PUBLIC
2019-01-16

Configuring SAP Afaria

THE BEST RUN SAP

Content

1 Configuring Afaria

This section provides the tasks for configuring Afaria for operations. You configure Afaria using the Afaria Administration console, a web-based system administration and device management tool available with Afaria.

This section includes tasks for:

- Logging in to the Afaria Administration console
- Verifying Server settings configured during install
- Creating additional users
- Configuring Afaria components

1.1 Server Page Layout Guide

Learn about the Server page user interface controls.

Device Page Layout and User Interface Controls

1. Banner toolbar – for navigating to Device, Group, Policy, and Server Dashboard pages.
2. Banner bar links and selectors – for opening help and other links, and selecting servers and tenants.
3. Left toolbar – for navigating to related pages for logs, alerts, configuration, and roles.
4. Top toolbar- restart a server or view its sessions.

1.1.1 Graphical Dashboards

In the Afaria Administration console, dashboard views are available within the Device, Group, Policy, and Server pages. The horizontal bar graphs, vertical bar graphs, and pie charts, help you gain a quick understanding about your devices and operations.

2 Starting Operations

To get started with Afaria after completing the installation, complete tasks that prepare for, and validate, basic operations.

2.1 Logging in to the Afaria Administration Console

You access the Afaria Administration console from a web browser by navigating to the Afaria Administration console and then providing appropriate account credentials when prompted.

Context

If you are using Microsoft Windows authentication with Afaria, enter your user name in the format `<domain>\<user>`. If you are using Microsoft Active Directory, use the format `<subdomain>.<domain.com>\<user>` or `<user>@<domain>`.

> **i Note**
>
> On the first login after installation, only the account provided during installation can log in to the Afaria Administration console. If you are logged in to the network using a different user, the Enter Network Password dialog opens and you are prompted to enter the domain, username, and password of the installing account.

Procedure

1. From your browser, navigate to the Afaria Administration console.

   The address is in the format: `http://<AfariaAdministratorAddress>/<AfariaAdministratorVirtualDirectory>`

   > **i Note**
   >
   > If you are unable to access the administration console from a browser, verify the Afaria API Server and Administrator and IIS settings.

2. From the Log In page, enter your user name and password and click *Log In*.

2.2 Starting, Stopping, and Restarting the Afaria Server

This task describes how to start, stop, and restart the Afaria Server.

Context

Server/client sessions can run only when the server is started. You can conduct other operations, such as reviewing logs or reports, performing server configuration, or performing administration and user support tasks when the server is in a stopped or started state. Some configuration changes require you to restart the server to take effect.

Procedure

1. From the Afaria Administration console Home page, click the *Server Dashboard* button.
2. From the Status page of the Server Dashboard, select the server you want to start, stop, or restart from the *Servers* list.
3. From the top of the *Servers* list, click the appropriate button:
   - *Start* – start a stopped server
   - *Stop* – stop a running server
   - *Restart* – stop then restart a running server

3 Tenants

A tenant is a collection of devices, groups, policies, and server configurations on the SAP Afaria Server that has associated devices, groups, policies, and server configurations. You can use tenants to separate devices and operations for different hosting customers, enterprise divisions, or other organizations.

The SAP Afaria Server includes a system tenant. The system tenant is a valid for device management. SAP Afaria includes a predefined system tenant. You can use the system tenant to create additional non-system tenants.

- System tenant – predefined with name that matches the server name. Consider these items about the system tenant:
  - It is the only tenant unless you add additional tenants. The tenant name matches the server name you defined during installation.
  - It is a valid tenant for devices, groups, policies, server configuration, and all operations.
  - Its policies are shared across all other defined tenants. From another tenant, you can use system tenant policies but cannot edit system tenant policies.
  - It has access to all server configuration properties.
  - The system tenant can view custom views from all tenants, but the views only return resources contained by the system tenant.
- Non-system tenants – optional. Consider these items about non-system tenants:
  - They are valid tenants for devices, groups, policies, some server configuration, and all operations.
  - They have access to a limited set of server configuration properties and rely on system tenant configuration settings for all other configuration properties.
  - When using a non-system tenant, system tenant policies are available for use, but not for editing. System tenant policies are identified in a non-system tenant's policy list by italic font.
  - A non-system tenant can view custom views from all tenants, but the views only return resources contained by the tenant.
  - A non-system tenant can only view message logs for devices contained by the tenant.

3.1 Configuration for Tenants

A tenant is an entity you associate with a subset of the device base and its related operations and assets. You must create a tenant record before you can enroll devices for a tenant.

Status – the state of the tenant:

- Enabled – associated devices can connect and get managed and an administrator can operate and support the tenant.
- Disabled – associated devices can connect but are denied additional management. However, the existing data remains accessible to administrators.

You can change a tenant's status at any time.

3.2 Selecting a Tenant

When multiple tenants are defined, select a tenant to change the tenant context for configuration and management. If the system has only one tenant, it is the system tenant, which appears on the Home page banner at all times and is the tenant for all operations.

Context

The tenant list is cached when you start a session. If one administrator makes a change to the list during a session, other administrators do not see the change until their next session.

Procedure

1. On the Home page banner, click the *Tenant selector* list.
2. Select a tenant.

   The tenant selection persists until you change it.

3.3 Creating a Tenant

You can create a tenant to manage a selection of devices, groups, and policies.

Procedure

1. On the *Server* page, click the *Configuration* icon.
2. On the *Server* list, click *Tenant*.
3. Click *New*.
4. Perform the following tasks:
   a. Select the state of the tenant.
   b. Type a name for the tenant.
   c. (Optional) Type a short description for the tenant.
   - State – enabled or disabled.
   - Tenant – name of the tenant.
   - Note – a short description of the tenant.
5. Click *Save* next to the *Note* field.
6. Click *Save* at the top of the page.

3.4 Disabling a Tenant

Disable a tenant to prevent devices from running sessions for a tenant but preserve all the tenant's existing data. You can disable a tenant on a temporary or permanent basis; you cannot disable the system tenant.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Tenant*.
3. Select a tenant in an Enabled state.
4. Click *Disable*.
5. Click *Save*.

3.5 Deleting a Tenant

Delete a tenant to permanently remove the record from your system. You cannot delete the system tenant.

Context

The scope of the tenant delete action includes deleting:

- Devices
- Groups
- Server schedules
- Substitution variables

If you plan to delete a tenant, you are advised to first delete the tenant-based items that are outside the scope of the tenant delete action:

- Logs
- Policies
- Device activity data, as defined on the Device Activity List page.

This tenant data is subject to becoming orphaned during a tenant delete action.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.

2. Select *Server* > *Tenant*.
3. Select a tenant to delete.
4. Click *Delete*.
5. Click *Yes, Continue*.
6. Click *Save*.

4 Roles

The Afaria Administration console uses roles to control access to the application and its individual features and tenants. Roles are assigned to user accounts on your network. For example, you can define a role with permission to view groups and policies but without permission to create, update, or delete them. You can then assign this role to a specific user on your network to ensure this user is restricted from updating policies. Roles can also be used to restrict a user to a specific tenant in the system.

Afaria installs with two predefined roles:

- Administrators – By default, this role allows users unrestricted access to the Afaria Administration console. Assign this role to users requiring full access to Afaria Administration console and all tenant settings.
- Help Desk – By default, this role allows users only view, access, and select permissions. Assign this role to users who perform administrative operations and provide support for users.

If your role is defined in Afaria Administration console, you can edit the predefined roles or add new roles.

4.1 Permissions

This section describes the permissions settings on the Role tab of the Add Role or Edit Role page.

4.1.1 Device, Groups, and Policy Permissions

The Device, Groups, and Policy permissions determine the actions the role can perform on devices, groups, and policies.

Permission	Description
Create	Allows the role to create groups and policies
Dashboard	Allows the role to view device, group, or policy dashboards
Delete	Allows the role to remove devices, groups, and policies
Link View	Allows the role to load, filter, sort, and link/unlink devices, groups, or policies in the link panel on device, group, or policy pages. For example, when a role includes the Link View permission for Policy:

Permission	Description
	• The role can access the policy grid in the link panel on the Group page. • The role can access the policy grid in the link panel on the Device page.
List View	Allows the role to view the list view on the device, group, and policy pages.
Update	Allows the role to edit devices, groups, and policies

4.1.2 Data Views Permissions

The Data View permissions determine which data views and logs a role can access.

Permission	Description
Select	Allows the role to select the data views displayed on the Device, Activity, and Server log pages. The role can select data views from the list of existing data views.
Update	Allows the role to create new data views

4.1.3 Device Inspector Tabs Permissions

The Device Inspector Tabs permissions determine the information a role can view in the Device Inspector.

Permission	Description
View	Allows the role to see the tabs in the Device Inspector that contain inventory information and log files.

4.1.4 Remote Actions on Devices Permissions

The Remote Actions on Devices permissions determine the remote actions a role can perform on devices.

Permission	Description
Access	Allows users to perform remote actions such as applying policies to a device, remotely wiping a device, and revoking certificates on a device.

4.1.5 Server Actions Permissions

The Server Actions permissions determine which actions a role can perform on servers.

Permission	Description
Access	Allows the role to perform actions such as restarting a server

4.1.6 Server Pages Permissions

The Server Pages permissions determine which Server pages a role can view or update.

> **i Note**
>
> The View permission for Configuration must be selected for the Server Configuration Pages permissions to apply.

Permission	Description
View	Allows the role to view Server pages
Update	Allows the role to configure alerts and roles

4.1.7 Server Configuration Pages Permissions

The Server Configuration Pages permissions determine which Server Configuration pages a role can view or update.

> **i Note**
>
> The Server Configuration Pages permissions apply only if the View permission is selected for Configuration in the Server Pages permissions. If the View permission is not selected for Configuration in the Server Pages permissions, the server configuration pages are not visible to the role.

Permission	Description
View	Allows the role to view Server Configuration pages
Update	Allows the role to edit Server Configuration pages

4.2 Configuration for Tenants

A tenant is an entity you associate with a subset of the device base and its related operations and assets. You must create a tenant record before you can enroll devices for a tenant.

Status – the state of the tenant:

- Enabled – associated devices can connect and get managed and an administrator can operate and support the tenant.
- Disabled – associated devices can connect but are denied additional management. However, the existing data remains accessible to administrators.

You can change a tenant's status at any time.

4.3 Creating a Role

This task provides the steps for defining a role, associating it with a tenant, and assigning it to one or more users or user groups.

Procedure

1. From the Server page, click *Role* on the left toolbar.
2. On the top toolbar, click *Add*.

   To edit an existing role, select it from the list and click *Edit*.
3. On the Role tab, type a name for the role and provide a description in the *Note* text box.
4. Select or clear checkboxes as required to grant or restrict permissions to policies and pages in the Afaria Administration console.
5. On the Tenants tab, select the tenants you want users assigned to this role to have access to.
6. On the Assignments tab, you can:
   - (Microsoft Active Directory only) Set a filter value in the Filter for next expansion text box to filter the contents that you see when you expand an organizational unit (OU) and click *Reload List*.

     > **i Note**
     >
     > The Filter for next expansion text box does not appear if Microsoft Windows NT is used in your environment.

   - To exclude seeing users within a group, select the group, click *Excluded in next expansion*, and click *Reload List*. To see the users within a group again, select the group, click *Excluded in next expansion*, and click *Reload List*.
   - Add a user or group by navigating the directory and selecting the user or group from the assignments tree.
   - Add a user or group by entering an explicit descriptor for the group (DomainName\GroupName) or user (UserName@Domain) in the Groups and Users for Role panel.

7. Click *Save*.

5 Configuring Afaria Connections

5.1 Verifying Afaria Server Settings for Device Communication

Verify server-device connection settings for connecting Android, Windows Mobile, and Windows devices for communications.

Context

After you configure Afaria Server for device communications, review your settings for correctness in Afaria Administration console.

Procedure

1. On the Server page, click *Configuration*, expand the *Communication* list, and click *Device Communication*.
2. Review the device communication settings for validity, namely: *Protocols and ports*, *Certificate settings*, and the *Address for Device communication*.

5.2 Verifying Afaria Server Settings After Installation

After you install Afaria Server, review your security (NT, Active Directory, or LDAP) and server farm settings in Afaria Administration console.

Procedure

1. On the Server page, click *Configuration*, expand the *Server* list, and click *Server Farm*.

   Review the settings for the server farm you set up for validity, namely: name, state, IP address, type, and replication address.

2. Select *Security*.

   Review and validate the settings for the NT, Active Directory, or LDAP domain.

6 Afaria Certificate Management

Afaria uses digital certificates to secure connections between managed mobile devices and servers and devices on your network such as your Enrollment Server, Exchange server, and WiFi routers. Certificates are issued by your enterprise's certificate authority (CA). You can use Afaria to request a certificate from your CA to send to the device. The device then uses the certificate to authenticate when it connects to your network.

Afaria supports Simple Certificate Enrollment Protocol (SCEP), Microsoft Certificate Authority, and Entrust Certificate Authority. SCEP is a widely-used certificate management protocol that allows you to request and issue large numbers of certificates with one request. You can use SCEP to request certificates from any SCEP-enabled CA.

Afaria also offers direct support for Microsoft and Entrust CAs. When you use one of these CAs, you can use Afaria not just to request certificates but also to manage these certificates in the Afaria Administration console. From the Device page, you can renew or revoke certificates on a device. For example, you can revoke a certificate on a lost device to prevent someone finding the device from gaining unauthorized access to your network. You can also use a number of certificate views to view information on active, expired, soon to expire, issued, and revoked certificates on your devices.

If you plan to use Microsoft Certificate Authority, you may need to install the CA proxy provided with Afaria on the server hosting the CA.

To configure Afaria for certificates, you must create one of more CA profiles from the *Server* > *Configuration* > *Certificate Authority* page. You use this page to enter CA server information such as server address and account credentials as well as requestor information such as organization and location. You then use this profile when you request a certificate from a configuration policy such as a Samsung SAFE WiFi policy or an iOS Exchange ActiveSync policy. When you apply the configuration policy, Afaria requests a certificate from your CA and sends it to the device. Certificates issued by supported CAs can be managed using a Device Certificates system view available from the Device page.

Afaria supports Entrust IdentityGuard versions 8 and 9 as the root CA. Please note that version 8 does not support revocation. If you renew a certificate issued by version 8, the old certificate is not revoked and stays active until it expires.

For more information on CA requirements, see the *SAP Afaria System Requirements*.

6.1 Creating Certificate Authority Profiles

Create a certificate authority profile to define the connections settings for certificate authorities that SAP Afaria uses.

Prerequisites

- Before you enable SSL, you must have a valid SSL certificate for the IIS server hosting the CA from a known certificate authority.
- To use SCEP, you must have the SCEP challenge details configured on the CA server.

Context

You can define up to 10 certificate authority (CA) profiles for each tenant. You can also define the information required to make SCEP requests to CA, to provide additional security.

Profiles are defined on a per-tenant basis. To configure a profile for more than one tenant, re-create the CA profile for each tenant using the same configuration information.

> **i Note**
>
> Afaria uses the largest renewal window from all configured profiles across all tenants and regardless of CA type.
>
> For example, consider an installation with two profiles:
>
> - Profile 1 has a CA Type of Microsoft Native and an auto-renewal window of 4 weeks. This profile is on the system tenant.
> - Profile 2 has a CA Type of Entrust and an auto-renewal window of 2 weeks. This profile is on a nonsystem tenant.
>
> In this scenario, Afaria renews all certificates, including those certificates issued from the Entrust CA, using the larger 4 week window set in Profile 1.

Once you have entered the required values, you can validate your configuration with the *Connectivity Test* button. For Entrust profiles, this test validates the following:

- The *Service URL* field has a properly formed URL starting with "http://".
- All required fields have been filled in. The required fields are Service URL, User, Entrust Group, Entrust Device Type, and Digital ID Config.
- Afaria can reach the Entrust server. If the connectivity test fails, Afaria displays the message returned from the endpoint such as `HTTP 405: Method Not Allowed` or `503: Server Unavailable`. Verify that the service URL is correct.

Procedure

1. In the Afaria Administration console, click *Server* > *Configuration*.
2. In the *Server* list, click *Certificate Authority*.
3. In the *Definition* pane, click *Add*.
4. In the *Name* field, type a name for the profile.

   The name of a profile must be unique to the tenant.
5. Select the CA type, either SCEP, Microsoft Native (if using a Microsoft CA), or Entrust.
6. Set properties for the profile as required.
7. Click *Connectivity Test* to test the CA connection from the testing server location.

