/HTTPS. This file includes a series of XML records: one for each device the ISAPI filter is likely to see trying to access the Exchange CAS.

Data you see in the Devices.xml file tells you what Afaria has stored in the database.

```
<client GUID="SAMSUNG1351822059308603" User="user" SP="1" ExID="sy-alphaqa.com\xoom" Type="-10" status="0" />
<client GUID="APPLDLXH20UKDKNW" User="sy-alphaqa.com\mangesh01" SP="66" ExID="SY-ALPHAQA.COM\USR0000" Type="-8" status="1" />
<client GUID="APPLDN50001EDEKPJ" User="USR0001" SP="66" ExID="SY-ALPHAQA.COM\USR0001" Type="-8" status="0" />
<client GUID="APPLDN50002EDEKPJ" User="USR0002" SP="66" ExID="SY-ALPHAQA.COM\USR0002" Type="-8" status="0" />
```
The GUID is what Afaria considers as the ActiveSyncID, ASID. The ExID is the Exchange Identity for the user account on the device. Status indicates whether a device should (1) or should not (0) be allowed to receive e-mail.

- `<ApplicationDataPath>\XSISAPI\XSISAPIPipe_Log.txt` - a trace file that is generated by the PipeServer. You should see a series of text lines that look similar to:

  13-05-14 06:41 Responding '0' to request: ID='SAMSUNG1351822059308603', USER='sy-alphaq.com\xoom', TYPE='SAMSUNGGTI9100'
  13-05-14 06:41 Responding '1' to request: ID='APPLDLXH20UKDKNW', USER='sy-alphaq.com\mangesh01', TYPE='iPad'
  13-05-14 06:41 Responding '2' to request: ID='APPLC38GPGXGVDT9V', USER='sy-alphaq.com\deepa1', TYPE='iPhone'

Problems are indicated by messages such as “PipeServer timed out” or “Can’t open named pipe”. The example above shows the information that is being sent by the XSISAPI.dll and how the PipeServer is responding to that data.

- (Temporary file) NewDevices.xml – iOS or Android devices that are connected to the Exchange Server for synchronization must send a unique Exchange identifying value to the Afaria server. If the ISAPI filter sees a device attempting to connect that it cannot identify, it reports that it may have already identified the device, and the account information it sees for the device, and adds the device to the NewDevices.xml file. This allows the filter to tell the Afaria server everything it knows about the device. Afaria may then be able to update the database with the complete and correct ASID to allow for successful identification on a future connection.

- HTTPS.txt – log file for HTTPSClient.ps1 operations. List of connections from the IIS Server by the Afaria polling agent, back to the Afaria server to refresh the Devices.xml list.

- Pipe.txt – log file for PipeServer.ps1 operations. List of client synchronization requests indicating synchronization status 1 for allowed or 0 for denied.
Installing Access Control for Local E-mail
Configuring Afaria for Access Control

This section describes how to configure Afaria to use Access Control. It includes topics on configuring the Afaria Filter Listener, the Relay Server, and Exchange ActiveSync. It also provides examples of using substitution variables and configuring e-mail on the Afaria client.

Configuring the Afaria Filter Listener

This section describes how to set parameters for the Afaria filter listener, including protocol type and port number used for connections.

The Afaria filter listener resides on the Afaria Server and, upon request, provides the PowerShell service component of the Afaria filter with a refreshed client and policy list.

1. From the Afaria Administrator Web console, select Configuration in the Server tile and navigate to the Server > Access Control Server page.

2. If using HTTP, select Use HTTP on port and enter the port number for listening to requests.

   Ensure that the port does not conflict with any other ports that the Afaria server uses.

3. If using HTTPS, select Use HTTPS on port and define the parameters of the HTTPS connection.
   a) Enter the port number for listening to requests.

   Ensure that the port does not conflict with any other ports that the Afaria server uses.
   b) Enter the HTTPS host name or the IP address that the PowerShell service component of the Afaria filter uses to reach the Afaria server.
   c) Click Browse to select the host's SSL certificate.

   The certificate must reside in the Afaria server's personal certificate store.

4. Click Save and restart the Afaria server service.
Configuring Relay Server for Access Control

To configure the Relay Server to support the Afaria filter used in Access Control for Email, define the relay server configuration file, configure settings on the Afaria Administrator, and reinstall the PowerShell component of the Afaria filter.

Prerequisites

- The Relay Server is configured for basic operations.

  Note: You must configure the Relay Server for your Afaria server, regardless of whether you plan to use it for device connections.

- The two components of the Afaria filter are installed and Access Control has been configured on the Afaria Administrator.

Task

The following steps describe how to add the relay server to your current configuration for Access Control for Email.

1. Configure the relay server configuration file rs.config to support the Afaria filter.

   In the [backend_farm] section, define the Afaria filter's farm ID by using
   `<AfariaServerFarmID>-IS`, where `<AfariaServerFarmID>` is the same farm ID you defined for the Afaria server.

   For example, if you define your Afaria server farm ID as Afariafarm, then define your Afaria filter's farm ID as Afariafarm-IS.

2. On the Server > Configuration > Access Control Server page of the Afaria Administrator, select Use Relay Server, then click Save.