   This test is valid only if the testing server can access the CA address. Accessing the CA from the testing server may differ from accessing it from the connecting devices.
8. Click *Save*.
9. Restart the Afaria server service.

Related Information

Associating Certificate Authorities for Enrollment and Package Servers [page 31]
Configuring Relay Server for Certificate Authority [page 86]

6.1.1 SCEP Profile Settings

For SCEP request profiles, set properties as described in the following table.

Setting	Description
HTTPS	Enable if you require SSL connections between Afaria and the certificate authority.
Server Address	Type the IP or fully qualified address of the certificate authority. Devices use this address to communicate with the certificate authority, so the address must be public. If you use SSL on a port other than port 443, type the server address using the syntax `<address>[:<port>]`.
Organization	Specify the organization to include in the certificate that the certificate authority delivers to devices.
Unit	Specify the unit to include in the certificate that the certificate authority delivers to devices.
City	Specify the city to include in the certificate that the certificate authority delivers to devices.

Setting	Description
State	Specify the state to include in the certificate that the certificate authority delivers to devices.
Country	Specify country to include in the certificate that the certificate authority delivers to devices.
Subject Alt Name Type	Select the Subject Alt Name type.
Subject Alt Name Value	Enter the Subject Alt Name value.
Auto Renewal	Enable if you want to automatically renew the certificate a given number of weeks before expiration.
Window	Enter the number of weeks before expiration. When a device with a certificate in the expiration window connects to Afaria, the CA issues a new certificate and revokes the old one. **i Note** When automatically renewing certificates, Afaria uses only the largest renewal window from all configured profiles across all tenants and regardless of CA type. For example, consider an installation with two profiles: • Profile 1 has a CA Type of Microsoft Native and an auto-renewal window of 4 weeks. This profile is on the system tenant. • Profile 2 has a CA Type of Entrust and an auto-renewal window of 2 weeks. This profile is on a nonsystem tenant. In this scenario, Afaria renews all certificates, including those certificates issued from the Entrust CA, using the larger 4 week window set in Profile 1.
Relay Server	Enable if you use a relay server with the certificate authority.
Server Address	Type the IP or fully qualified address of the relay server.
Farm ID	Specify the farm ID for the relay server.
Device URL Prefix	Specify the device URL prefix for the relay server
Challenge	Enable if you want devices to be able to submit SCEP requests to the certificate authority.
Domain	Type the domain of the account that devices use to submit SCEP requests.
User	Type the username of the account that devices use to submit SCEP requests.
Password	Type the SCEP password challenge.
Confirm	Retype the SCEP password challenge to confirm.

6.1.2 Microsoft CA Profile Settings

For Microsoft Native profiles, set properties as described in the following table.

Setting	Description
Server Address	Type the IP or fully qualified address of the certificate authority. Devices use this address to communicate with the certificate authority (CA), so the address must be public. If you use SSL on a port other than port 443, type the server address using the syntax `<address>[:<port>]`.
CA Name	Type the exact name of the certificate authority. The CA Name is not the same as the host name of the CA server.
CA Proxy	If you set up a CA proxy to communicate with your CA, click *Setup* and provide the name, IP address, and port of the proxy.
User	Type the user name of a domain user or a trusted domain user account with batch logon permissions. This account must have the following permissions in the CA: • Read and Enroll permissions for certificate templates • Read, Issue, and Manage Certificates, and Request Certificates in the Security options at the CA level to issue and revoke certificates **i Note** If you set up a CA proxy, use the same account you defined during CA proxy setup.
Password	Type the password of the account.
Confirm	Retype the password to confirm.
Template	Select a template for the certificate. Click *Update* to refresh the list with available templates.
Organization	Specify the organization to include in the certificate that the certificate authority delivers to devices.
Unit	Specify the unit to include in the certificate that the certificate authority delivers to devices.
City	Specify the city to include in the certificate that the certificate authority delivers to devices.
State	Specify the state to include in the certificate that the certificate authority delivers to devices.
Country	Specify country to include in the certificate that the certificate authority delivers to devices.
Subject Alt Name Type	Select the Subject Alt Name type.
Subject Alt Name Value	Enter the Subject Alt Name value.
Auto Renewal	Enable if you want to automatically renew the certificate a given number of weeks before expiration.

Setting	Description
Window	Enter the number of weeks before expiration. When a device with a certificate in the expiration window connects to Afaria, the CA issues a new certificate and revokes the old one. **i Note** When automatically renewing certificates, Afaria uses only the largest renewal window from all configured profiles across all tenants and regardless of CA type. For example, consider an installation with two profiles: • Profile 1 has a CA Type of Microsoft Native and an auto-renewal window of 4 weeks. This profile is on the system tenant. • Profile 2 has a CA Type of Entrust and an auto-renewal window of 2 weeks. This profile is on a nonsystem tenant. In this scenario, Afaria renews all certificates, including those certificates issued from the Entrust CA, using the larger 4 week window set in Profile 1.
Revocation	Enable if you want to allow administrators to revoke certificates that are issued using this profile. When you revoke an active certificate outside the expiration window, the CA adds the certificate to the Certificate Revocation List (CRL). Certificates on the CRL are not valid and cannot be used. If the certificate is within the expiration window or has expired, the certificate is revoked locally with Afaria. To improve performance, Afaria does not revoke these certificates with the CA.

6.1.3 Entrust Profile Settings

For Entrust profiles, set properties as described in the following table.

Setting	Description
API Level	Enable if you are using version 8 of the Entrust CA. Please note that v8 does not support revocation.
Service URL	Enter the fully qualified service URL and URI for the Entrust MDM Web Service. The service URL is composed of the server URL and web service URI in the format `<hostname>:<port>/<URI>`. The hostname is the IP or fully qualified address of the Entrust MDM Web Service. For example: `https://mobileservices.entrust.com:19443/mdmws/services/AdminServiceV9`

Setting	Description
	Note If you use the Entrust Managed Services PKI MDM web service, then the default port is `19443`. If you use the Entrust Authority Administration Services MDM web service, then the default port is `19443`. If you use Entrust IdentityGuard MDM web service, then the default port is `8444`.
User	The user name that Afaria uses to authenticate with the Entrust server
Password	The password that Afaria uses to authenticate with the Entrust server
Confirm	Retype the password to confirm.
Entrust Group	Entrust Security Manager group. Blank is interpreted as the default group.
Entrust Device Type	Entrust device type, such as MDM.
Digital ID Config	Enter the Digital ID as per your configuration. The Digital ID is the name of the template the Entrust CA uses to create the certificate.
Auto Renewal	Enable if you want to automatically renew the certificate a given number of weeks before expiration.
Window	Enter the number of weeks before expiration. When a device with a certificate in the expiration window connects to Afaria, the CA issues a new certificate and revokes the old one. Please note that version 8 of the Entrust CA does not support revocation. At renewal, the old certificate stays active until it expires. **Note** When automatically renewing certificates, Afaria uses only the largest renewal window from all configured profiles across all tenants and regardless of CA type. For example, consider an installation with two profiles: • Profile 1 has a CA Type of Microsoft Native and an auto-renewal window of 4 weeks. This profile is on the system tenant. • Profile 2 has a CA Type of Entrust and an auto-renewal window of 2 weeks. This profile is on a nonsystem tenant. In this scenario, Afaria renews all certificates, including those certificates issued from the Entrust CA, using the larger 4 week window set in Profile 1.
Revocation	Enable if you want to allow administrators to revoke certificates that are issued using this profile. When you revoke an active certificate outside the expiration window, the CA adds the certificate to the Certificate Revocation List (CRL). Certificates on the CRL are not valid and cannot be used.

Setting	Description
	If the certificate is within the expiration window or has expired, the certificate is revoked locally with Afaria. To improve performance, Afaria does not revoke these certificates with the CA.

6.2 Associating Certificate Authorities for Enrollment and Package Servers

Associate certificate authority (CA) profiles to the enrollment or Package Server to support enrollment of iOS and Windows Phone devices, or to provide user or device certificates to facilitate application onboarding.

Context

If you are using relay server, the relay server settings of the enrollment or package server are used for the initial communication to Afaria. The relay server settings of the CA profile retrieve certificates for the enrollment or Package Server.

Procedure

1. On the Server page, click *Configuration* on the left toolbar, expand the *Server* list, and click *Certificate Authority*.
2. Select a CA profile for the Enrollment Server from the *For Enrollment Server* list.
3. Select a CA profile for the Package Server from the *For Package Server* list.

   The lists show only the CA profiles defined for your tenant. The system tenant CA profiles are visible to all tenants.
4. Click *Save*.

Related Information

Creating Certificate Authority Profiles [page 25]

7 Configuring Afaria Components

Related Information

Configuring Afaria Server for Package Server [page 39]
Configuring Relay Server for Access Control [page 60]
Configuring the Relay Server for Certificate Authority and Enrollment Server Connections [page 37]

7.1 Enrollment Server

The SAP Afaria Enrollment Server supports device enrollment.

During the enrollment of devices, the Enrollment server retrieves enrollment policies from the SAP Afaria database and sends the enrollment policies to the devices.

The Enrollment server sends MDM payloads to iOS devices. To help prevent tampering with the MDM payloads during delivery, you can configure the Enrollment Server to use a certificate to digitally sign the MDM payloads.

You can install the Enrollment Server on the same computer as the SAP Afaria Server or on a separate computer in the same network.

7.1.1 Configuring Afaria Server for Basic Enrollment Server

Configure the Afaria Server for the Enrollment Server, as installed with payload-signing disabled, without enabling SSL on the HTTPS port, and without enabling relay server.

Procedure

1. On the Server page, click *Configuration* on the left toolbar, expand the *Component* list, and click *Enrollment Server*.
2. Accept or define the IP or fully qualified server address devices use to connect to the Enrollment Server.

   The address must be externally accessible.
3. Accept or define the unauthorized and authorized virtual directory names, as defined during the Enrollment Server installation.

The unauthorized directory accepts an initial device connection and processes any required user authentication.

The authorized directory accepts device connections in the connection series after the device connects to the unauthorized directory.

4. Only if you are required to use a proxy for the Apple APNS and feedback servers, click *APNS/Feedback Configuration* and change the predefined settings to your proxy server.
   - APNS domain and port for sending notifications.
   - Feedback domain and port for soliciting feedback, as defined by Apple.

   The feedback service is an aid for gaining feedback about devices that no longer have MDM control installed. Afaria captures feedback data in the A_iphone_feedback_log table. If feedback is received about a device having removed control, Afaria updates the known device state and adds an entry to the Messages log identifying the device and indicating that control is removed.
5. Click *Save*.

7.1.2 Configuring Afaria Server for Enrollment Codes

Enable at least one URL shortening service before creating enrollment policies.

Prerequisites

To enable the Google URL service, you need a Google API key, as issued by Google to your enterprise, as part of the Google API program. You can obtain the API key from the Google Developers website.

Context

Service terms are between your enterprise and the service provider. You must accept the terms of service to enable a service.

Procedure

1. On the Server page, click the *Configuration* icon on the left toolbar, expand the *Server* list and select *Enrollment Code*.
   - TinyURL service
   - Google URL service (including the API Key)
2. (Optional) Click the test links to verify connectivity and a call to the service.
3. To change how long an enrollment code is valid for iOS and Android device enrollment, under Self-Service Portal enrollment requests, specify *how long a user request is valid to use for enrollment* in days, hours and minutes.

Self-Service Portal enrollment for other device types does not include a validity time window.

4. Click *Save*.

Related Information

Configuring Firebase/Google Cloud Messaging [page 133]

7.1.3 Configuring Afaria Server for iOS Notifications

Add Apple push certificates for iOS device management to the Afaria Server, define the text to send to devices for SMS-based outbound notifications, and select whether managed applications collect diagnostic information.

Context

The Apple Push Notification service (APNs) certificate, as issued by Apple to your enterprise, uniquely identifies an Afaria Server and its associated enterprise to the APNs. See *Apple Certificates* in the *Preparing to Install SAP Afaria* document.

> **i** Note
>
> The SSL certificate that you create for your custom-signed iOS client (step 3) through the Apple developer portal must be for the production APNs servers. Do not use a development SSL certificate.

Consider the configuration of your enterprise tenant environment before operating Afaria:

- If you are an enterprise using only system tenant, install your Apple push certificate on the system tenant.
- If you are an enterprise, using multiple tenants to separate operations install your Apple push certificate on the system tenant.
- If you are a hosting enterprise using multiple tenants to separate multiple customers, ensure each customer installs their own Apple push certificate on their tenant. Do not install a push certificate on the system tenant; it is the backup certificate for tenants that do not have a certificate.

Procedure

1. On the Afaria Administration console Server page, click the *Configuration* icon on the left toolbar, expand the *Component* list and select *iOS Notification*.
2. In the APNS Push Certificate (for Mobile Device Management) pane, perform the following tasks to add an APNs push certificate for mobile device management:
   a. Click *Browse* to navigate to and select the certificate.

If you use an iPad for managing devices, the browse option does not work as there is no file system support on iOS devices.

The certificate is installed to the local machine personal certificate store on the Afaria Server. The MDM certificate name populates the page. The Current Push Service is the topic name, as defined by Apple on the certificate.

(System tenant) If your Apple root and intermediate certificates are not installed, the interface prompts you to install them.

(Non-system tenant) If Apple root and intermediate certificates are not installed, the interface opens an error. Notify your system tenant administrator.

b. In the *Password* field, type the password for the certificate.
c. Click *Install* to install the certificate.

3. In the APNS Push Certificate (for Custom-Signed Afaria Application) pane, perform the following tasks to add an APNs push certificate for custom-signed applications:
   a. Click *Browse* to navigate to and select the certificate.

> **i Note**
>
> Ensure you use a production SSL certificate. Do not use a development SSL certificate.

   If you use an iPad for managing devices, the browse option does not work as there is no file system support on iOS devices.
   b. In the *Password* field, type the password for the certificate.
   c. Click *Install* to install the certificate.
4. In the Notification Messages pane, perform the following tasks to include a customized message on devices when Afaria delivers policies:
   a. Select *Include following text*.
   b. Type the message.
5. In the Managed App Feedback pane, select whether managed applications collect diagnostic information about the application and send the information to Afaria.

   The application must include functionality to collect the diagnostic information.
6. Click *Save*.

7.1.4 Configuring SSL Connections for Enrollment Server

Configure the Afaria Server for enrollment server SSL connections when preferred or required for network security.

Prerequisites

This task assumes that you have a valid SSL certificate from a known certificate authority for your enrollment server's IIS server.

Procedure

1. On the Afaria Administration console Enrollment Server page, in the Enrollment Server group, click *Use HTTPS on Enrollment Server connections*.
2. Ensure that the server address uses the fully qualified address or IP address, as declared on the associated SSL certificate.
3. If you enabled the Enrollment Server's SSL on a port other than default port 443, update the server address to include the port suffix using the syntax `<Address>[:<port>]`.

   Windows Phone device enrollment works only with HTTPS, when communicating with the discovery service and the enrollment server. For Windows Phone devices, if you use non-default port and HTTPS in a self-signed environment, you must specify the port in the enrollment server address, for the enrollment to work. If you use default port in a self-signed environment, the enrollment settings configured for HTTP will automatically switch to HTTPS on the device.
4. Restart the Afaria Server service.

7.1.5 Adding iOS MDM Payload Signing for iOS

Add payload signing to ensure that payloads are not tampered with during delivery. You can use your Apple APNS certificate for signing.

Prerequisites

Install, configure, and verify the iOS implementation before adding signing.

Procedure

1. Copy the Apple root and application integration certificates and your Apple Push Notification Service (APNS) certificate to the enrollment server.
2. On the enrollment server, import your Apple root and application integration certificates as trusted root certificates.
3. Reinstall the enrollment server to enable signing and import your APNS certificate.
4. Use the Afaria Administration console Enrollment Server page to enable signing.
5. Restart Afaria Server.
6. Enroll one or more test devices and observe the user interface to determine whether the certificate is untrusted or trusted.

   The expected result, after a possible user authentication prompt, is either:
   - Signed, but untrusted – the Apple Profile Service dialog is exposed to the user and indicates status "Not Verified."
   - Signed and trusted – the Apple Profile Service dialog is exposed to the user and indicates status "Verified."

7. If untrusted and you require trust, deploy a root certificate to the client that matches the root certificate that the enrollment server is using and retry the enrollment.

7.1.5.1 Configuring Afaria Server for iOS MDM Payload Signing

Configure the Afaria Server to enable signing for all iOS MDM payloads.