3. Reinstall the PowerShell component of the Afaria filter. In the Server Settings page of the installation wizard, enter the relay server address and farm ID.

   The farm ID you enter must match the farm ID you defined for the Afaria server in the relay server configuration file. The installation wizard automatically appends -IS to match the farm ID defined for the Afaria filter.

4. Restart the machine on which you reinstalled the PowerShell component.

5. Restart the relay server host.

6. In the Afaria Administrator, restart the Afaria server service.
Configuring Exchange ActiveSync for iOS Devices

Configure an Exchange ActiveSync account with a Microsoft Exchange server. You can create a policy for users by specifying the user name, host name, and e-mail address, or only the host name.

**Note:** This task is applicable for hosted e-mail and local e-mail environments.

1. From the Afaria Administrator Web Console, click the **Policy** tab.
2. Do one of the following:
   - To create a new iOS Configuration policy, click **New > Configuration > iOS** and provide information on the Summary page.
   - To edit an existing iOS Configuration policy, select the policy from the list and click **Edit**.
3. Expand the **MDM Payload** menu and select **Exchange ActiveSync**.
4. Click **Add**.
5. Provide the following information:
Configuring Afaria for Access Control

- **Name**: Enter a unique name.
- **Host**: Enter the host. For example, m.outlook.com.
- **Domain Host**: Leave this field blank or add an administrative e-mail address.
- **User**: Enter an Exchange 365 e-mail address. For example, BlockMe@afaria13.onmicrosoft.com.
- **Password**: Enter your password.

If you want to use substitution variables, click the **Substitution** link next to the following boxes and select the variables indicated below:

- **Domain Host**: Use the variable `%S.ExchangeDomain%`.
- **User**: Use the variable `%S.ExchangeUser%`.
- **E-mail Address**: Use the variables `%S.ExchangeUser%` and `%S.ExchangeDomain%`.
  The format is `%S.ExchangeUser%@%S.ExchangeDomain%`.
- **Password**: Use the variable `%S.ExchangePassword%`.

---

**Editing the Registry to Create Extra Logs**

If Afaria 7 SP2 Hotfix 14 is installed, create a `loginfo` (DWord) registry key at `HKEY_LOCAL_MACHINE\SOFTWARE\AFARIA\AFARIA\ISAPI` and set it to 1.

If you need the `XSISAPI.DLL` log, create an `ISAPIDebug` (DWord) registry key at `HKEY_LOCAL_MACHINE\SOFTWARE\AFARIA\AFARIA\ISAPI`. Set it to > 1 and run `Debugview` as administrator.

---

**Required Variables While Creating/Editing an iOS or Android Enrollment Policy**

When you are creating and editing an iOS or Android enrollment policy, add the following variables:

- **ExchangeDomain** (for Exchange and Domino environments)
- **ExchangePassword** (for Exchange and Domino environments)
- **ExchangeUser** (for Exchange and Domino environments)
- **UserName**
Examples for Using Substitution Variables When Creating/Editing an Android or iOS Configuration Policy

This section provides examples of how to use substitution variables when creating or editing an Android or iOS configuration policy.

**Example 1**
When creating or editing a configuration policy for built-in email on a Samsung device from Policy > Edit > Android Configuration > Samsung > Exchange account policy page, you can use substitution variables for:

- Domain – %S.ExchangeDomain%
- Email Address – %S.ExchangeUser%@%S.ExchangeDomain%.

**Note:** In case of built-in email account, configuration policy fetches ASID for Android devices are supported to MDM 2.0 or 2.0 + devices.

![Configuration setting screen](image)

**Example 2**
While creating or editing a configuration policy for NitroDesk from Policy > Edit > Android Configuration > Account configuration page, you can use substitution variables for:

- User ID – %S.ExchangeUser%
- Password – %S.ExchangePassword%
- Email Address – %S.ExchangeUser%@%S.ExchangeDomain%
- Domain - %S.ExchangeDomain%
Example 3
While creating or editing a configuration policy for iOS from Policy > Edit > iOS Configuration > Exchange ActiveSync page, you can use substitution variables for:

- Host – subcas. %S.ExchangeDomain%, where subcas is a sample CAS server name.
- Domain Host – Do not include %S.ExchangeDomain% for Domain Host. However, if you choose to use the substitution variable %S.ExchangeDomain%, ensure that the domain is specified on enrollment policy General page or Exchange domain prompt is selected on Enrollment policy Variable page.
- User – %S.ExchangeUser%
- Email Address – %S.ExchangeUser%@%S.ExchangeDomain%
- Password – %S.ExchangePassword%. You can also choose to leave the Password field blank.
Required E-Mail Formats for Android Devices

For Android devices, the e-mail user name requirement for Afaria Access Control for Email varies according to your enterprise environment.

Ensure that users enter the information correctly. On the device's Afaria application configuration page (Afaria > Configuration), the e-mail user name must comply with your e-mail server's requirement for user name. The format, as observed in Afaria table A_ANDROID_DEVICES, is:

- (for Samsung devices) domain\user
- (for Motorola devices) user@domain
Client Configuration Examples

The three client configuration examples in this section are examples only. The screens and prompts you see may be different, depending on your environment and requirements.

Configuring Android Native Email Client for Exchange ActiveSync (Microsoft Active Directory Authentication)

Configure the Android native e-mail client for Exchange ActiveSync through Afaria with Microsoft (MS) Active Directory (AD) authentication and ISAPI filter on CAS server.

Prerequisites

- An Afaria 7.0 SP2 HotFix 14 server that has access to Microsoft AD
- An accessible MS domain
- An MS Exchange Server with a working user account and mailbox
- A Relay Server, which can be required for device access
- An Android device. This example uses a Samsung Galaxy Note with Android 4.1.2

Task

Afaria Server Preparations:

1. From the Server > Configuration > Security page, configure the Server configuration security settings.
These are the required security settings for MS active directory access, which is required to use AD variables.

The Afaria Server Configuration Access Control Options are not configured. Everything is default.

2. Create an enrollment policy for Android. In the left pane, select **Summary**, then create a URL Code for enrollment. For example, Tiny URL is configured.
3. In the left pane, select **General** and configure the required settings.

4. In the left pane, select **Group** to assign a group. The screen below shows that a static group is assigned.
5. Configure variables for the user prompts. The *ExchangeUser* variable is required for ISAPI validation.

**Note:** ExchangeUser must be configured with the FQDN Domain name using the syntax "%FQDN%\User Name". For example "sap.com\m muster". Ensure that there are no spaces. ExchangePassword is optional for ISAPI validation. The user is prompted for a password when connecting to Exchange the first time.

6. Create a configuration policy for Android.

Select **Require user authentication**. This example enables **Inventory**.
7. On the Samsung Exchange account policy, configure the required variables. To use MS AD variables, click the substitution variables icon next to the variable field and select the variable from the list.

In this example, the following variables are configured:
Configuring Afaria for Access Control

- Domain: %D.wWWHomePage%
- E-mail Address: %D.mail%
- User: %D.sAMAccountName%
- Password: %S.ExchangePassword%

“S” is a standard Afaria System variable. “D” is for Microsoft Active Directory (MS AD) usage. “U” is a self-created Afaria variable.

8. Link the policy to the static group.

Starting the Device Connection to the Afaria Server

This example uses a Samsung Galaxy Note with Android 4.1.2 installed. In some cases, you must manually start the device mail client to activate the EAS account. This example is also likely to be different on Android 2.3.x devices, where the EAS profile is just created without any user intervention.

Set the Exchange Domain with a fixed value on the EAS policy settings. You can also remove the Afaria variable “ExchangePassword” from the enrollment policy user prompts. Change the AD password periodically to comply with security policies. For this example, you can configure a dummy password on the EAS policy setting. The user is prompted for the right password during the first EAS client connection to Exchange.

1. Configure the device security settings to allow unknown sources. This is required for the MMEP client extension which allows you to configure specific Samsung configuration features. The MMEP extension APK is not currently available from the Google play store. Select the unknown sources option for all applications that are not directly installed from the play store.

2. On the Android device, open the market and search for “Afaria”. Select the Afaria Client for Android to install.
3. Tap Install.

4. Tap Open.

5. Tap Activate.
6. Enter the configured Tiny URL and tap **OK**.

7. Enter the Exchange user ID and password. Tap **Done**.
You are prompted again to authenticate against Microsoft Active Directory.

8. Re-enter the user account and password and tap **OK**.

The Afaria client connects to the Afaria Server, and receives the MMEP Client extension.

9. Tap **Install** to install the Afaria Samsung MMEP client.

10. Tap **Activate**.
11. Tap the New e-mail account message on the right side of the button line.

12. Tap OK for activation.
The device mail client upgrades the account for EAS. You'll be prompted to update security settings to use EAS.

13. Tap OK.

14. Tap Activate.
The mail client configuration for EAS is finished. The device now appears on the Afaria Admin UI device list.

Configuring NitroDesk Touchdown Email Client on Android (Microsoft Active Directory Authentication)

This topic describes how to configure the Nitrodesk Touchdown e-mail client on Android using Afaria with Microsoft Active Directory (MS AD) authentication, Afaria user group policy assignment and the ISAPI filter on CAS server.

Prerequisites

- An Afaria 7.0 SP2 HotFix 14 server that has access to Microsoft AD
- An accessible MS domain
- An MS Exchange Server with a working user account and mailbox
- A Relay Server, which can be required for device access
- An Android device. This example uses a Samsung Galaxy S3 with Android 4.1.2

Task

Afaria Server Preparations:

1. From the Server > Configuration > Security page, configure the Server configuration security settings.
These are the required security settings for MS active directory access, which is required to use AD variables.

The Afaria Server Configuration Access Control Options are not configured. Everything is default.

2. Create Afaria groups.

Two groups are created. One static group which is configured to use with the enrollment policy and one Afaria user group that is linked to the MS AD group “Android”.

3. Create Android enrollment, configuration, and application policies.

From the Policy > Edit > Android Enrollment > Summary page, create a URL code for enrollment. The example below uses TinyURL.
4. On the General screen, configure the required settings.