Procedure

1. On the Server page, click *Configuration* on the left toolbar, expand the *Component* list, and click *Enrollment Server*.
2. Enter the signing certificate name, which is the common name for the signing certificate, as defined on the certificate and during enrollment server installation.
3. (Optional) Click *Encrypt payload* to encrypt the signed payloads.
4. Click Save.
5. Restart Afaria Server.
6. Provision one or more test devices and observe the user interface to determine whether the certificate is untrusted or trusted.

   The expected result, after a possible user authentication prompt, is either:
   - Signed, but untrusted – the Apple Profile Service dialog is exposed to the user and indicates status "Not Verified."
   - Signed and trusted – the Apple Profile Service dialog is exposed to the user and indicates status "Verified."
7. If untrusted and you require trust, deploy a root certificate to the device that matches the root certificate that the enrollment server is using and retry the provisioning.

7.1.6 Configuring the Relay Server for Certificate Authority and Enrollment Server Connections

(Optional) Set up relay server to increase your enterprise network security. A relay server is installed in the DMZ and operates as a proxy for HTTP and HTTPS sessions between two components.

Context

The enrollment server acts as a proxy for all certificate requests coming from devices. The devices connect to the enrollment server and then the enrollment server connects to the certificate authority (CA). You can

configure a relay server connection between the enrollment server and the CA, and a separate relay server connection between the devices and the enrollment server.

Related Information

Relay Server 16 (Deprecated) [page 69]
Server Configuration for Installation and Management [page 122]

7.1.7 Configuring Domains for Enrolling Windows Phone and Windows DM Devices

Configure domains for enrolling Windows Phone and Windows DM (Windows 8.1) devices through the discovery server.

Context

Domains are created specific to tenants. A domain can be part of only one tenant in the system. Multiple domains are allowed in a single tenant.

Procedure

1. On the Server page, select *Configuration* > *Enrollment* > *Domains*.
2. Click *Add*, and enter the domain name.

   > **i Note**
   >
   > Sub-domains must be explicitly defined; they are not assumed when domains are defined.

3. Click the *Save* icon, and then click the *Save* button.

7.2 About the Package Server

The SAP Afaria Package Server sends enterprise application packages to devices, and certificates and provisioning data to enterprise applications on devices.

The Package Server does not send commercial application packages to devices.

7.2.1 Configuring Afaria Server for Package Server

Configure the Afaria Server for the Package Server, without enabling SSL on the HTTPS port and without enabling relay server.

Procedure

1. On the Server page, click *Configuration* on the left toolbar, expand the *Component* list, and click *Package Server*.
2. Accept or define the virtual directory name, as defined during the package server installation.
3. In the Package Server Direct Access group, accept or define the IP or fully qualified server address devices use to connect to the Package Server.

   The address must be externally accessible.
4. Click *Save*.

Related Information

Relay Server 16 (Deprecated) [page 69]
Server Configuration for Installation and Management [page 122]

7.2.2 Configuring SSL Connections for Package Server

Configure the Afaria server for package server SSL connections when preferred or required for network security.

Prerequisites

This task assumes that you have a valid SSL certificate from a known certificate authority for your package server's IIS server.

Procedure

1. On the Afaria Administrator Package Server page, in the Package Server group, click *Use HTTPS on Package Server connections*.
2. Ensure that the server address uses the fully qualified address or IP address, as declared on the associated SSL certificate.

3. If you enabled the package server's SSL on a port other than default port 443, update the server address to include the port suffix using the syntax `<Address>[:<port>]`.
4. Restart the Afaria server service.

7.3 Self-Service Portal

The Self-Service Portal lets users enroll Android, iOS, Windows DM (Windows 8.1), Windows Phone, or Windows Mobile devices in Afaria management, view device information, and issue commands such as to remote lock or remote wipe a device.

> **i Note**
>
> For iOS devices using a non-custom version of the Afaria application (obtained from the App Store), the portal is the only method of obtaining iOS Enterprise Applications marked as Optional. The Afaria application does not display iOS Enterprise Applications on the apps tab, but will prompt the user to install any Required Enterprise Applications.

To use a signed and certified custom version of the Afaria application, contact Afaria technical support or refer to the support Website.

7.3.1 Afaria Self-Service Portal Address

The address for end-users to access the portal uses the portal's server address (host), the "SSP root virtual directory" you specify during installation, and a "Relative URL" value specified in the Afaria Administrator. The relative URL is at the end of the Self-Service Portal address and is used to distinguish one Self-Service Portal from another across the Afaria system.

To configure the relative URL value in the Afaria Administrator Web console, see the topic *Configuring Enrollment Codes for Self-Service Portal*.

The SSP URL uses the Relative URL value to access a specific portal record specified in Afaria Administration console using the following syntax:

`<protocol>://<host>/<SSP root dir>/<relative URL>`

The “SSP root dir” value in the URL format is specified while running the SSP installation program, and it cannot be changed once the SSP Website is installed. For more information, refer to the *Installing Afaria* guide.

For example:

- HTTP://portal.company.com/ssp/sales
- HTTP://63.176.1.74/ssp/accounts
- HTTPS://portal.company.com/ssp/marketing

7.3.2 Configuring Enrollment Codes for Self-Service Portal

Configure enrollment codes for different device types, and associate with an instance of the Self-Service Portal.

Procedure

1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Enrollment* > *Self-Service Portal* page.

   > **i Note**
   >
   > Every tenant has one self-service portal created for that tenant, containing default enrollment policies assigned to the portal, to aide in quick Self-Service Portal setup. You are free to edit this portal record, as well as add new portal records as desired.

3. On the Portals tab, click *Add* to add an instance of the Self-Service Portal.
4. Enter the description for the Self-service portal instance.
5. Enter the Relative URL portion of the SSP URL.

   The Relative URL value uniquely identifies this particular portal entry when accessing the SSP website. When creating a new SSP record, the Relative URL value will default to the tenant name, but should be changed to be unique. The Relative URL value is not case sensitive, and can only contain alpha numeric characters a-z, A-Z, 0-9, and an underscore (_) or dash (-).

   Make note of how the relative URL value will be used to navigate to the Afaria SSP URL with the following URL format: `<protocol>://<host>/<SSP root dir>/<Relative URL>`.

   > **i Note**
   >
   > The `<SSP Root dir>` portion of the SSP URL format is specified during the installation of the Self-Service Portal website, and cannot be changed after installation. For more information, refer to the *Installing Afaria* Guide.

6. Select the default enrollment codes or the enrollment policies/codes that were created earlier for the device types from the corresponding drop-down lists.

   The default enrollment codes for devices are created after installing Afaria. You can view the default enrollment settings in the *Server* > *Configuration* > *Default Enrollment Settings* page.

   > **i Note**
   >
   > The default enrollment codes are applicable for Android, iOS, Windows Phone and Windows DM devices only.

   For a device type, all the enrollment policies having enrollment codes enabled for the portal appear in the list.
7. Click the *Save* icon to save the changes to the SSP record, and then click *Save* at the top of the page after editing all SSP records.

7.3.3 Configuring User Group Access Gating for Self-Service Portal

You can optionally configure each Self-Service Portal to allow only preapproved group members to gain access to it.

Context

If this option is not enabled, any user in the Directory Server can log into the Afaria Self-Service Portal. The gating option prevents users who are not in the approved list of groups from logging in to the Self-Service Portal.

Procedure

1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Enrollment* > *Self-Service Portal* page.

   > **i Note**
   >
   > Every tenant has its own Self-Service Portal, which contains default enrollment policies intended to assist Self-Service Portal setup. You can edit this portal record, as well as add new ones.

3. On the Portals tab, click *Add* to add an instance of the Self-Service Portal.
4. Enter a description for the Self-Service Portal instance.
5. Enter the relative URL portion of the SSP URL.

   The relative URL value uniquely identifies this particular portal entry on the SSP Web site. When you create a new SSP record, the relative URL value defaults to the tenant name, but you should change it to a unique value. The relative URL value is case-insensitive, and can contain only alphanumeric characters a-z, A-Z, 0-9, underscores, and dashes.

   The relative URL value will navigate to the Afaria SSP URL, using the following URL format: `<protocol>://<host>/<SSP root dir>/<Relative URL>`.

   > **i Note**
   >
   > The `<SSP Root dir>` portion of the SSP URL format is specified during the installation of the Self-Service Portal website, and cannot be changed after installation. See the *Installing Afaria Guide*.

6. On the *Codes* subtab, select the default enrollment codes or the enrollment policies/codes that were created earlier for the device types.

   The default enrollment codes for devices are created after Afaria is installed. You can view the default enrollment settings on the *Server* > *Configuration* > *Default Enrollment Settings* page.

> **Note**
>
> The default enrollment codes are applicable only for Android, iOS, Windows Phone and Windows DM devices.

For each device type, all the enrollment policies having enrollment codes enabled for the portal appear in the list.

7. On the *Access* subtab, enable access gating by selecting *Restrict Access to Selected Afaria User Groups*. Select the existing Afaria user groups that are permitted to access the Self-Service Portal.

   When restricted access is enabled, any users that are not in the selected Afaria groups are denied access to the Self-Service Portal. The Afaria groups must be created prior to this step.

8. Click *Save* to save the changes to the SSP record, then click *Save* at the top of the page after editing all SSP records.

7.3.4 Configuring Afaria Server for Self-Service Portal Acceptance Message

Configure Afaria server to set up an optional acceptance message for the Self-Service Portal, in any of the languages supported by the system.

Prerequisites

Verify that the acceptance message in the required language is available for upload in HTML or text format. Contact the customer's legal department or other relevant sources to obtain a copy of the acceptance message.

Context

The end users can view, review, and accept the message, while accessing and enrolling devices using the Self-Service Portal.

Procedure

1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Enrollment* > *Self-Service Portal* page.
3. On the Acceptance tab, select the options for the acceptance message prompt on theSelf-Service Portal.
   - No prompt

- First time the user logs in to the Self-Service Portal
- Each time the acceptance message changes
- Each time the user enrolls a device using Self-Service Portal

> **i Note**
>
> By default, the option "Each time user enrolls device via Self-service portal" is selected.

4. Click *Add* to browse and select the custom acceptance message in the required language.

> **i Note**
>
> If you do not browse and select the custom acceptance message, the default acceptance message file (Default EULA) file will be used for acceptance message.

If you cancel the changes after uploading the acceptance file, the acceptance file is not deleted. Delete the file manually by clicking *Delete*.

If you want to reset the custom acceptance message files back to the default acceptance message files (Default EULA), click *Reset to defaults*.

5. Click *Preview* to view the acceptance message, as it will appear on the Self-Service Portal.
6. Click *Save*.

7.3.5 Configuring Afaria Server for Self-Service Portal Request Timeout

Configure the Afaria server to limit the amount of time Self-Service Portal users have to complete device enrollment, once started.

Context

You may have already configured this setting when configuring for enrollment server. This setting applies only for Android, iOS, Windows Phone, and Windows DM devices.

Procedure

1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Enrollment* > *Self-Service Portal* page.
3. On the Requests tab, specify the duration for the validity of the enrollment request.

   The default timeout is set to one hour.
4. By default, the checkbox Use Self-service portal registered user for assignments (all enrolling devices) and bypass authentication during enrollment (iOS only) is selected.

5. Click *Save*.

7.3.6 Editing Enrollment Codes for Self-Service Portal

Add new enrollment codes or edit existing enrollment codes for the Self-Service Portal in the Afaria Administration console.

Procedure

1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Enrollment* > *Self-Service Portal* page.
3. Select the portal instance for which you need to add or edit the enrollment code details.
4. Click *Edit* to modify the details as required.
   All enrollment codes available for a device type appear in the corresponding drop-down list.

7.3.7 Removing Association of Enrollment Codes from Self-Service Portal

Remove the association of an enrollment code from an instance of the Self-Service Portal if you no longer wish to use that enrollment code with a portal.

Procedure

1. On the Home page Server tab, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Enrollment* > *Self-Service Portal* page.
3. Edit the portal instance you wish to disassociate from the enrollment code.
4. Remove the enrollment policy association from the portal by selecting a different enrollment code, or setting it to blank (no enrollment policy associated).
5. Save your changes.
   Removing the association from the portal does not delete the enrollment policy or code; it only de-links the association between the enrollment code and the portal instance.

7.3.8 Configuring Self-Service Portal iOS Consolidated Authentication

Configure Afaria to use Self-Service Portal credentials for iOS device authentication during enrollment, when enrolling iOS devices via MDM-first enrollment.

Context

If this setting is turned on (default value is on), the end-user enters credentials and authenticates with the Self-Service Portal, and will not be requested to enter credentials to authenticate with enrollment server during enrollment. If this setting is turned off, the end-user enters credentials and authenticates with the portal and will be requested to enter credentials to authenticate with enrollment server during enrollment.

Procedure

1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Enrollment* > *Self-Service Portal* page.
3. On the Requests tab, in the 'Self-service portal consolidated authentication' section, turn on or off the setting to use the portal credentials for iOS device authentication during enrollment.

   This setting is turned on, by default.
4. Click *Save*.

7.3.8.1 Using iOS Consolidated Authentication with User Group Assignments

An advanced capability of the iOS consolidated authentication setting is to leverage user group assignments for iOS 8 and later devices based on the authenticated Self-Service Portal user name.

In addition to enabling this setting, the authentication methods of your Afaria components and user group assignments also must be set up and configured properly.

> **i** Note
>
> After completing MDM-first enrollment with iOS 8 and later devices, the policies linked to the user group assignments will be delivered to the device prior to the end-user launching the Afaria application on the device. If the end-user launches the Afaria application before receiving the polices linked to the user group assignments, the Afaria application will prompt the end-user for credentials, based on the authentication setup for enrollment server and package server.

7.3.9 Afaria-Managed Authentication for Self-Service Portal

The Self-Service Portal (SSP) uses Afaria-managed authentication, which authenticates the users with the directory security settings specified for the SSP's tenant.

The SSP authentication mechanism is not specified during installation of the Self-Service Portal. Instead, the Relative URL value that uniquely identifies the SSP, along with the tenant that the SSP belongs to, together determine the directory security authentication that the SSP uses when authenticating a user into the portal.

In addition to the Self-Service Portal, both the Enrollment Server and the Package Server use the same Afaria-managed authentication settings for the given tenant for both authentication and user group assignments. You control authentication for the Enrollment Server and Package Server using the *Server* > *Configuration* > *Security* page in the Afaria Administrator, and it can also optionally be disabled. However, the SSP authentication mechanism cannot be disabled; Afaria-managed authentication is always turned on for the SSP.

7.4 Setting Up SMTP

You can use the SMTP page to configure your SMTP server to send e-mail communications and e-mail-based Short Message Service (SMS) messages related to Afaria operations.

Procedure

1. On the Server page, click *Configuration*.
2. Enter the name of the SMTP Server.

   This field can contain either the IP address or the host name of the SMTP server that you use to send SMS messages.
3. Enter the *user ID* for the SMTP server account that you use to send SMS messages
4. Enter the *reply address* that appears on the SMS messages.
5. Click *Restart Server* for the changes to take effect.

7.5 SMS Gateway

Afaria uses the SMS Gateway to deliver outbound notifications, remote wipe commands, and any other communication that is addressed for SMS routing to supported devices.

The solution leverages the Cygwin product libraries and tools and other open source tools to implement its SMS Gateway. The Cygwin product is a set of libraries and tools developed by Cygnus Solutions that creates a Unix-emulating environment on a Windows operating system.

Due to the nature of open source licensing practices, cited in the GNU General Public License, SAP cannot distribute, install, or license the libraries and tools as part of a commercial product delivery. Therefore, you

must obtain and install the required items on behalf of your organization to enable the SMS Gateway operations.

7.5.1 Configuring SSL Connections for SMS Gateway

HTTPS support for SMS Gateway requires you to install a certificate that is known to both Windows and Linux.

Context

SMS Gateway runs on the Afaria Server and is encapsulated within an emulated Linux operating system environment; the Afaria Server runs on a Windows operating system. A certificate is required for proper communication between the two separate operating systems on the same server.

Procedure

1. Obtain a certificate and key that identify the Afaria server in PEM format.

   Ensure that the common name attribute on the certificate is the name of the Afaria Server, exactly as the name is defined in the Gateway Host field on the SMS Gateway configuration page.
2. Certificate for Windows – import the PEM-formatted certificate and its associated key as a visible Windows Trusted Root Certificate Authority. The Windows Trusted Root is accessible only to the Afaria Server.
3. Certificate for Linux – complete the "Cert file" and "Key file" fields on the SMS Gateway Interface configuration page to point to the certificate and key files. The files must reside on the Afaria Server. The SMS Gateway uses these references to access the certificates, as it cannot access certificates as imported into the Windows Trusted Root Certificate Authority.

7.5.2 Configuring Afaria Server for SMS Gateway

SMS Gateway configuration settings and data elements establish connectivity between the Afaria Server hosting the SMS Gateway and the Afaria SMS Gateway.

Context

In a farm environment, Afaria is always the main server.

To successfully start the SMS Gateway, you must define SMS Gateway properties and at least one SMSC server configuration entity.

Procedure

1. On the Server page, click the Configuration icon on the left panel, expand the Server list, and select *SMS Gateway*.
   The SMS Gateway page appears with the Gateway tab enabled.
2. Enter the Port number for the first Afaria Server port number dedicated to SMS Gateway communication. The server uses this port and the next two consecutive ports. For example, if you select port 3000, then the SMS Gateway uses ports 3000, 3001, and 3002.
3. Enter the Access Phrase for all communications from an Afaria Server to the SMS Gateway. SMS Gateway ignores all communications requests that do not include this phrase.
4. Click the *Character Set* SMS Gateway uses to compose SMS messages. The appearance of the message at the client depends on device support for a given character set. Devices that support ASCII but are sent a Unicode-based message show messages padded with extra characters.
5. (Optional) Click *Enable HTTPS Support* to enable HTTPS support for secure communications from the Afaria Server to the SMS Gateway.
6. Enter the Certificate File path and file name on the main Afaria Server for the PEM-formatted certificate file. The SMS Gateway uses this file to verify the identity of the Afaria Server.
7. Enter the Key File path and file name on the main Afaria server for the PEM-formatted key file. The SMS Gateway uses the file to verify the identity of the Afaria Server.
8. Define an SMSC server configuration entity.

7.5.3 Setting Up an SMS Modem

For each SMS modem from your providers, add and configure Afaria Server for communication.

Prerequisites

Follow the instructions from your modem provider to connect the modem to the Afaria Server.

Context

SMS modems are typically carrier specific, as each modem uses a carrier's Subscriber Identity Module (SIM) card. They use the associated carrier's network to deliver SMS messages to an SMSC; messages take an indirect path to the SMSC. Modems can often support basic SMS message (example: text messages) delivery to different carrier networks.

Procedure

1. On the Server page, click the *Configuration* icon, select the *Modem* tab, and click *Add*.
   You see a new line of configuration fields.
2. Select *Enable* to enable communications with this entity. Unselect the check box to suspend communications but retain the configuration values.
3. Enter the Name.
   The name you enter directly impacts how Afaria routes Afaria-initiated messages.
4. Select an Afaria Server COM port.
   Ports 1–16 are valid for the SMS Gateway operations.
5. Complete the required port, source, and destination properties guided by the definitions in the SMPP Configuration Properties topic.
6. Click *Save*.

7.5.4 Setting Up an SMPP Service

You can configure Short Message Peer-to-Peer (SMPP) entities for use with SMS Gateway on the Afaria Server.

Context

Short Message Peer-to-Peer (SMPP) is a protocol for delivering SMS messages directly to a Short Message Service Center (SMSC) or SMSC aggregator.

SMPP services are typically carrier agnostic. Message routing from the SMS Gateway is direct to the SMSC, rather than over a carrier network. As a result, an SMPP service can typically deliver most SMS messages to any carrier network.

> **i** Note
>
> You can create multiple SMPP entities, but Afaria Server uses only those that you enable.

Procedure

1. On the Server page, click the *Configuration* icon, select the *SMPP* tab, and click *Add*.
2. Select *Enable* to enable communications with this entity. Unselect the check box to suspend communications but retain the configuration values.
3. Enter the Name of the service.
   The name you enter directly impacts how Afaria routes Afaria-initiated messages.
4. As defined by your SMPP service provider, define the remaining property values.

5. Click *Save*.

7.6 Access Control

Access control regulates synchronization requests to email severs, both hosted and local, based on the settings in access control policies.

There are two implementations of Access Control:

- Access control remote for hosted email servers
- Access control filter for local email servers

7.6.1 Access Control Remote

Access control remote regulates synchronization requests to hosted email servers.

7.6.1.1 Configuring Access Control Remote

You can set up Access Control Remote for hosted email with Office 365 or local email using Microsoft Exchange PowerShell commandlets.

Prerequisites

- Ensure that the Access Control Filter is not installed.
- The PowerShell virtual directory is created when you install Exchange. Enable the powershell remoting by enabling Basic Authentication on the virtual directory in IIS.

Context

You can configure access control to match devices against multiple domains in a single active directory forest on your network by using the "Global" setting in the *Domain* list. To configure this, define a separate profile for each MS Exchange Client Access Server (CAS) you want to include. If your email is hosted externally, you are restricted to the "Local" setting. With the "Local" setting, access control can only match accounts in the same domain as the account you enter here.

E-mail services are available locally, where a local Exchange server is used. E-mail services are also 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. Afaria server communicates with Exchange for updating device status.

Afaria uses the following API calls on the Exchange server:

- Get-ActiveSyncDevice
- Get-CASMailbox
- Set-CASMailbox

For more information on these Microsoft Exchange server API calls, refer to Microsoft Exchange documentation.

In addition to the API calls on the Exchange server, Afaria also issues some setup commands to initiate the remote PowerShell session with the Exchange server.

Procedure

1. Log in to the Afaria Administration console.
2. Navigate to the *Server* > *Configuration* > *MS Exchange* page.

   > **i Note**
   >
   > Devices with ISAPI account and Microsoft Exchange account cannot co-exist in a tenant as this configuration is not supported. Ensure that this page is empty if the tenant is supposed to be used for local exchange.

3. Click *Add*.
4. Enter the following information:
   - List View – Select Include to include the CAS profile in the list
   - Remote – Select Include to match devices against this CAS server for access control.
   - MS Exchange CAS URL – Enter the URL of the hosted or local Exchange CAS server.
   - Domain – Select "Global" if you intend to define multiple CAS servers on your network. If your email is hosted externally, only the "Local" setting is available.
   - Account User – Enter the hosted or local Exchange Admin User ID. Create a user that is a member of the Exchange Organization Managers group so that the user will have minimum permission to execute PowerShell commands.
   - Password – Enter the hosted or local Exchange Admin password.

   > **i Note**
   >
   > Ensure that the Microsoft Exchange account credentials have Administrator privileges.

5. Click *Test connection* to authenticate the account credentials and test connectivity for the local Exchange or hosted accounts.

   If the account credentials are valid, you see a success message; otherwise, you see an error message.
6. Click *Save*.

   When Microsoft Exchange triggers e-mail blocking using access control, it may take as long as 10 minutes for Exchange to block e-mail messages.
7. Repeat steps 3 to 6 for each additional CAS server as required.

7.6.2 Access Control

Access control regulates synchronization requests to email servers.

Access Control can prevent synchronization requests that do not meet the access control policies in SAP Afaria. Access control policies include a list of known devices, their associated policies, any remediation actions, and any defined polices for unknown devices.

In addition to synchronization requests from devices, Access Control Filter can regulate synchronization requests from desktop and Web email clients.

7.6.2.1 Access Control Filter Components

The Access Control Filter includes a filter, data handler services, and a filter listener.

Filter (XSISAPI.dll)

The filter accepts inbound synchronization requests from devices and passes them to the data handler. The filter must reside on a server that can accept inbound requests.

Data Handler Services (XSISAPIReversePipe.exe)

The Data Handler Services determine whether to allow or block incoming synchronization requests.

Filter Listener (XISAPIServer.exe)

The Filter Listener queries the SAP Afaria database for the access control list and sends it to the Data Handler Services. The filter listener resides on the SAP Afaria server.

7.6.2.2 Installing Access Control Components on a Single Machine

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

Context

If all 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.

If 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.

Procedure

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*.

   Choose the appropriate version of the filter for your operating system: *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. If this option is selected, all traffic is allowed. If you do not select this option, only ActiveSync traffic is allowed and all other traffic is blocked. Any other Web sites on the same IIS are also blocked.
   b. Select an installation method – *Install ISAPI filter for IIS Server* or *Install ISAPI for ISA Server*.

   > **i Note**
   >
   > The ISAPI filter affects Outlook Web Access (OWA) if the Allow all traffic but Microsoft-Active-Sync option is not selected and OWA is being accessed from Client Access System (CAS) on which the filter is installed.
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.

7.6.2.3 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.

7.6.2.3.1 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. This option installs `XSISAPI.dll` and `XSISAPIReversePipe.exe` on an IIS/ISA server.

Context

Run the procedure on each IIS/ISA box.

Procedure

1. 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*.

   Choose the appropriate version of the filter for your operating system: *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 host name and port for the PowerShell proxy server and click *Next*.
8. From the Blocking Option screen, do the following, 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 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.

7.6.2.3.2 Installing Only the Data Handler

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.

Context

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

Procedure

1. 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*.

   Choose the appropriate version of the filter for your operating system: *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 host name 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.

7.6.2.4 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:

- `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. The 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="APPLDN50001EDKPJ" User="USR0001" SP="66" ExID="SY-ALPHAQA.COM
  \USR0001" Type="-8"  status="0" />
  <client GUID="APPLDN50002EDKPJ" 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-alphaqa.com\xoom', TYPE='SAMSUNGGTI9100'
  13-05-14 06:41 Responding '1' to request: ID='APPLDLXH20UKDKNW', USER='sy-
  alphaqa.com\mangesh01', TYPE='iPad'
  13-05-14 06:41 Responding '2' to request: ID='APPLC38GPXGVDT9V', USER='sy-
  alphaqa.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 – 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.

7.6.2.5 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.

7.6.2.6 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.

7.6.2.6.1 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.

Context

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.

Procedure

1. From the Afaria Administration 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.

7.6.2.6.2 Configuring Relay Server for Access Control

To configure the relay server to support the access control filter, define the relay server configuration file, configure settings on the Afaria Administration console, and reinstall the PowerShell component of the access control filter.

Prerequisites

- Configure the relay server for basic operations.
- Configure the relay server for the SAP Afaria, regardless of whether you plan to use it for device connections.
- Install and configure the access control filter components.

Procedure

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 filter's farm ID as **`Afariafarm-IS.`**

2. On the *Server* > *Configuration* > *Access Control Server* page of the Afaria Administration console, select *Use Relay Server*, then click *Save*.
3. Reinstall the PowerShell component of the 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 filter.
4. Restart the machine on which you reinstalled the PowerShell component.
5. Restart the relay server host.
6. In the Afaria Administration console, restart the Afaria server service.

Related Information

Access Control [page 51]
Relay Server 16 (Deprecated) [page 69]
Server Configuration for Installation and Management [page 122]

7.6.2.6.3 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.

Context

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

Procedure

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:
   - **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%`.

     > **i Note**
     >
     > If you use the `%S.ExchangeDomain%` variable, configure the enrollment policy so that either the domain is specified on the General page or the Exchange Domain device prompt is selected on the Variable page.
   - **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%`.

7.6.2.6.4 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:

Context

- ExchangeDomain (for Exchange and Domino environments)
- ExchangePassword (for Exchange and Domino environments)
- ExchangeUser (for Exchange and Domino environments)
- UserName

7.6.2.6.5 Substitution Variables Examples

This section provides examples of how to use substitution variables.

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%.

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.

7.6.2.6.6 Required E-Mail Formats for Android Devices

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

Ensure that users enter the information correctly. On the device's 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 table `A_ANDROID_DEVICES`, is:

- domain\user
- user@domain

7.6.2.6.7 Adding Unknown Devices to Access Control

You can add unknown devices to access control so that SAP Afaria recognizes the devices and applies the correct access control policies.

Context

SAP Afaria uses default access control policies for unknown devices. 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.

Procedure

1. Try to configure e-mail on the device.
2. On the server that hosts the Afaria access control filter, capture the Android device type reported by the device in `C:\Windows\System32\config\systemprofile\AppData\Roaming\XSISAPI\XSISAPIPipe_Log.txt`.
3. 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`.

   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.

   For example, the device may report itself with a device type value such as TOUCHDOWN, MotoDROID2v451, or htcholiday.

   The following is a sample entry from `XSISAPIPipe_Log.txt`:

   ```
   12-09-27 08:43 Responding '2' to
   request:ID='313334383734363434393232383538353835', USER='domain-name
   \droid',TYPE='TouchDown'
   ```

4. Using the Afaria Administration console, restart the Afaria service.

   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.
5. Try to configure email on the device again.

   As unknown policy is set to block, you will not be allowed to configure e-mail but this step is required to generate the file `C:\Windows\System32\config\systemprofile\AppData\Roaming\NewDevices.xml` on the server that hosts the Afaria access control filter.
6. Wait for the polling period defined on the *Server* > *Configuration* > *Component* > *Access Control Option* page.
7. Install the Afaria application on the device.
8. 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*.
9. Connect to Afaria.
10. Go to the Afaria Administrator Web Console and navigate to *Server* > *Configuration* > *Component* > *Access Control Option* page. 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.

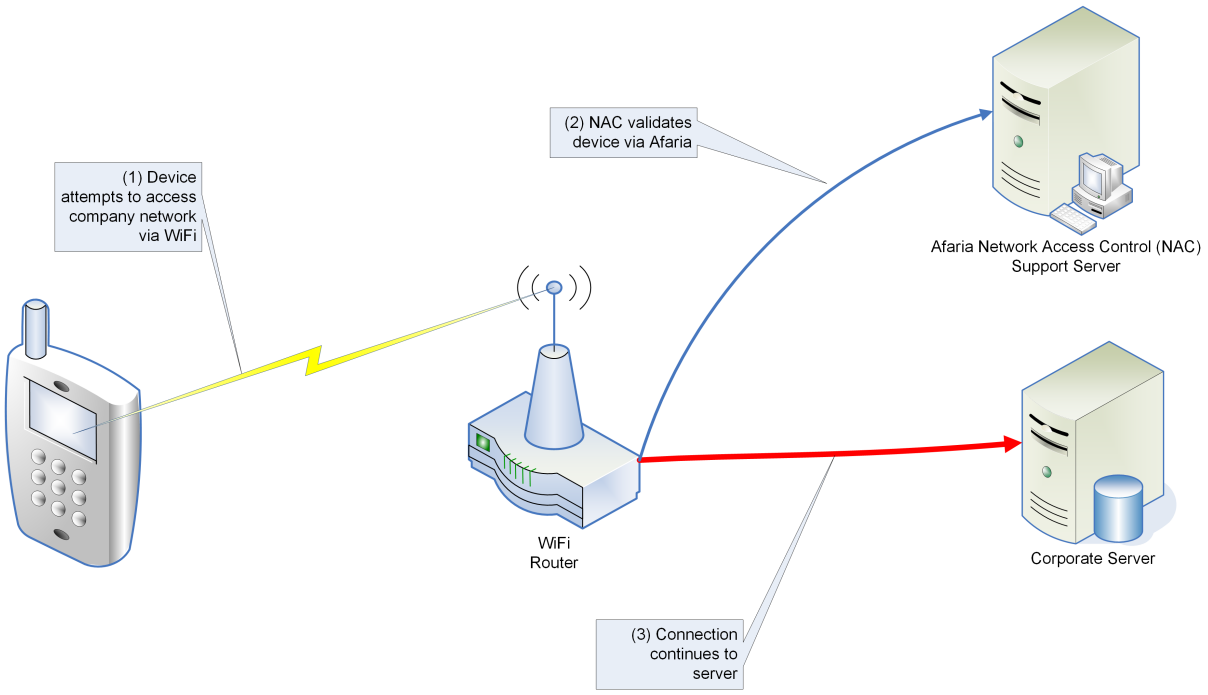
7.7 Support for Network Access Control

A Network Access Control (NAC) device can interface with the Afaria Network Access Control web service to manage the access of Android and iOS devices to corporate WiFi networks by ensuring the devices are under

Afaria control before WiFi access is granted. This ensures that devices are kept in compliance with Afaria MDM control, enforcing inventory collection and security policies on the device before permitting access to enterprise networks.

The process flow for a Network Access Control environment that uses Afaria NAC service to manage a device's connection to corporate WiFi is described below:

1. User's device attempts to access company network via WiFi.
2. The NAC WiFi router queries the NAC web service via RESTful APIs to validate if the device is known and secure..
3. The NAC WiFi router allows the connection if the device is under Afaria MDM control. If the device is not under Afaria control, the NAC WiFi router could redirect the device user to a URL with a customizable web page that indicates the device is not recognized by Afaria, and to contact the Afaria administrator to learn how to enroll in device management.
   The unmanaged device web page can be customized by editing the default html file located in the NAC installation folder: `C:\Program Files (x86)\AfariaNetworkAccessControlService\Unmanaged\UnmanagedDevicePage.htm`.
   Alternatively, you can change the redirect URL in the Network Access Control configuration page in the Afaria Administrator.