5. On the Group screen, link the static group.
6. Configure the variables for the user prompts. The *ExchangeUser* variable is required for ISAPI validation. The user is not asked for the Exchange user password, but must enter the password during the Nitrodesk configuration wizard. In this scenario, no password information is stored on the Afaria database.

7. From **Policy > Edit > Android Enterprise Application > Summary** page, create an Enterprise Application policy.
8. From the General page, select the **Required** option to allow that app to automatically install in the background.
9. From **Policy > Edit > Android Configuration > Summary** page, create an Android configuration policy.

Select **Require user authentication**. The screen below indicates that for this this example, Inventory is enabled. No other options are configured for this policy.
10. Create another Android configuration policy to be used for NitroDesk Touchdown configuration.

11. Configure the NitroDesk Account configuration.
In this example, the following variables are configured:

- E-mail address: \%D.mail\%
- User ID: \%D.sAMAccountName\%

For the Password option, enter a dummy password. The value for Domain is set to a fixed value.

12. Link the policies to Afaria groups as follows:

- Policies linked to the Afaria static group:

- Policy linked to the Afaria user group:
Starting the Device Connection to the Afaria Server

This example uses a Samsung S3 with Android 4.1.2 installed.

1. Configure the device security settings to allow the unknown sources. This is required for the MMEP client extension, which allows you to configure specific Samsung configuration features. The MMEP extension APK is not currently available from the Google play store. The unknown sources option must be enabled for all applications, which are not directly installed from the play store. In this example also for the NitroDesk client will be installed as enterprise app through Afaria.

2. Open the play store and search for “Afaria”. Select the Afaria Client for Android to install.

3. Tap Install.
4. Tap Accept and download.
5. Tap **Open**.

Configuring Afaria for Access Control
6. Tap Activate.
7. Enter the enrollment code and tap **OK**.
8. Set the user prompt for the Exchange User and tap **Done**.
You'll be prompted to authenticate against MS AD. Tap **OK**.
9. Enter the MS AD user account as the user principal name the password and tap **OK**.
During the initial Afaria session, it downloads the MMEP client extension. 

10. Tap **Install**.
11. Tap **Activate**.
12. Tap **Done**.
Note: Do not connect again: the session is still running and the device is installing the NitroDesk app in the background.

13. Accept the License Agreement for the Touchdown client.
14. Tap **Back** to change the password.
15. Reenter the password for the user account and tap Next.
The wizard fails again because the device has not validated yet.
16. Press and hold the **Home** button on the device to switch to the Afaria client.
17. Tap Connect.
18. Press and hold the Home button on the device to switch back to the Nitrodesk Touchdown wizard.
19. Tap **Back** to return to the previous screen of the wizard and then tap **Next** to start NitroDesk Touchdown configuration.
The device sets up the account. When the NitroDesk Touchdown wizard finishes, you can now access Exchange and the device now appears on the Afaria Admin UI device list.

Configuring iOS Native Email Client for Exchange ActiveSync (Microsoft Active Directory Authentication)

This topic describes how to configure the iOS native E-mail client for EAS through Afaria with Microsoft Active Directory authentication and ISAPI filter on CAS server.

Prerequisites

- An Afaria 7.0 SP2 HotFix 14 server that has access to Microsoft AD
- An accessible MS domain
- An MS Exchange Server with a working user account and mailbox
- A Relay Server, which can be required for device access
- An iOS device able to connect the Afaria and the Exchange Server. This example uses an iPhone 3GS with iOS 6.1.3.
Task
Afaria Server Preparations:

1. From the **Server > Configuration > Security** page, configure the Server configuration security settings. These are the required security settings for MS active directory access, which is required to use AD variables.

The Afaria Server Configuration Access Control Options are not configured. Everything is default.

2. Create Afaria groups.

Two groups are created. One static group which is configured to use with the enrollment policy and one Afaria user group that is linked to the MS AD group “iOS”.
3. Create iOS enrollment and configuration policies.

4. From the **Policy > Edit > iOS Enrollment > Summary** page, create a URL code for enrollment. The example below uses TinyURL.
5. On the General screen, configure the required settings.

6. On the Group screen, link the static group.
7. From the Policy > Edit > iOS Enrollment > Variable page, configure the variables for the user prompts. *ExchangeUser* and *ExchangeDomain* variables are required for ISAPI validation. The user is not prompted to enter an Exchange user password, but must enter the password when the EAS profile is installed. No password information is stored on the Afaria database in this scenario.

Both variables are required for iOS validation through ISAPI. The ExchangeDomain variable should be filled out with the FQDN. Do not use the NetBios Domain name.

8. From Policy > Edit > iOS Configuration > Summary page, create an iOS configuration policy.

In this example, only the device password policy is configured.
9. Create another iOS configuration policy, which is used for Exchange configuration.

In this example, the following variables are configured:

- E-mail address: \%D.mail\%
- User ID: \%D.sAMAccountName\%
For the Password option, a dummy password is entered. The value for Domain Host is set to an Afaria Variable called “%S.ExchangeDomain%”.