The NAC router makes a request to Afaria NAC service on the Afaria Administrator server. The request is processed by the Afaria NAC service. The Afaria NAC service then sends the appropriate response to the NAC router making the request.

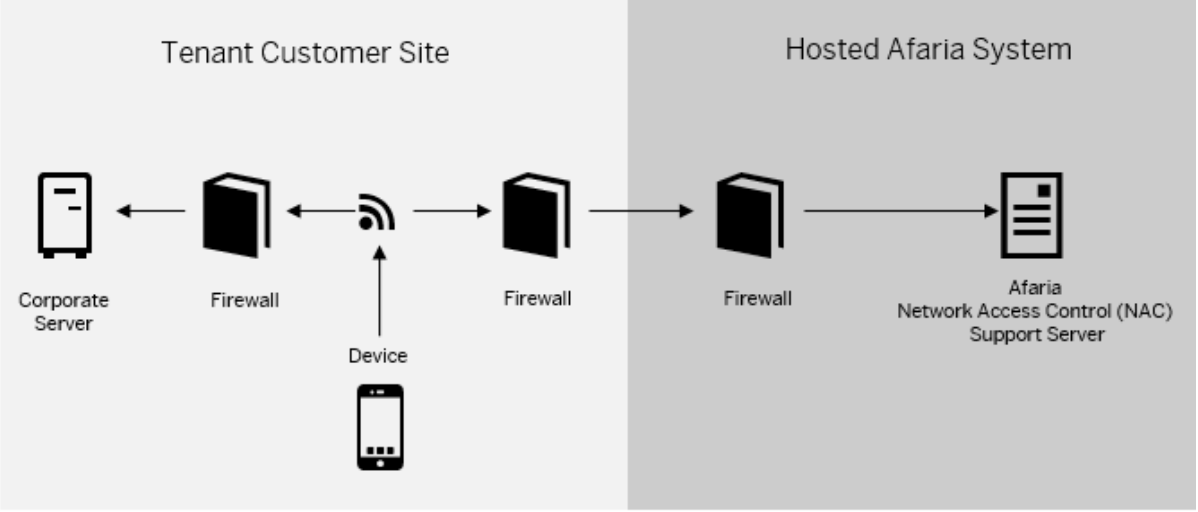
If Afaria server is hosted, and a device is trying to connect to a corporate server at a tenant customer site, the NAC router at the tenant site first authenticates the device and then contacts the Afaria NAC service at the hosting site. After Afaria responds to the NAC server request, the NAC server can then allow the compliant device to access the corporate server at the tenant customer site.

NAC is hosted in IIS as a web service under two virtual directories: `/NetworkAccessControl` and `/CiscoISE`. Either virtual directory can be used to access the NAC service, with the following difference between the two:

/NetworkAccessControl virtual directory Includes device software inventory as part of the response to a "get device info" request.

/CiscoISE virtual directory Does not return any device software inventory in any response.

The NAC web service is only accessible via HTTPS port 443 through IIS; any requests to this service over unsecured HTTP port 80 will be denied.



7.7.1 SSL Certificate Configuration for NAC

Configure an SSL certificate in IIS to use NAC over https port 443.

Consider the following two scenarios:

- Scenario# 1: Enrollment Server is already configured to use https over port 443. In this case, it is not necessary to create and bind an SSL certificate in IIS as it has already been done for Enrollment Server.
- Scenario# 2: There is no existing SSL certificate installed in IIS on port 443. In this case, create and bind an SSL certificate for https to work over port 443.

7.7.1.1 Creating a Self-Signed Certificate

If you do not have an SSL certificate from a top-level domain SSL certificate provider, you can optionally create a self-signed certificate for use on the server where NAC is installed. However, it is recommended that you use a full SSL certificate from a top-level provider rather than a self-signed certificate. If you are using a regular SSL certificate, skip these steps; otherwise, use these steps for the self-signed certificate creation:

Procedure

1. Launch Server Manager on your server.
2. Under Server Manager, go to *Roles* > *Web Server (IIS)* > *Internet Information Services (IIS) Manager*
3. Select your server under connections.
4. Click *Server Certificates* in IIS.
5. In Actions, click *Create Self-Signed Certificate*.
6. Specify a name for the certificate in 'Create Self-Signed Certificate' window and then click *Ok*.

7.7.1.2 Binding Self-Signed Certificate with https Port 443

Bind the self-signed certificate with https port 443.

Procedure

1. Launch Server Manager on your server.
2. Under Server Manager, go to *Roles* > *Web Server (IIS)* > *Internet Information Services (IIS) Manager*.
3. Select your server under connections. Expand it.
4. Expand Sites inside the server.
5. Select 'Default Web Site'.
6. In Actions, click *Bindings*.
7. Click *Add* on the Site Bindings window.
8. Select type as https, IP Address as the address of your server, SSL certificate as the one you just created and port as 443.
9. Click *Ok*.
   The self-signed certificate is now successfully bound to https port 443.

7.7.2 Adding an Account Name on Afaria NAC Server

Each web service request made to the Afaria NAC web service must include a valid username and password to authenticate each web service request (IIS-managed authentication).

Context

The account name used to authenticate the request to IIS must be a local Windows machine account that exists on the server hosting NAC. The NAC service does not use Afaria device directory security configuration;

it only uses the local Windows machine account for authentication regardless of the Afaria directory security configuration settings.

Add the local machine account name to the Network Access Control configuration screen in the Afaria Administrator for the tenant whose devices will be managed by NAC. A separate account name can be configured for each Afaria Tenant. When a NAC request is made to the Afaria NAC web service, the account used to authorize the request will be matched with the tenant for which the account name was configured, and only the devices in that tenant will be used to satisfy the request. If the account name presented in the NAC web service request is not configured for any tenant in Afaria, then the NAC service will return 401-unauthorized, even if the password was correct.

Procedure

1. On the Home page Server tab, click *Configuration*.
2. Navigate to the *Server* > *Network Access Control* page.
3. Click *Add*.
4. Enter an account name for a Windows account on the server that is authorized to access the Afaria NAC services, and optionally add a note. The format for the account name can be either `username` or `Domain\username`.
5. Click *Save*.

7.7.3 Testing the Afaria NAC Service

After you have installed NAC and added an account name to the NAC service using the Afaria Administration console, confirm the operation of the Afaria NAC service by manually performing the procedure given below.

Context

The Afaria NAC web service can be tested manually, after the following configuration steps have been completed:

1. The NAC service has been installed.
2. IIS has been configured for traffic on port 443 with an SSL certificate.
3. A local machine account has been created for use with the NAC service, and this account has been configured for the desired tenant in the Afaria Admin's NAC configuration screen.

After the above steps have been completed, the Afaria NAC web service can be tested by invoking a basic informational web service command as follows:

Procedure

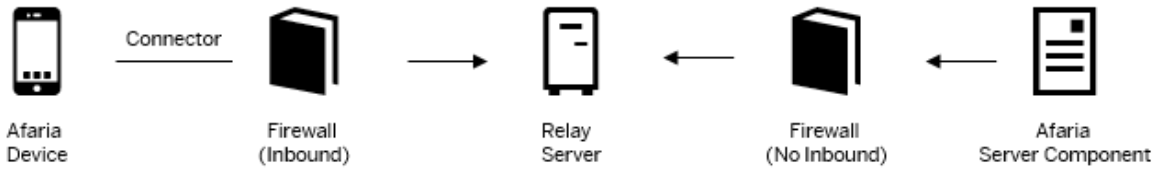
1. Open a Web browser and enter the URL `https://<server>/networkaccesscontrol/mdminfo` (replace `<server>` with the address for your Afaria NAC web server).
2. When prompted, enter the local machine account username and password.
3. If the NAC service is configured properly, you should then receive an XML response which includes a handful of attributes including name, version, etc.
4. If you receive a 401-unauthorized error, then check the password for the account that was used as well as ensure the account was added properly to the NAC configuration screen in the Afaria Administrator. In addition, check that the Basic Authentication module is installed and enabled in IIS for the `/networkaccesscontrol` virtual directory.
5. If you attempt to browse to the NAC service without https, you will receive an error. The NAC service will only respond to https requests.

7.8 Relay Server 16 (Deprecated)

SAP Afaria supports using a relay server to operate as a proxy for HTTP and HTTPS sessions between SAP Afaria server components and devices.

> **i Note**
>
> Relay Server 16 is no longer supported, but may still be used in your environment as a bridge until clients have been reconfigured to connect via a supported version.
>
> Use of a relay server is not a requirement; it is bundled with the Afaria product on the product installation image as an optional component.

A relay server lets you further secure your enterprise network by moving the session connection point from within your firewall to your demilitarized zone (DMZ).



When you use a relay server, devices and Afaria server components never make a direct connection. The relay server transfers session traffic from devices to the component, and from the component to the devices. The Afaria server component initiates an outbound connection through the enterprise firewall to the relay server,

then waits for the relay server to send session traffic. Devices can initiate a connection to the relay server—as if it were an Afaria server component—and maintain their session with the relay server, which continues to relay traffic until the session is complete.

The relay server component may be a single server or it may be a load-balanced server farm.

Afaria supports using the relay server with any of these Afaria server components:

- Afaria server
- Enrollment server
- iOS certificate authority
- Afaria filter used in Access Control for Email
- Package server
- Application Onboarding certificate authority

An Afaria server component may be a single server or a farm. You can configure relay servers to support more than one Afaria server component.

Related Information

Configuring Relay Server for Package Server [page 88]
Configuring Relay Server for Access Control [page 60]
Configuring Relay Server for Certificate Authority [page 86]

7.8.1 Relay Server Executable Components

Relay server operations include two main executable components: the relay server host and the relay server outbound enabler.

Relay server host (rshost.exe) The host resides on the relay server, and is responsible for, accepting a single, inbound connection from the outbound enabler; accepting multiple, inbound connections from Afaria devices; handling the associated processes that occur on the relay server for Afaria sessions. Install the relay server using files available on the Afaria product image. Define its configuration settings by modifying a sample configuration file.

Relay server outbound enabler (rsoe.exe) The outbound enabler is the relay agent on the Afaria server component, and is responsible for initiating an outbound connection with the relay server. The Afaria setup program automatically installs the outbound enabler on the Afaria server. To support components other than the Afaria server, copy the binary for the `rsoe.exe` on the components. Define the relay server outbound enabler configuration settings using the Afaria Administration console.

Afaria devices include configuration settings for using a relay server but do not require a separate, executable component.

7.8.2 Setting Up the Relay Server for Basic Operations

To use the relay server to increase your enterprise network security, you must set up the relay server for basic operations before you configure it to support any server components.

7.8.2.1 Setting Up the Relay Server for Basic Operations with IIS 7.5

For planned relay servers running Windows Server 2008 R2 (x64) with Internet Information Services (IIS) 7.5, set up the relay server for basic operations before you configure it to support any server components.

1. Copying Relay Server Files [page 71]
   Copy the relay server files from the Afaria product image to the machine where the relay server will be installed.
2. Configuring IIS 7.5 for Relay Server Basic Operations [page 72]
   To setup the relay server for basic operations, configuring IIS on your relay server.
3. Editing the Relay Server Configuration File [page 76]
   Edit the relay server configuration file to configure the relay server's basic operations.
4. Installing the Relay Server Host as a Windows Service [page 78]
   Install the relay server host as a Windows service by running a service utility available in the relay server installation folder.

7.8.2.1.1 Copying Relay Server Files

Copy the relay server files from the Afaria product image to the machine where the relay server will be installed.

Procedure

1. On the machine where you plan to install the relay server, create a new folder named `RelayServer`. Its path will become your relay server installation path, for example, `C:\Program Files\RelayServer`.
2. On the Afaria product image, navigate to:
   `<product image>\relay_server16\64 Bit\ias_relay_server`.
3. Copy the folder `ias_relay_server` from the product image to your relay server installation path. Ensure that you copy the folder, rather than just the files in the folder.

Task overview: Setting Up the Relay Server for Basic Operations with IIS 7.5 [page 71]

Next task: Configuring IIS 7.5 for Relay Server Basic Operations [page 72]

7.8.2.1.2 Configuring IIS 7.5 for Relay Server Basic Operations

To setup the relay server for basic operations, configuring IIS on your relay server.

Prerequisites

From the server manager utility of your relay server, verify that these roles and features are installed:

- IIS
- Web Server Service
- Common HTTP Features
- Static Content
- Default Document
- Directory Browsing
- HTTP Errors
- ISAPI Extensions
- HTTP Logging
- Request Monitor
- Request Filtering
- Static Content Compression
- IIS Management Console
- IIS Management Scripts and Tool
- IIS 6 Management Compatibility
- IIS 6 Metabase Compatibility
- IIS 6 WMI Compatibility
- IIS 6 Scripting Tools
- IIS 6 Management Console

Install any missing items.

Context

Complete the following tasks to configure IIS 7.5 for relay server basic operations:

Task overview: Setting Up the Relay Server for Basic Operations with IIS 7.5 [page 71]

Previous task: Copying Relay Server Files [page 71]

Next task: Editing the Relay Server Configuration File [page 76]

Related Information

Editing the Relay Server Configuration File [page 76]

7.8.2.1.2.1 Creating a Relay Server Application Pool on IIS 7.5

Use your relay server's IIS manager utility to create an IIS application pool for relay server operations.

Procedure

1. Navigate to *Start* > *Control Panel* > *System and Security* > *Administrative Tools* and double-click *Internet Information (IIS) Manager.*
2. From the Connections pane of the IIS manager utility, navigate to `<MachineName>` > *Application Pools.*
3. Right-click *Application Pools* and select *Add Application Pool.*
4. Add an application pool with these attributes:
   - Name – **`RelayServer`**
   - .NET Framework version – .NET Framework v2.0.50727
   - Managed pipeline mode – integrated
   - Start application pool immediately – selected

   The list of application pools shows the RelayServer application pool.
5. Right-click the newly created application pool and select *Advanced Settings*. Set these properties:
   - General > Queue Length – **`65535`**
   - CPU > Limit Interval (minutes) – **`0`**
   - Process Model > Identity – ApplicationPoolIdentity
   - Process Model > Idle Time-out (minutes) – **`0`**
   - Process Model > Maximum Worker Processes – **`20`**
   - Process Model > Ping Enabled – false
   - Process Model > Ping Maximum Response Time (seconds) – **`90`**
   - Process Model > Ping Period (seconds) – **`30`**
   - Rapid-Fail Protection > Enabled – false
   - Recycling > Disable Overlapped Recycle – true
   - Recycling > Regular Time Interval (minutes) – **`0`**

7.8.2.1.2.2 Creating a Web Application for the Relay Server on IIS 7.5

Use the IIS 7.5 manager utility to create a Web application for the relay server.

Context

You can create the Web application for your relay server under the root directory of either the default Web site or a custom web site. The custom Web site must use a different port than the default Web site.

Procedure

1. Navigate to *Start* > *Control Panel* > *System and Security* > *Administrative Tools* and double-click *Internet Information Services (IIS) Manager.*
2. From the Connections pane of the IIS manager utility, navigate to `<MachineName>` > *Sites.*
3. Right-click the Web site you want to use (either default or custom) and select*Add Application.*
4. Add a web application with these attributes:
   - Alias – **`ias_relay_server`**
   - Application pool – RelayServer
   - Physical path – `<relay server installation path>\ias_relay_server`

   The web application ias_relay_server will be listed under the root directory of the Web site you chose.
5. Edit the Request Filtering Settings for the ias_relay_server Web application.
   a. In the Connections pane, highlight the *ias_relay_server* application.
   b. In the IIS group, double-click *Request Filtering.*
   c. In the Actions pane, click *Edit Feature Settings* and edit these attributes:
      - Maximum allowed content length (bytes) – **`2147483647`**
      - Maximum query string (bytes) – **`65536`**
6. Edit the permissions for the ias_relay_server Web application.
   a. In the Connections pane, highlight the *ias_relay_server* application.
   b. In the IIS group, double-click *Handler Mapping.*
   c. In the Actions pane, click *Edit Feature Permissions* and ensure that only *Script* and *Execute* are selected.
7. Verify that the ias_relay_server web application does not require SSL.
   a. In the Connections pane, highlight the *ias_relay_server* application.
   b. In the IIS group, double-click *SSL Settings* and ensure that *Require SSL* is not selected.