10. Link the policies to Afaria groups.

- This screen shows a policy that is linked to the Afaria static group:

- This screen shows a policy that is linked to the Afaria user group:

### Starting the Device Connection to the Afaria Server

1. From the Apple App Store on the iOS device, search for “Afaria” and then tap **Install**.
2. Open the Afaria client.
3. Enter the enrollment code.
4. Enter the AD user authentication data and tap **OK**.
5. Enter your AD username and logon domain and tap **Done**.
6. Install the profile.
7. Tap **Done**.
You should see the Config Payload and the iOS config policies on the device profile list.
8. Enter the Exchange Account password.
You can now receive e-mails. EAS profile success is configured.
The device now appears on the Afaria Admin UI device list.

Independent of the device connecting to Exchange, the Devices.xml file is updated with an empty "client GUID" when the iOS device is enrolled, and configured with the ExchangeUser and ExchangeDomain values. During the initial Exchange connection, the incoming username is validated and if it matches with an existing empty client GUID entry in Devices.xml, a Newdevices.xml file is created on the ISAPI filter. This temporary XML file contains the iOS Exchange device identifier, which must be uploaded to the Afaria server to update the device information to the Afaria database. The updated information, which now includes the Exchange Identifier, is returned to the ISAPI filter and updates the Devices.xml file with the client GUID. An iOS device can not be validated without a valid client GUID.
Configuring Afaria for Access Control
Defining Access Control Policies

Access Control Policies define default synchronization policies, by device type or by group, for devices that synchronize with your enterprise’s e-mail environment, including those that are not managed by Afaria.

Access Control Policy Conflict Resolution

When a device is subject to more than one access control policy, the most restrictive policy takes precedence.

For example, if an Android device is subject to a default policy for Android that allows access, and a group policy that blocks access, then the device is blocked from synchronizing with the e-mail server.

Defining an Access Control Policy for Android

Define a default access control policy to manage e-mail synchronization for Android devices that enroll or reenroll in Afaria device management. When both group policies and device type policies are defined, the most restrictive policy is the one that takes effect.

Changing the default policy affects only newly enrolling or re-enrolling devices; Afaria does not retroactively apply such changes to devices that are already enrolled.

1. From the Afaria Administrator Web console, click Server > Configuration.
2. Navigate to the Component > Access Control Option page.
3. Click on the Access Policy tab.

Note: For the best control of access control policy on Android devices, configure NitroDesk by Afaria.

4. On the Android tab, indicate the access policy action parameters.
   - Always allow – allow synchronization requests at all times.
Defining an Access Control Policy for iOS

Define a default access control policy to manage e-mail synchronization for iOS devices that enroll or reenroll in Afaria device management.

Access control policies are prioritized in this order: group-level policy, device-level policy, server-level policy.

1. On the Home page Server tile, click Configuration.
2. Navigate to the Component > Access Control Option page.
3. Click the Access Policy tab.

4. Select the iOS tab, indicate the access policy action parameters.
   - Always allow – allow synchronization requests at all times.
   - Always block – block synchronization requests at all times.
   - Allow when:
     - Administered by mobile device management – the device is under Afaria iOS mobile device management (MDM) control.
     - Afaria installed and device connected within xx days and xx hours – Afaria is installed on the device and the device is connected within the number of days and hours specified.
hours specified here. If Afaria application is removed from the device, access is blocked.

• Assigned policy delivered within xx days and xx hours – assigned policies are reported to the Afaria server as delivered and installed on the device within the number of days and hours specified here, and as verified in the Policy Delivery log.

• Device hardware encrypted – the device has the hardware encryption feature enabled.

• Device uncompromised – the device's most recent connection did not report the device's status as jailbroken.

Defining an Access Control Policy for Windows Mobile

Define a default access control policy to manage e-mail synchronization for Windows Mobile devices that enroll or reenroll in Afaria device management. When both group policies and device type policies are defined, the most restrictive policy prevails.

Changing the default policy affects only newly enrolling or reenrolling devices; Afaria does not retroactively apply such changes to devices that are already enrolled.

1. From the Afaria Administrator Web console, click Server > Configuration.
2. Navigate to the Component > Access Control Option page.
3. Click the Windows Mobile tab.

4. Select the default policy:
   • Always allow – allow synchronization requests at all times.
   • Always block – block synchronization requests at all times.
   • Allow when connected within time frame – allow synchronization requests if its most recent Afaria device connection occurred within the defined time frame.
Add a Domain for Access Control

Add, modify, or delete an Exchange server domain for access control.

1. On the Home page Server tile, click Configuration.
2. Navigate to the Component > Access Control Option page.
3. Click the Domains tab.

4. Click Add.

- Enter the primary domain of the tenant. A primary domain maps to the network domain on which the server resides.
- Select the required access control policy.
- Specify the retry rate, in minutes.
  Retry rate is the interval time (in minutes) for a domain, based on the HTTP client requests that are made to the Afaria server. Retry rate lists the known devices for that domain, along with their Always allow or Always block status.
- Enter accepted domains of a primary domain. You can add multiple accepted domains, separated by a comma. There is no limit on the number of accepted domains. The name of each accepted domain must be fewer than 65 characters in length. The total list of accepted domains, including comma separators, must be fewer than 2550 characters in length.
  Exchange servers often host e-mail messages for multiple domains.
Duplicate accepted domains are automatically deleted from the Accepted Domains field when you save the domain information.

5. Click Save.

6. (Optional) To make changes to a domain, click the Domains tab, select the domain to change, then click Edit or Delete.

Note: Restart the ISAPI service if you are making any changes in the Domains tab to ensure that the ISAPI filter works properly.

Primary Domain/Accepted Domains Scenarios

This section discusses couple of primary domain and accepted domains scenarios.

Note: Only FQDN values are supported these scenarios. You cannot configure NetBIOS domain name.

Scenario 1: CAS 1 on one network domain and CAS 2 and CAS 3 are on a different network domain

CAS A runs on domain domainA.com, services domains A.com, AA.com, and AAA.com.
CAS B runs on domain domainB.com, services domains B.com, BB.com, and BBB.com.
CAS C runs on domain domainB.com, services domains C.com, CC.com, and CCC.com.

A primary domain maps to the network domain on which the server resides. The accepted domain list includes all supported e-mail domains. Therefore, this scenario has two primary domains on the Server > Configuration > Access Control Option page:

- One primary domain for domainA.com with accepted domains A.com, AA.com, and AAA.com
- One primary domain for domainB.com with accepted domains B.com, BB.com, BBB.com, C.com, CC.com, and CCC.com.

Scenario 2: CAS 1, CAS 2, and CAS 3 on different network domains

CAS A runs on domain domainA.com, services domains A.com, AA.com, and AAA.com.
CAS B runs on domain domainB.com, services domains B.com, BB.com, and BBB.com.
CAS C runs on domain domainC.com, services domains C.com, CC.com, and CCC.com.

A primary domain maps to the network domain on which the server resides. The accepted domain list includes all supported e-mail domains. Therefore, this scenario has three primary domains on the Server > Configuration > Access Control Option page:

- One primary domain for domainA.com with accepted domains A.com, AA.com, and AAA.com
Defining Access Control Policies

- One primary domain for domainB.com with accepted domains B.com, BB.com, and BBB.com
- One primary domain for domainC.com with accepted domains C.com, CC.com, and CCC.com.

Defining an Access Control Policy to Block or Allow by Group

To allow or block e-mail synchronization requests by group, create group-specific policy. When both group policies and device type policies are defined, the most restrictive policy prevails.

Blocking and allowing by groups can let you block devices that do not meet some criteria, or allow devices that meet some criteria. You define dynamic group with your criteria to use with this feature.

The frequency of the Dynamic Group Refresh schedule, access control polling interval, and device inventory reporting all affect when a group policy goes into effect on a device.

1. On the Home page Server tile, click Configuration to open the Server Configuration page.
2. Navigate to the Component > Access Control Option page.
3. Click the Groups tab.
4. (Optional) For blocking specific groups, in the block area, select a group in the available list and click the Arrow icon to move it to the selected list.
5. (Optional) For allowing groups, in the allow area, click Enable, select a group in the available list and click the Arrow icon to move it to the selected list.
6. Click Save.

If you create policies that conflict for a device, the most restrictive policy prevails.

Providing Access Control Information While Creating/Editing an iOS Enrollment Policy

You can set an access control policy for an iOS device while creating or editing an iOS enrollment policy.

1. From the Afaria Administrator Web console, click the Policy tab.
2. Click New > Enrollment > iOS.
3. In the left pane, select **General**.

4. Provide the following information in the Access Control section:
   - **Domain** – domain node of the e-mail address, expressed as a fully qualified domain.
   - **Policy** – accept (use default policy) or override (use explicit policy) the enterprise default policy for iOS, as defined in the iOS tab in the **Server > Configuration > Access Control Option** page. If you choose to use the explicit policy, select one of the following options:
     - Always allow – allow synchronization requests at all times.
     - Always block – block synchronization requests at all times.
     - Allow when
       - Administered by mobile device management – the device is under Afaria iOS mobile device management (MDM) control.
       - Afaria installed – Afaria is installed on the device and the device is connected within the number of days and hours specified in the **Server > Configuration > Access Control Option** page. If Afaria application is removed from the device, access is blocked.
       - Assigned policy delivered – assigned policies are reported to the Afaria server as delivered and installed on the device within the number of days and hours specified in the **Server > Configuration > Access Control Option** page, and as verified in the Policy Delivery log.
• Device hardware encrypted – the device has the hardware encryption feature enabled.
• Device uncompromised – the device's most recent connection did not report the device's status as jailbroken.

5. In the left pane, select **Variable** and add enrollment variables:
   a) Click **Add**
   b) Select one of the following variables:
      • ExchangeDomain (for Exchange and Domino environments)
      • ExchangePassword (for Exchange and Domino environments)
      • ExchangeUser (for Exchange and Domino environments)
      • UserName
   c) Enter a valid device prompt.
   d) Indicate whether to mask the device with asterisk (*) characters as the user types.
   e) Click the green checkmark to save the enrollment variable.
   f) Repeat for the remaining variables.
Defining Access Control Policies
Managing Devices

This section provides tasks for manually adding a device for access control and for viewing and editing the access control settings applied to a device.