7.8.2.1.2.3 Adding ISAPI extensions for Relay Server Operations

Use the IIS 7.5 manager utility to add two ISAPI extensions to your server to handle requests from devices and the Afaria server.

Procedure

1. Navigate to *Start* > *Control Panel* > *System and Security* > *Administrative Tools* and double-click *Internet Information (IIS) Manager.*
2. On the Connections pane of the IIS manager utility, highlight the machine name where the relay server resides.
3. In the IIS group, double-click *ISAPI and CGI Restrictions.*
4. In the Actions pane, click *Add* to add two ISAPI restrictions with these settings:
   - ISAPI or CGI Path – `<<relay server installation path>>\ias_relay_server\server\rs_server.dll`
   - Description – **`RS Server DLL`**
   - Allow extension path to execute – selected
   - ISAPI or CGI Path – `<<relay server installation path>>\ias_relay_server\client\rs_client.dll`
   - Description – **`RS Client DLL`**
   - Allow extension path to execute – selected

Results

The two ISAPI restrictions you added are listed in the ISAPI and CGI restrictions list of your server.

7.8.2.1.2.4 Updating the Relay Server IIS Configuration

Run the `adsutil.vbs` script to update the IIS server configurations.

Procedure

1. From a command prompt running with administrator privileges, navigate to the directory where the `adsutil.vbs` script is located, for example, `C:\Inetpub\AdminScripts.`
2. To run the script, issue:

```
cscript adsutil.vbs set w3svc/<<Web Site ID>>/uploadreadaheadsize 0
```

where <<Web Site ID>> is the ID of the Web site used for the relay server. If you use the default Web, the ID is 1.

Results

The command returns the current value of the <<uploadreadaheadsize>> variable and updates the IIS configurations.

7.8.2.1.3 Editing the Relay Server Configuration File

Edit the relay server configuration file to configure the relay server's basic operations.

Context

A sample configuration file is provided with the relay server files that you copied from your Afaria product image.

Procedure

1. Find the sample configuration file `rs.config`, located in <<relay server installation path>>\ias_relay_server\server.
2. Use a text editor to make appropriate changes to the [options] and [relay_server] sections in the configuration file.

   > **i** Note
   >
   > The configuration file can contain only ASCII characters.

3. Save the edits.
4. Restart the relay server host.

Task overview: Setting Up the Relay Server for Basic Operations with IIS 7.5 [page 71]

Previous task: Configuring IIS 7.5 for Relay Server Basic Operations [page 72]

Next task: Installing the Relay Server Host as a Windows Service [page 78]

Related Information

Configuring IIS 7.5 for Relay Server Basic Operations [page 72]
Installing the Relay Server Host as a Windows Service [page 78]

7.8.2.1.4 Configuration File Definitions for Basic Operations with IIS 7.5

The relay server configuration file `rs.config` consists of several sections. Use sections [options] and [relay_server] for relay server basic operations. The remaining sections are for supported server components.

[options] general options for relay server operations.

- start – set value to "auto" to automatically start the relay server engine when an Afaria server connects successfully.
  For Windows Server 2008 R2 (IIS 7.5), this value is normally set to `=NO` when the Relay Server is installed as a Windows Service.
- verbosity – controls the level of logging. Logs always include errors. Log levels 1 – 5 always include warnings.
  - 0 – no logging.
  - 1 – session-level logging.
  - 2 – request-level logging.
  - 3 – packet-level logging, terse.
  - 4 – packet-level logging, verbose.
  - 5 – transport-level logging.

[relay_server] identifies your relay server and its respective ports for HTTP and HTTPS communications. The relay server's ports must match the IIS server ports.

- enable – controls whether the relay server operates.
  - yes – operate.
  - no – do not operate.
- host – relay server IP address or host name. The IP address must be the internal IP address or DNS name that can be reached by the Afaria server or other supported server components.
- http_port – TCP port matching the relay server's IIS setting for HTTP communications. The port must be the internal TCP port that can be reached by the Afaria server or other supported server components.
- https_port – set value to match the relay server's IIS setting for SSL communications.
- description – user-defined description.

> **i Note**
>
> Values are case-sensitive.

> **Example**
>
> Sample section of a relay server configuration file showing settings for basic operations.

```
#-------------------------------------
# Relay server
#-------------------------------------
[options]
start = no
verbosity = 1
# Note: When auto start is used, the default log file is
#       <tmpdir>\ias_relay_server_host.log while rshost is active.
#       The value of <tmpdir> is filled using the following environment
variables
#       searched in this order:
#               SATMP
#               TMP
#               TMPDIR
#               TEMP
#--------------------
# Relay server
#--------------------
[relay_server]
enable          = yes
host            = 123.45.6.78
http_port       = 80
https_port      = 443
description     = Machine #1 in RS farm
```

Restart the relay server engine (`rshost.exe`) any time you make changes to the configuration file.

7.8.2.1.5 Installing the Relay Server Host as a Windows Service

Install the relay server host as a Windows service by running a service utility available in the relay server installation folder.

Prerequisites

In the [options] section of the relay server configuration file, set the value of `start` to **`=no.`**

Context

The relay server installation folder includes `dbsvc.exe`, a service utility that installs the relay server host as a Windows service. Use the same utility to uninstall the service.

Procedure

1. On the machine where you installed the relay server, execute this command at a command prompt running with administrator privileges:

```
<installation directory>\ias_relay_server\server\dbsvc.exe" -as -s auto -sn
RelayServer -w RelayServer "<installation directory>\ias_relay_server\server
\rshost.exe" -q -f "<installation directory>\ias_relay_server\server\rs.config"
-o "<installation directory>\ias_relay_server\server\log.txt".
```

For a complete list of the service utility's command line switches, execute:

```
"<installation directory>\ias_relay_server\server\dbsvc.exe".
```

- The command prompt displays a line confirming that the "RelayServer" service was successfully created.
- The RelayServer service is listed in the list of Windows services.

2. Change the login account of the newly created "RelayServer" service from Local System to an account that is a member of the local Administrator group.

Next Steps

To uninstall the "RelayServer" Windows service, execute this command at a command prompt running with administrator privileges:

```
"<installation directory>\ias_relay_server\server\dbsvc.exe" -d RelayServer.
```

Task overview: Setting Up the Relay Server for Basic Operations with IIS 7.5 [page 71]

Previous task: Editing the Relay Server Configuration File [page 76]

Related Information

Editing the Relay Server Configuration File [page 76]

7.8.3 Restarting the Relay Server Host

You can restart the relay server host to apply changes that you make to the relay server configuration file.

Context

The relay server starts automatically when configured to do so as part of its basic operations. The automatic start feature is defined when you use the `start=auto` attribute in the relay server's configuration file [options] section. IIS must be running before the automatic start feature can take effect.

Restarting the relay server does not require that you restart IIS and does not cause any disruption to other IIS applications.

Procedure

1. From a command prompt running with administrator privileges, navigate to `<<installation directory>>\ias_relay_server\server.`
2. Issue this command:

   ```
   rshost.exe -u -qc -f rs.config
   ```

   For a complete list of command line switches and their meaning, enter **`rshost`** at the command prompt and press *Enter.*

Next Steps

You may want to create a batch file for the commands and store it in a convenient location in your relay server environment.

7.8.4 Relay Server Support for Server Components

To configure the relay server to support an Afaria server component, define the relay server configuration file and configure settings on the Afaria Administration console.

Afaria supports using the relay server with any of these server components:

- Afaria server
- Enrollment server
- iOS certificate authority server
- Afaria filter used for Access Control for Email
- Package server
- Application Onboarding certificate authority

The relay server configuration file `rs.config` consists of several sections. Use [backend_farm] and [backend_server] for each supported server component.

[backend_farm] creates a single, case-sensitive identifier for a component server environment, regardless of whether you are operating a single component server or a farm of component servers.

- enable – controls whether the farm operates.
  - yes – operate.
  - no – do not operate.
- id – user-defined, case-sensitive value for identifying a server farm. Each farm in the relay server configuration file must have a unique ID.
- description – user-defined description.
- client_security – specifies the secure communication protocol requirement for clients connecting to the relay server. This is an optional section that is not represented in the sample configuration file. Omitting the section results in the relay server enforcing the default value.
  - on – HTTPS is required.

    - off – default. HTTPS is not required; HTTP and HTTPS are both valid connection protocols.
- backend_security – specifies the secure communication protocol requirement for component servers connecting to the relay server. Omitting the section results in the relay server enforcing the default value.
    - on – HTTPS is required.
    - off – default. HTTPS is not required; HTTP and HTTPS are both valid connection protocols.

[backend_server] identifies a single component server to the relay server. You must have one [backend_server] section for each component server in your component server environment.

- enable – controls whether the server operates.
    - yes – operate.
    - no – do not operate.
- farm – the case-sensitive farm value is the same for each server. Use the same farm ID as from [backend_farm].
- ID – the ID value is unique for each server in the farm. If a server hosts more than one supported server component, then all server IDs on the host must be unique. For example, if a server hosts both an Afaria server and a package server, and both are defined in separate farms in the relay server configuration file, then the server IDs used for the two server components must be must be different.
- mac – mac address of the server component.
- token – the token is any string that you create. Use the same token value for each server in a farm.

> **i** Note
>
> Values are case-sensitive.

Restart the relay server engine (`rshost.exe`) any time you make changes to the configuration file.

7.8.4.1 Relay Server Configuration File–Examples

Examples of the structure of the relay server configuration file based on the Afaria environment supported.

Single Afaria server – in an environment with a single relay server supporting a single Afaria server, the configuration file includes these sections:

- [options] – one instance.
- [relay_server] – one instance.
- [backend_farm] – one instance.
- [backend_server] – one instance.

Afaria server farm with four servers – in an environment with a single relay server supporting an Afaria server farm with four servers, the configuration file includes these sections:

- [options] – one instance.
- [relay_server] – one instance.
- [backend_farm] – one instance.
- [backend_server] – four instances.

Afaria server farm with four servers plus a package server – in an environment with a single relay server supporting an Afaria server farm with four servers and a package server, the configuration file includes these sections:

- [options] – one instance.
- [relay_server] – one instance.
- [backend_farm] – two instances.
- [backend_server] – five instances.

Example

This is a sample section of a relay server configuration file showing settings for a single Afaria server. Settings includes an instance of the [backend_farm] section and an instance of the [backend_server] section. The sample does not include the sections for the relay server basic operations.

```
#---------------
# Backend farms
#
# Notice that the case sensitive farmID must match the farmID set in the
Afaria Administrator's
# relay server configuration page.  Default value in Afaria is farmID=Afaria.
#---------------
[backend_farm]
enable          = yes
id              = farmID
description     = Afaria Farm
#-----------------
# Backend servers
#
# id must match regKey HKLM\Software\Afaria\Afaria\Server\TransmitterId
# on your afaria server
#-----------------
[backend_server]
enable   = yes
farm     = farmID
id       = sc
token    = zyyxpj22p
```

7.8.4.2 Configuring Relay Server for Afaria Server

To configure the relay server to support one or more Afaria servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

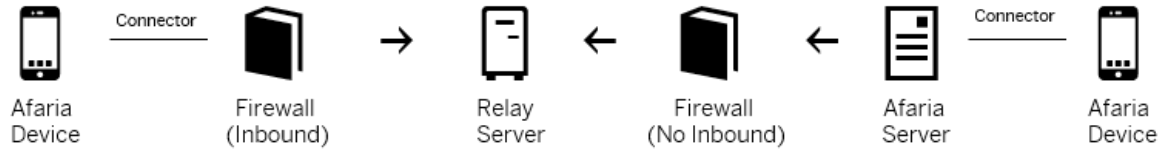
- As all relay server communications must use HTTP or HTTPS protocol, configure the Afaria server and devices to use HTTP or HTTPS.
- Set up the relay server for basic operations.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more Afaria servers. Consider these items when defining the [backend_farm] and [backend_server] sections.
   - [backend_farm]
     id – user-defined, case-sensitive value for identifying the server farm. The farm ID you define must match the farm ID you define on the Afaria Administration console *Server* > *Configuration* > *Relay Server* page. On the Relay Server page, the default value is "afaria".
   - [backend_server]
     - id – define the server ID value to match the `TransmitterID` value defined in each Afaria server's registry key `HKLM\Software\Afaria\Afaria\Server\TransmitterId`.
     - Token – the farm token you define must match the farm token you define on the Afaria Administration console *Server* > *Configuration* > *Relay Server* page.
2. On the *Server* > *Configuration* > *Relay Server* page of the Afaria Administration console, configure settings for communications between the relay server and the Afaria server component.
   - *Start the outbound enabler* – select this option to apply an automatic start-up attribute to the outbound enabler service. Afaria logging captures the outbound enabler's restart and failure events.
   - *Farm ID* and *Farm token* – a pair of case-sensitive, ASCII text strings that your relay server uses to direct incoming client communication to your Afaria Server, either a standalone server or server farm. The combination of the strings must be unique for a given Afaria instance.
     - *Farm ID* – value must match the corresponding value in your relay server's configuration file and in your device configuration settings.
     - *Farm token* – value must match the corresponding value in your relay server's configuration file.
   - *Server address and Server port* – the Afaria server IP address or "localhost" and HTTP port that the Afaria server is using for communications. In a server farm environment, you must enable HTTP on each Afaria server in the farm and use "localhost" rather than the IP address.
   - *RS address and RS port* – the relay server IP address or fully qualified domain name and port that the outbound enabler service uses to connect to the relay server.
   - *RS URL suffix* – text string used as an IIS parameter for invoking the relay server's Afaria Server Web services, as per the relay server installation instructions for creating the IIS application pool.
   - *Maximum restarts* – the maximum number of times the outbound enabler attempts to start if it stops unexpectedly.
   - *Client URL prefix*– text string used as an IIS parameter for invoking the relay server's Afaria client Web services, as per the relay server installation instructions for creating the IIS application pool. This value is also required as a configuration value on Afaria devices.
   - *Use HTTPS* – enable the outbound enabler to communicate via SSL to the relay server.
   - *Certificate path* – the path and file name on the Afaria server for the relay server's certificate file. The certificate contains the relay server's identity and public key.
3. Restart the relay server host.
4. Restart the Afaria server service.

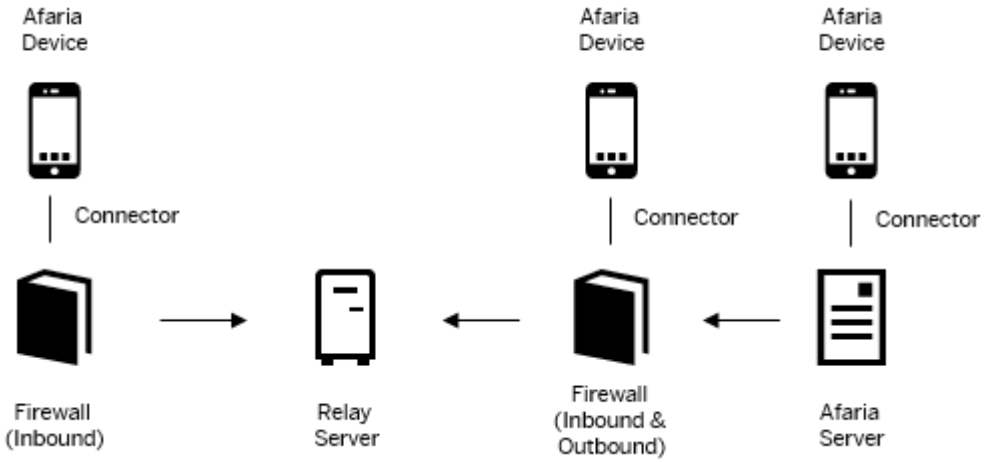
7.8.4.2.1 Relay Server Bypass

Even after your relay server is operational, the Afaria Server continues to support direct device connections. If it is appropriate for your environment, you may allow devices to continue to connect to the Afaria server directly, bypassing the relay server.



Bypass Relay Server—Sample 1

As the above diagram illustrates, if you have Afaria devices that are inside your organization's firewall and want to connect, you can allow these devices to make direct connections with the Afaria server using any of Afaria supported session protocols. These connections need not to pass through the firewall, so the firewall can support higher security.



Bypass Relay Server—Sample 2

As the above diagram illustrates, if you have devices that are outside your organization's firewall and want to connect, you can allow these devices to make direct connections with the Afaria server using any of Afaria supported session protocols as long as your firewall permits the traffic.