Manually Adding a Device for Access Control

To manage access control to the e-mail server for devices (Android and Windows Mobile) that are not enrolled in Afaria management, manually add the device to the access control device list.

Note: iOS devices do not follow this procedure. Access control of iOS devices is managed only when it is enrolled with the Afaria server.

Manually add a device when it:

• synchronizes with your e-mail server but is not managed by Afaria.
• has, or will have, an installed Afaria application that has not connected to the server yet, and you want to ensure that the first synchronization request is managed with a non-default policy.

To add a device manually:

1. From the Afaria Administrator Web console, click Server > Configuration.
2. Navigate to the Component > Access Control Option page.
3. Click the Devices tab.
4. Click Add.
5. Complete the new device information.
• Device – identifier of the device that is synchronizing with the email environment.
• User name – the user node of the fully qualified e-mail user name used to synchronize with the email server.
• Domain – the domain node of the fully qualified e-mail user name used to synchronize with the email server.

Note: If the user name is in the format username@domain, then do not provide domain information in the Domain field. When the record is saved, the user name displays as \user@domain and the record is not eligible for further editing. To change the access policy, delete the access policy that was created earlier and add a new access policy.

6. Select the operating system of the device.
7. Select an access control policy for the device.
8. Click Save.

Viewing Access Control Information of a Device

To view access control information for Android and iOS devices, use the Device Inspector.

1. From Afaria Administrator Web console, click the Device tab.
2. Select a device.
3. Click the Show/Hide Inspector icon.
The Device Inspector displays the following information about access control:
- Access control policy that is applicable to the device
- Current access policy state for the device: allowed or blocked
- Device compliance state: Whether the device is compliant or not
- Last remediation timestamp for the device

**Access Control Device List**

Afaria displays access control devices and their policy assignments in different locations of the user interface, depending upon the device type.

Assignment locations include:
- Android, Windows Mobile, and Windows Phone — **Access Control Option > Devices** page tab.
  
  On the Devices tab, the device list displays your Afaria devices and white list devices that are access control devices. The Afaria server populates this list with Afaria devices after it assigns a synchronization policy to a connecting device. White list devices populate the list as you add them. Therefore, the list starts empty and grows as each Afaria device connects and receives its synchronization policy assignment, and as you manually add devices.

**Note:** When an Android device does not contain a known ActiveSync ID or an Exchange User ID, Access Control ID displays the value NOT_EXCHANGE followed by the client GUID.

- iOS — **Device List page**
Editing Device Information of an iOS Device

Edit device information, such as device name, device ownership type, values for user variables, Self-Service Portal registered username, and Afaria Access Control for E-mail policy.

You can edit information for an iOS device by following the procedure below from Device Inspector page, or you can select an iOS device from the Device page and click the Modify Access Control Policy icon.

1. From Afaria Administrator Web console, click the Device tab.
2. On the Device page, select a device.
3. On the top toolbar, click Edit.
4. Edit data as appropriate in the Device > Edit page.
• Device – click **Setup** to open the ID Setup dialog and select naming options:
  • (Optional) Optional Prefix – enter a prefix to use for the name. For example "Sales_".
  • (Optional) Data Column – select a data item to concatenate with the prefix. Selecting something meaningful to your organization can help facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
• Device Owner – set a corporate or personally owned device or reset to default value.
• (SSP) Registered User – device user name, as a user would provide for WindowsNT or LDAP authentication in your Afaria environment, such as Domain\UserName. If users have enrolled in management, this is the user name they provided for authentication on the Afaria Self-Service Portal or in response to a prompt for a user name.
• Notification Address – if a phone number is unavailable for SMS messaging, enter the address to which the server sends outbound notifications for configuring the Afaria application.
• E-mail Address and password – e-mail address and password for access control policy.
• Access Control Policy – click Setup to open the Device > Access Control Policy Setup dialog.

Accept (use default policy) or override (use explicit policy) the enterprise default policy for iOS, as defined on the iOS tab on the Server > Configuration > Access Control Option page. Select one of the following options to use an explicit policy:

• Always allow – allow synchronization requests at all times.
• Always block – block synchronization requests at all times.
• Allow when:
  • Administered by mobile device management – the device is under Afaria iOS mobile device management (MDM) control.
  • Afaria installed – the Afaria App Store application is installed.
  • Assigned policy delivered – assigned policies are reported to the Afaria server as delivered and installed on the device, as verified in the Policy Delivery log.
  • Device hardware encrypted – the device has the hardware encryption feature enabled.
  • Device uncompromised – the device's most recent connection did not report the device's status as jailbroken.

5. (Optional) Substitution – if you include user-defined substitution variables in policies that are planned for this device, define values for the appropriate variables. If the variable is not yet on the list, click Add to enter the variable name and value for the current device, as appropriate for your requirements.
The variables on the list are global for the current tenant. The values you define for the variables are for only the current device.

6. On the top of the page, click **Save**.
Managing Devices
Troubleshooting

If a device is not receiving e-mail, track down the relevant entries in the log file and in the Devices.xml file, and:

- Make sure ActiveSync IDs (ASIDs) in both files agree.
- Verify that the Exchange account information in both files agrees.
- Ensure the device is not being blocked because Afaria believes it to be out of compliance with policy.
Reference

This section provides a task for manually retrieving a device's "DeviceID" value. It also includes tasks for manually updating the database with nonstandard device types and for obtaining the email username format required by Afaria.