7.8.4.3 Configuring Relay Server for Enrollment Server

To configure the relay server to support one or more enrollment servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

- Set up the relay server for basic operations.
- Ensure that IIS is running on your enrollment servers.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more enrollment servers
   Consider this item when defining the [backend_farm] section:
   - id – user-defined, case-sensitive value for identifying the server farm.
2. Configure settings for communications between the relay server and the enrollment server component.
   a. In the Afaria Administration console, open the *Server* > *Configuration* > *Enrollment Server* page.
   b. In the Enrollment Server group, select *Use Relay Server.*
   c. In the Relay Farm ID field, enter the farm ID identifying your enrollment server farm.
   The value you enter must match the ID value you defined in the [backend_farm] section.
   d. In the relay server group, define these settings:
      - If using HTTPS, select *Use HTTPS on Relay Server connections*
      - *Server address* – address of the relay server
      - *Client URL prefix* – IIS path to `rs_client.dll`, as defined in the machine hosting the relay server.
      The default value may differ from your relay server's IIS path.
   e. Click *Save.*
3. Restart the relay server host.
4. (Optional) Restart the Afaria server service from the Afaria Administration console.
5. On your Afaria server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler` and import it to each machine where you installed an enrollment sever.
6. On each machine where you installed an enrollment server, launch the relay server outbound enabler from the command prompt.

7.8.4.4 Configuring Relay Server for Certificate Authority

To configure the Relay Server to support one or more certificate authority servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

- Set up the relay server for basic operations.
- Ensure that IIS is running on your certificate authority.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more certificate authority servers.
   Consider this item when defining the [backend_farm] section:
   - id – user-defined, case-sensitive value for identifying the server farm.
2. Configure settings for communications between the relay server and the certificate authority.
   a. In the Afaria Administration console, open the *Server* > *Configuration* > *Certificate Authority* page.
   b. Select the *Enable* check box for relay server and define these settings:
      - *Server address* – address of the relay server
      - *Farm ID* – farm ID identifying your iOS certificate authority farm.

        > **Note**
        > The value you enter must match the ID value you defined in the [backend_farm] section.

      - *Device URL prefix* – IIS path to `rs_client.dll`, as defined in the machine hosting the relay server. The default value may differ from your relay server's IIS path.
   c. Click *Save.*
3. Restart the relay server host.
4. (Optional) Restart the Afaria Server service from the Afaria Administration console.
5. On your Afaria Server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler` and import it to each machine where you installed a certificate authority server.
6. On each machine where you installed a certificate authority server, launch the relay server outbound enabler from the command prompt.

7.8.4.5 Configuring Relay Server for Access Control

To configure the relay server to support the access control filter, define the relay server configuration file, configure settings on the Afaria Administration console, and reinstall the PowerShell component of the access control filter.

Prerequisites

- Configure the relay server for basic operations.
- Configure the relay server for the SAP Afaria, regardless of whether you plan to use it for device connections.
- Install and configure the access control filter components.

Procedure

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 filter's farm ID as **Afariafarm-IS.**

2. On the *Server* > *Configuration* > *Access Control Server* page of the Afaria Administration console, select *Use Relay Server*, then click *Save*.
3. Reinstall the PowerShell component of the 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 filter.
4. Restart the machine on which you reinstalled the PowerShell component.
5. Restart the relay server host.
6. In the Afaria Administration console, restart the Afaria server service.

Related Information

Access Control [page 51]
Relay Server 16 (Deprecated) [page 69]
Server Configuration for Installation and Management [page 122]

7.8.4.6 Configuring Relay Server for Package Server

To configure the relay server to support one or more Package Servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

- Set up the relay server for basic operations.
- Ensure that IIS is running on your package servers.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more Package Servers. Consider this item when defining the [backend_farm] section:
   - id – user-defined, case-sensitive value for identifying the server farm.
2. Configure settings for communications between the relay server and the package server component.
   a. In the Afaria Administration console, open the *Server* > *Configuration* > *Package Server* page.
   b. In the Package Server (Direct Access) group, select *Use HTTPS on Package Server connections* and enter the server address for the package server.
   c. In the Package Server (Indirect Access) group, select *Use Relay Server* and enter the farm ID identifying your Package Server farm.
   The value you enter must match the id value you defined in the [backend_farm] section.
   d. In the Indirect Access (Relay Server) group, define these settings:
      - If using HTTPS, select *Use HTTPS on Relay Server connections.*
      - Server address – address of the relay server
      - Device URL prefix – IIS path to `rs_client.dll`, as defined in the machine hosting the relay server. The default value may differ from your relay server's IIS path.
   e. Click *Save.*
3. Restart the relay server host.
4. (Optional) Restart the Afaria Server service from the Afaria Administration console.
5. On your Afaria Server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler` and import it to each machine where you installed a Package Server.
6. On each machine, launch the relay server outbound enabler from the command prompt.

Related Information

Relay Server 16 (Deprecated) [page 69]

7.8.5 Launching the Relay Server Outbound Enabler

Launch the relay server outbound enabler (RSOE) from the command prompt of the server component.

Prerequisites

1. On your Afaria Server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler`.
2. Import the folder to the machine hosting the server component.

Context

- The RSOE is the relay server's agent on a server component, such as the package server and the enrollment server. It initiates an outbound connection with the relay server.
- The executable file for the RSOE is `rsoe.exe`.
- SAP recommends matching the versions of the RSOE and the relay server.

Procedure

1. From the command prompt of the machine hosting the server component, navigate to the `RSOutboundEnabler` directory that you copied from the Afaria Server.
2. To launch the RSOE, use the command line:
   `rsoe -cr <param> -f <farm> -id <id> [options]`
   - -cr – parameters for the relay server connection.
   - -f – server component farm ID, as defined in the relay server configuration file.
   - -id – unique ID identifying the server component, as defined in the relay server configuration file.

   For a complete list of command line switches and their meanings, enter **`rsoe`** at the command prompt and press *Enter*.

   If you include the security token when you define the [backend_server] section in the relay server configuration file, you must use the -t switch when launching the RSOE.

   When using the -cs switch, do not use "localhost" for the server address and do not use spaces in the name.

> ✤ Example
>
> This is a sample command line to launch the RSOE on a machine hosting the iOS certificate authority:
>
> **`rsoe.exe -cr "host=www.rs.com;port=80" -cs "host= <<IP Address>>;port=80" -f CAFarmName -id CAID -t CAToken`**

Next Steps

(Optional) Install the RSOE as a Windows service.

7.8.5.1 Installing the Relay Server Outbound Enabler as a Windows Service

Install the relay server outbound enabler (RSOE) as a Windows service by running the `dbsvc.exe` service utility at the command prompt.

Prerequisites

1. On your Afaria server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler.`
2. Import the folder to the machine hosting the server component.

Context

- Each instance of the RSOE can be installed as a Windows service.
- The RSOutboundEnabler folder includes `dbsvc.exe`, a service utility that installs the RSOE as a Windows service.

Procedure

On the machine hosting the server component, execute this command at a command prompt running with administrator privileges:

```
dbsvc.exe -as -s auto -sn "AfariaRSOE" -w AfariaRSOE "<<full path>>
\RSOutboundEnabler\rsoe.exe" @"<<full path>>\RSOutboundEnabler\rsoe.config"
```

For a complete list of the service utility's command line switches, enter **`dbsvc.exe`** at the command prompt and press *Enter.*

Results

- The command prompt displays a line confirming that the "AfariaRSOE" service was successfully created.

- The "AfariaRSOE" service is listed in the list of Windows services of the machine hosting the server component.

7.8.6 Relay Server with SSL

To configure the relay server to use SSL, you must install a trusted certificate on the server that is running the relay server's Microsoft Internet Information Services (IIS) Server and the relay server engine, `rshost.exe`.

You can configure Afaria devices to connect securely using the relay server address and HTTPS protocol after you have installed the certificate. Connecting to the relay server with SSL ensures that the traffic from devices to the relay server is encrypted. If your Afaria Server and relay server are behind the same firewall, this configuration is all you need to secure your data.

Encrypting traffic between the relay server and the Afaria Server requires that you export the relay server's public key and copy the resulting file to the Afaria Server, then use the Afaria Administration console relay server page to enable HTTPS and specify the location of the public key file. All traffic is encrypted after you restart the Afaria Server.

7.8.7 Relay-Server-Related Logging

Relay-server-related logging allows you to retrieve connections and restart attempts occurred both on the Afaria Server and the relay server.

Context

- Afaria-side logging – captures the outbound enabler restart attempt events; it does not capture relay server start events when started by the Afaria service, as occurs when the "Start the outbound enabler" setting is selected.
- Relay-server-side logging – relay server logging captures events while `rshost.exe` is active. When started using the relay server's configuration file setting for auto start, the log is stored in the following relay server path:`<<tmpdir>>\ias_relay_server_host.log`. The value of <`<tmpdir>`> is populated with the first-available environmental variable, according to the search order SATMP, TMP, TMPDIR, TEMP.

The relay server log captures connections from the Afaria Server to the relay server and successful device connections. The log does not capture unsuccessful client connections.

Procedure

1. To retrieve logging from the relay server to the Afaria server, unselect *Start the outbound enabler* to prevent the outbound enabler from starting during the next restart.
2. Restart the Afaria Server service.

3. On the Afaria Server, open a command prompt and navigate to `<<Afaria Server Installation Directory>>\bin\RSOutboundEnabler`.
4. Restart the outbound enabler using this single, continuous command:
   `rsoe.exe -id <<AfariaServerID>> -f <<FarmID>> -t <<Farm token>> -cs "host=localhost;port=<<AfariaHTTPPort>>;" -cr "host=<<RelayServerIP>>;port=<<RelayServerHTTPPort>>;url_suffix=<<RsURLSuffix>>;url_prefix=<<ClientURLPrefix>>" -v <<LogVerbosity>> -o <<LogOutputPathFile>>`
   - `<<AfariaServerID>>` – the Afaria server ID value. The ID value is defined in the Afaria Server registry key HKLM\Software\Afaria\Afaria\Server\TransmitterId.
   - `<<FarmID>>` – farm ID, as stored on the Relay Server configuration page.
   - `<<Farm token>>` – farm token, as stored on the Relay Server configuration page.
   - `<<AfariaHTTPPort>>` – Afaria HTTP port, as stored on the Client Communications configuration page.
   - `<<RelayServerIP>>` – relay server IP address.
   - `<<RelayServerHTTPPort>>` – relay server HTTP port.
   - `<<RsURLSuffix>>` – RS URL suffix, as stored on the Relay Server configuration page.
   - `<<ClientURLPrefix>>` – client URL Prefix, as stored on the Relay Server configuration page.
   - `<<LogVerbosity>>` – controls the level of logging. Logs always include errors. Logs always include warning for levels 1-5.
     - 0 – no logging.
     - 1 – session-level logging.
     - 2 – request-level logging.
     - 3 – packet-level logging, terse.
     - 4 – packet-level logging, verbose.
     - 5 – transport-level logging.
   - `<<LogOutputPathFile>>` – Afaria Server path and file name for the log file.

   For a complete list of command line switches and their meanings, enter **`rsoe`** at the command prompt and press *Enter*.

Example

This sample writes the log file to `c:\outbound.log` on the Afaria Server.

```
rsoe.exe -id got -f AfariaFarm -t Token_00 -cs "host=localhost;port=80;" -cr
"host=10.14.229.21;port=80;url_suffix=/ias_relay_server/server/
rs_server.dll;url_prefix=/ias_relay_server/client/rs_client.dll" -v 5 -o c:
\outbound.log -af
```

7.9 Relay Server 17

SAP Afaria supports using a relay server to operate as a proxy for HTTP and HTTPS sessions between SAP Afaria server components and devices.

> **i** Note
>
> Use of a relay server is not a requirement; it is bundled with the Afaria product on the product installation image as an optional component.

A relay server lets you further secure your enterprise network by moving the session connection point from within your firewall to your demilitarized zone (DMZ).

When you use a relay server, devices and Afaria server components never make a direct connection. The relay server transfers session traffic from devices to the component, and from the component to the devices. The Afaria server component initiates an outbound connection through the enterprise firewall to the relay server, then waits for the relay server to send session traffic. Devices can initiate a connection to the relay server—as if it were an Afaria server component—and maintain their session with the relay server, which continues to relay traffic until the session is complete.

The relay server component may be a single server or it may be a load-balanced server farm.

Afaria supports using the relay server with any of these Afaria server components:

- Afaria server
- Enrollment server
- iOS certificate authority
- Afaria filter used in Access Control for Email
- Package server
- Application Onboarding certificate authority

An Afaria server component may be a single server or a farm. You can configure relay servers to support more than one Afaria server component.

7.9.1 Relay Server Components

Relay server operations include two main components: the relay server and the relay server outbound enabler.

Relay server host IIS The relay server web application resides on the web server facing the internet, and is responsible for, accepting a single, inbound connection from the outbound enabler; accepting multiple,

inbound connections from Afaria devices; handling the associated processes that occur on the relay server for Afaria sessions. Install the relay server using files available on the Afaria product image. Define its configuration settings by modifying a sample configuration file.

Relay server outbound enabler (rsoe2.exe) The outbound enabler is the relay agent on the Afaria server component, and is responsible for initiating an outbound connection with the relay server. The Afaria setup program automatically installs the outbound enabler on the Afaria server. To support components other than the Afaria server, copy the binary for the `rsoe2.exe` on the components. Define the relay server outbound enabler configuration settings using the Afaria Administration console.

Afaria devices include configuration settings for using a relay server but do not require a separate, executable component.

7.9.2 Setting Up the Relay Server for Basic Operations

To use the relay server to increase your enterprise network security, you must set up the relay server for basic operations before you configure it to support any server components.

7.9.2.1 Setting Up the Relay Server for Basic Operations with IIS 7.5

For planned relay servers running Windows Server 2008 R2 (x64) with Internet Information Services (IIS) 7.5, set up the relay server for basic operations before you configure it to support any server components.

7.9.2.1.1 Copying Relay Server Files

Copy the relay server files from the Afaria product image to the machine where the relay server will be installed.

Procedure

1. On the machine where you plan to install the relay server, create a new folder named `RelayServer`. Its path will become your relay server installation path, for example, `C:\Program Files\RelayServer17`.
2. On the Afaria product image, navigate to: `<product image>\relay_server\Windows\IIS`.
3. Copy the folder `IIS` from the product image to your relay server installation path. Ensure that you copy the folder, rather than just the files in the folder. After copying the folder, rename the copied IIS folder to `ias_relay_server`.

7.9.2.1.2 Configuring IIS 7.5 for Relay Server Basic Operations

To setup the relay server for basic operations, configuring IIS on your relay server.

Prerequisites

None.

Context

The file `<relay server installation path>\ias_relay_server\iis7_plus_setup_Afaria.bat` quick setup script performs the following tasks:

1. Installs the supported version of IIS that is available and turns on the required features.
2. Configures the installed IIS for the Relay Server.

Web Server administrators can customize the script as necessary. The default virtual directory name is `rs17` and the default application pool is named `RS17AppPool`.

Complete the following tasks to configure IIS 7.5 for relay server basic operations:

Procedure

1. As an administrator, open a command prompt.
2. Change directory to `<relay server installation path>\ias_relay_server`.
3. To configure IIS, run `iis7_plus_setup_Afaria.bat`.
4. Run `iisreset`.

7.9.2.1.3 Editing the Relay Server Configuration File

Edit the relay server configuration file to configure the relay server's basic operations.

Context

A sample configuration file is provided with the relay server files that you copied from your Afaria product image.

Procedure

1. Find the sample configuration file `rs.config`, located in `<<relay server installation path>>\ias_relay_server.` and copy or rename it to `rs.config`.
2. Use a text editor to make appropriate changes to the [options] and [relay_server] sections in the configuration file.

   > **Note**
   >
   > The configuration file can contain only ASCII characters.

3. Save the edits.
4. Restart the relay server.

7.9.2.1.3.1 Sample rs.config File

Modifying the relay server configuration file, `rs.config`, allows you to configure the relay server's basic operations.

The following information is provided as a sample only. You will need to ensure your `rs.config` file is modified appropriately to meet your needs. See Relay Server Support for Server Components [page 108] for details on relay server configuration options.