Exchange Environment Unique Device ID Value

For the Afaria Access Control for Email feature in a Microsoft Exchange environment, the Unique Device ID value is the “DeviceID” value stored in the device's registry.

You can obtain the value from a device if it has already connected to the e-mail server. Afaria cannot retrieve the value for you if an Afaria client is not installed. You can use your own method to retrieve the value or:

- Use a device utility to read the value.
- Use your Exchange Server ActiveSync Web Administration tool (browser address: http://<YourExchangeServer>/mobileadmin, this is the default location) to run a query that retrieves the value. Choose the **Remote Device Wipe** menu option and query for the user of interest. The query returns information about the devices associated with the user. Copy the value from the Device ID column and exit the page without initiating any further action.

Building a Database of Known Android Devices

To allow Afaria to map Android devices that use nonstandard device type identifiers for the Android default policy, capture the device type value from the access control filter log and add it to the Afaria database table. Note that this section describes how to configure built-in e-mail manually.

Afaria has no way of identifying incoming devices as Android devices. As a result, it cannot determine if the default policy must be applied to the device that is attempting to connect. Nonstandard device type values include MotoDROID2v451 and htcholiday.

For Afaria to identify the Android device and add it as an access control device, you must:

- Capture the Android device type.
- Add a value to an Afaria database table to identify the device type values that Android devices identify themselves as Known Android devices.
- Use data from the Afaria access control filter logs to configure the Android e-mail user name property.
The manner in which Android devices identify themselves to Afaria depends on the local e-mail server configuration and manufacturer specifications. Afaria requires additional steps to add Android devices for access control.

1. On an Android device that is enrolled in Afaria management, configure the native e-mail application or NitroDesk TouchDown application.
2. Connect the device to synchronize with the e-mail server.
3. On the server that hosts the Afaria access control filter, obtain the device type reported by the device in the C:\Windows\System32\config\systemprofile\AppData\Roaming\XSISAPI\XSISAPIPipe_Log.txt. For example, the device may report itself with a device type value such as TOUCHDOWN, MotoDROID2v451, htcholiday.

The following is a sample entry from XSISAPIPipe_Log.txt:

12-09-27 08:43 Responding '2' to request:ID='313334383734363439323238353835', USER='domain-name\droid',TYPE='TouchDown'

4. Compare the device type reported in the XSISAPIPipe_Log.txt with the device type in C:\Windows\System32\config\systemprofile\AppData\Roaming\XSISAPI\Devices.xml file.

If the device type reported by the device is not in the Devices.xml file, the Android device cannot be managed by Access Control. If the device type is in Devices.xml, no further action is required.

5. Open the A_CONFIGURATION_PROPERTY table in your database management console and update the ISAPIAndroidDeviceTypes row to add the new device type reported in XSISAPIPipe_Log.txt.

6. Using the Afaria Administration Client, restart the Afaria service.

7. Allow sufficient time for the Afaria server to update the devices list, according to the polling period defined on the Server > Configuration > Component > Access Control Option page.

8. After the polling period occurs, validate that the new device type is included in the devices list.
Manually Configuring an E-mail Application for Android Devices While Using an Access Control Policy

Configure an e-mail application for Android devices manually for access control policy.

Prerequisites

- Add the device type to the database. See Building a Database of Known Android Devices.
- Record the correct e-mail address format.

Task

Afaria has no way of identifying incoming devices as Android devices and therefore cannot map the Android default policy to the device. After an Android device type is listed in the Afaria database table as a known Android device, use data from the Afaria access control filter logs to configure the Android e-mail user name property.

Note: The e-mail address format must match the format that the device reported in the Afaria table A_ANDROID_DEVICES when it connects to the e-mail environment.

1. Configure e-mail on the device.
2. Connect the device to synchronize with the e-mail server.
3. On the server that hosts the Afaria access control filter, obtain the e-mail user name format (domain\user or user@domain) reported by the device in C:\Windows\System32\config\systemprofile\AppData\Roaming\XSISAPI\XSISAPIPipe_Log.txt.
4. Install the Afaria application on the device.
5. Enroll the device in Afaria management using an enrollment policy that includes a user-facing prompt for the device user name.
   If the MS Exchange user name prompt is not used, go to the Afaria application on the device and select Configuration > Exchange User Name. Enter the same e-mail user name format obtained from the XSISAPIPipe_Log.txt file.
6. Connect to Afaria.
7. Go to the Afaria Administrator Web Console and navigate to Server > Configuration > Component > Access Control Option. The Android device appears with the correct Device ID and Exchange ID in the Devices tab. You can now manage Android devices using separate, per-device policies, rather than having to use the default policy.
Reference
Index

A
access control 81
  add 91
  adding a domain 84
  Android 81
  device 91
  device list 93
  iOS 82
  Windows Mobile 83
Android 25, 101, 103

D
Data handler 5

Data Handler 12
Database 101

E
e-mail 25, 103

F
Filter 5

I
ISAPI 5, 8, 9