Sample Code

```
####
# Sample rs.config
####
[options]
description = Email <a href="mailto:changeit@changeit.com">RS
administrator</a> in case of relay issues
shared_mem = 50M
verbosity = 1
status_refresh_sec = 0

[relay_server]
enable = yes
host = 10.180.10.199
http_port = 80
https_port = 443


[backend_farm]
enable = yes
id = RSFarm1-AS
description = RSFarm1 Afaria Server
[backend_farm]
enable = yes
id = RSFarm1-ES
description = RSFarm1-Enrollment Server
[backend_farm]
enable = yes
id = RSFarm1-PS
description = RSFarm1-Package Server
[backend_server]
description = Afaria Master Server
```

```
enable = yes
farm = RSFarm1-AS
#id = <Insert the Afaria Server TransmitterID found in the registry at HKLM
\Software\Afaria\Afaria\Server>
id = eqbu
token = {619e8692-9a46-41f9-8447-d69ded0993a4}
[backend_server]
description = Afaria Slave Server
enable = yes
farm = RSFarm1-AS
#id = <Insert the Afaria Server TransmitterID found in the registry at HKLM
\Software\Afaria\Afaria\Server>
id = x3n
token = {8e9789be-0e51-4e42-b086-7aaa9f2c06d1}
[backend_server]
description = Afaria Enrollment Server
enable = yes
farm = RSFarm1-ES
id = enrollment-id
token = {8e9b00b1-50a7-478d-927b-a341fcb8f432}
[backend_server]
description = Afaria Package Server 1
enable = yes
farm = RSFarm1-PS
id = package1-id
token = {69c223f2-a026-4b1b-bb76-25890acf5f82}
[backend_server]
description = Afaria Package Server 2
enable = yes
farm = RSFarm1-PS
id = package2-id
token = {b1cf243b-4078-4b6f-99e8-e8c7816a0dbf}
```

7.9.2.1.4 Configuration File Definitions for Basic Operations with IIS 7.5

The relay server configuration file `rs.config` consists of several sections. Use sections [options] and [relay_server] for relay server basic operations. The remaining sections are for supported server components.

[options] general options for relay server operations.

- verbosity – controls the level of logging. Logs always include errors. Log levels 1 – 5 always include warnings.
  - 0 – no logging.
  - 1 – session-level logging.
  - 2 – request-level logging.
  - 3 – packet-level logging, terse.
  - 4 – packet-level logging, verbose.
  - 5 – transport-level logging.

[relay_server] identifies your relay server and its respective ports for HTTP and HTTPS communications. The relay server's ports must match the IIS server ports.

- enable – controls whether the relay server operates.
  - yes – operate.
  - no – do not operate.

- host – relay server IP address or host name. The IP address must be the internal IP address or DNS name that can be reached by the Afaria server or other supported server components.
- http_port – TCP port matching the relay server's IIS setting for HTTP communications. The port must be the internal TCP port that can be reached by the Afaria server or other supported server components.
- https_port – set value to match the relay server's IIS setting for SSL communications.
- description – user-defined description.

> **Note**
>
> Values are case-sensitive.

> **Example**
>
> Sample section of a relay server configuration file showing settings for basic operations.

```
Sample section of a relay server configuration file showing settings for
basic operations.

#-------------------------------------
# Relay server
#-------------------------------------
[options]
verbosity = 1
description = Email <a href="mailto:changeit@changeit.com">RS
administrator</a> in case of relay issues
#--------------------
# Relay server
#--------------------
[relay_server]
enable = yes
host = 123.45.6.78
http_port = 80
https_port = 443
description = Machine #1 in RS farm
```

(Optional) Restart the relay server any time you make changes to the configuration file.

7.9.2.2 Relay Server Outbound Enabler Command (RSOE2) Reference

The rsoe2 command opens outbound connections from the Relay Server Outbound Enabler (RSOE) to the Relay Server.

```
rsoe2 [ <option> ]+
```

```
rsoe2 @{ <filename> | <environment-variable> } ...
```

Parameters

Options

Options that have defaults are optional. At a minimum, the Outbound Enabler needs to supply the connection string for the Relay Server (-cr), the farm (-f), and server (-id) names. If a security token is configured, then it must also be specified (-t).

rsoe2 options	Description
@<data>	Reads options from the specified environment variable or configuration file. To protect information in the configuration file, use the File Hiding utility (dbfhide) to encode the contents of the configuration file.

rsoe2 options	Description
-cr <"connection-string">	Specifies the Relay Server connection string. The format of the Relay Server connection string is a semicolon-separated list of keyword=value pairs. **host** The IP address or hostname of the Relay Server. The default is localhost. **port** Required. The port that the Relay Server is listening on. **http_userid** Optional. The user ID for authentication. Consult your web server (or proxy) documentation to determine how to set up HTTP authentication. **http_password** Optional. The password for authentication. Consult your web server (or proxy) documentation to determine how to set up HTTP authentication. **http_proxy_userid** Optional. The user ID for proxy authentication. Consult your web server (or proxy) documentation to determine how to set up HTTP authentication. **http_proxy_password** Optional. The password for proxy authentication. Consult your web server (or proxy) documentation to determine how to set up HTTP authentication. **proxy_host** Optional. The host name or IP address of the proxy server. > **i** Note > If you experience issues with proxy servers that are taking too long to buffer, then use HTTPS, which prevents proxy buffering. **proxy_port** Optional. The port number of the proxy server. **url_suffix** Required. The URL path to the server extension of the Relay Server. **https** 0 - HTTP (default) 1 - HTTPS

rsoe2 options	Description
	For *https=1*, the following options can also be specified. Specify at least one of certificate_name, certificate_company, or certificate_unit to ensure that the Outbound Enabler is connecting to the correct Relay Server. To prevent checking the certificate, specify the certificate_name_check option. **certificate_name** The common name field of the certificate. **certificate_company** The organization name field of the certificate. **certificate_unit** The organization unit field of the certificate. **identity** This option provides the credentials to establish mutually authenticated TLS between the Outbound Enabler and the Relay Server. Mutual authentication is required for the Relay Server. **identity_password** This option provides the credentials to establish mutually authenticated TLS between the Outbound Enabler and the Relay Server. Mutual authentication is required for the Relay Server. **fips** Choose whether to use FIPS-certified encryption implementations for TLS encryption and end-to-end encryption. **skip_certificate_name_check** Controls whether the client library skips the check of the server host name against the database server certificate host names. Set this boolean option to ON or OFF to control whether the host name of the Relay Server matches any of the host names in the root certificate. Enabling this option may prevent the client from fully authenticating the server, leaving it vulnerable to attack. When initiating TLS or HTTPS connections, the client libraries check the host name of the Relay Server against the certificate provided by that server using the procedure described in RFC 2818. This check only happens if none of the certificate_name, certificate_company, or certificate_unit options are specified, or if the skip_certificate_name_check option is not ena-

rsoe2 options	Description
	bled. If any of certificate_name, certificate_company, or certificate_unit are specified, then only those options are verified. The skip_certificate_name_check option disables the host name check when enabled. The host names or IP addresses are derived from the subjectAltName (Subject Alternative Name or SAN) extension and the Common Name (CN) field. The SAN may contain multiple host names with wild cards. For example, a Google certificate might include *.google.com, *.google.ca, and *.android.com. Thus, www.google.ca is a valid host name. **trusted_certificates** This parameter takes the name of a file that contains a list of PEM-encoded X.509 trusted root certificates. To verify the Relay Server, and only the Relay Server, set this property to *backend_server_public_cert_filename*. `trusted_certificates=backend_server_public_cert_filename` On Microsoft Windows, if *trusted_certificates* is not set, then the operating system certificate store is used.

rsoe2 options	Description
`-cs <"connection-string">`	Specifies the backend server connection string. The format of the connection string is a semicolon-separated list of name-value pairs. **host** The IP address or hostname of the backend server. The default is localhost. **port** Required. The port the backend server is listening on. The default is 0. **https** 0 - HTTP (default) 1 - HTTPS By default, MobiLink starts the TCP/IP communication protocol. When starting MobiLink for use with the RSOE, start the communication protocol that your RSOE configuration requires. For example, if you specify HTTPS as the backend security, then MobiLink must be started with HTTPS. When the https=1 parameter is included in the -cs option, the default port changes to 443. For *https=1*, you can specify the following options. Specify at least one of certificate_name, certificate_company, or certificate_unit to ensure that the Outbound Enabler is connecting to the correct backend server. To prevent checking the certificate, specify the skip_certificate_name_check option. **identity** The path and file name of the identity file that is to be used for server authentication. Provides the credentials to establish mutually authenticated TLS between the Outbound Enabler and the backend server. Mutual authentication is required for the backend server. **identity_password** An optional parameter that specifies a password for the identity file. When this option is specified, the identity option must also be specified. Provides the credentials to establish mutually authenticated TLS between the Outbound Enabler and the backend server. Mutual authentication is required for the backend server. **skip_certificate_name_check**

rsoe2 options	Description
	Controls whether the client library skips the check of the server host name against the database server certificate host names. Set this boolean option to ON or OFF to control whether the host name of the backend server matches any of the host names in the root certificate. Enabling this option may prevent the client from fully authenticating the server, leaving it vulnerable to attack. When initiating TLS or HTTPS connections, the client libraries will check the host name of the backend server against the certificate provided by that server using the procedure described in RFC 2818. This check only happens if none of the certificate_name, certificate_company, or certificate_unit options are specified, or if the skip_certificate_name_check option is not enabled. If any of certificate_name, certificate_company, or certificate_unit are specified, then only those options are verified. The skip_certificate_name_check option disables the host name check when enabled. The host names or IP addresses are derived from the subjectAltName (Subject Alternative Name or SAN) extension and the Common Name (CN) field. The SAN may contain multiple host names with wild cards. For example, a Google certificate might include *.google.com, *.google.ca, and *.android.com. Thus, www.google.ca is a valid host name. **trusted_certificates** This parameter takes the name of a file that contains a list of PEM-encoded X.509 trusted root certificates. To verify the backend server, and only the backend server, set this property to `<backend-server-public-cert-filename>`: `trusted_certificates=<backend-server-public-cert-filename>` On Microsoft Windows, if *trusted_certificates* is not set, then the operating system certificate store is used.
-d `<seconds>`	Sets the frequency of the backend server liveness ping and backend server status request. The default is 5 seconds.

rsoe2 options	Description
-dl	Use this option to display log messages in the Relay Server Outbound Enabler console. By default, log messages are not displayed for verbosity levels 1 and 2.
-f `<farm>`	Specifies the name of the farm that the backend server belongs to.
-id `<id>`	Specifies the name assigned to the backend server.
-jsh `<number>`	Specifies the maximum number of junctions in the idle junction pool. The total number of junctions is allocated evenly across the number of Relay Servers in the farm. The default value is 200.
-jsl `<number>`	Specifies the minimum number of junctions in the idle junction pool. The total number of junctions is allocated evenly across the number of Relay Servers in the farm. The default value is 10.
-jl `<number>`	Specifies the maximum number of junctions (the sum of active and idle junctions). The total number of active and idle junctions is allocated evenly across the number of Relay Servers in the farm. This setting is overridden by the setting for max_junction in the Backend Server section of the Relay Server configuration file. The default value is 1000.
-o `<file>`	Specifies the file to log output messages to.
-oq	Prevents the appearance of the error window when a startup error occurs.
-os `<size>`	Sets the maximum size of the message log files. The minimum size limit is 10 KB.
-ot `<file>`	Truncates the specified log file and logs messages to it.
-q	Runs with a minimized window on startup.
-qc	Shuts down the window on completion.
-s	Stops the Outbound Enabler.
-t `<token>`	Sets the security token to be passed to the Relay Server.

rsoe2 options	Description
-uc	Starts rsoe2 in shell mode. This is the default. Applies to UNIX and Linux. Only specify one of -uc, -ui, -um, or -ux. When you specify -uc, the RSOE starts in the same manner as previous releases of the software.
-ud	Instructs rsoe2 to run as a daemon. Applies to UNIX and Linux platforms only.
-ui	Starts rsoe2 in shell mode if a usable display is not available. This option is for Linux with X window server support. When -ui is specified, the RSOE attempts to find a usable display. If it cannot find one, for example because the X window server isn't running, then rsoe2 starts in shell mode.
-ux	Opens the RSOE messages window where messages are displayed on Linux. On Microsoft Windows, the RSOE messages window appears automatically. When -ux is specified, the RSOE must be able to find a usable display. If it cannot find one, for example because the DISPLAY environment variable is not set or because the X window server is not running, the RSOE fails to start. To run the RSOE messages window in quiet mode, use -q.

rsoe2 options	Description
-v <level>	Sets the verbosity level to use for logging. The <level> can be 0, 1, 2, or higher (higher levels are used primarily for Technical Support): **0** Log errors only. Use this logging level for deployment. **1** Session level logging. This is a higher level view of a synchronization session. **2** Request logging. Provides a more detailed view of HTTP requests. **3 or higher** Detailed logging. Used primarily for Technical Support. Levels 1 and 2 are only written to the message log file and are not displayed. To have all log messages displayed, use the -dl option.

7.9.2.3 Restarting the Relay Server

If desired, you can restart the relay server to apply changes that you make to the relay server configuration file.

Context

The relay server automatically detects changes to the `rs.config` file without disrupting other IIS applications, but you may be more comfortable ensuring the configuration is read cleanly.

Procedure

From a command prompt running with administrator privileges, Issue this command: `iisreset`.

7.9.2.4 Relay Server Support for Server Components

To configure the relay server to support an Afaria server component, define the relay server configuration file and configure settings on the Afaria Administration console.

Afaria supports using the relay server with any of these server components:

- Afaria server
- Enrollment server
- iOS certificate authority server
- Afaria filter used for Access Control for Email
- Package server
- Application Onboarding certificate authority

The relay server configuration file `rs.config` consists of several sections. Use [backend_farm] and [backend_server] for each supported server component.

[backend_farm] creates a single, case-sensitive identifier for a component server environment, regardless of whether you are operating a single component server or a farm of component servers.

- enable – controls whether the farm operates.
  - yes – operate.
  - no – do not operate.
- id – user-defined, case-sensitive value for identifying a server farm. Each farm in the relay server configuration file must have a unique ID.
- description – user-defined description.
- client_security – specifies the secure communication protocol requirement for clients connecting to the relay server. This is an optional section that is not represented in the sample configuration file. Omitting the section results in the relay server enforcing the default value.
  - on – HTTPS is required.
  - off – default. HTTPS is not required; HTTP and HTTPS are both valid connection protocols.
- backend_security – specifies the secure communication protocol requirement for component servers connecting to the relay server. Omitting the section results in the relay server enforcing the default value.
  - on – HTTPS is required.
  - off – default. HTTPS is not required; HTTP and HTTPS are both valid connection protocols.

[backend_server] identifies a single component server to the relay server. You must have one [backend_server] section for each component server in your component server environment.

- enable – controls whether the server operates.
  - yes – operate.
  - no – do not operate.
- farm – the case-sensitive farm value is the same for each server. Use the same farm ID as from [backend_farm].
- ID – the ID value is unique for each server in the farm. If a server hosts more than one supported server component, then all server IDs on the host must be unique. For example, if a server hosts both an Afaria server and a package server, and both are defined in separate farms in the relay server configuration file, then the server IDs used for the two server components must be must be different.
- mac – mac address of the server component.
- token – the token is any string that you create. Use the same token value for each server in a farm.

> **Note**
>
> Values are case-sensitive.

Restart the relay server engine (`rshost.exe`) any time you make changes to the configuration file.

7.9.2.4.1 Relay Server Configuration File–Examples

Examples of the structure of the relay server configuration file based on the Afaria environment supported.

Single Afaria server – in an environment with a single relay server supporting a single Afaria server, the configuration file includes these sections:

- [options] – one instance.
- [relay_server] – one instance.
- [backend_farm] – one instance.
- [backend_server] – one instance.

Afaria server farm with four servers – in an environment with a single relay server supporting an Afaria server farm with four servers, the configuration file includes these sections:

- [options] – one instance.
- [relay_server] – one instance.
- [backend_farm] – one instance.
- [backend_server] – four instances.

Afaria server farm with four servers plus a package server – in an environment with a single relay server supporting an Afaria server farm with four servers and a package server, the configuration file includes these sections:

- [options] – one instance.
- [relay_server] – one instance.
- [backend_farm] – two instances.
- [backend_server] – five instances.

> **Example**
>
> This is a sample section of a relay server configuration file showing settings for a single Afaria server. Settings includes an instance of the [backend_farm] section and an instance of the [backend_server] section. The sample does not include the sections for the relay server basic operations.

```
#---------------
# Backend farms
#
# Notice that the case sensitive farmID must match the farmID set in the
Afaria Administrator's
# relay server configuration page.  Default value in Afaria is farmID=Afaria.
#---------------
[backend_farm]
enable          = yes
id              = farmID
description     = Afaria Farm
#-----------------
# Backend servers
```

```
#
# id must match regKey HKLM\Software\Afaria\Afaria\Server\TransmitterId
# on your afaria server
#-----------------
[backend_server]
enable    = yes
farm      = farmID
id        = sc
token     = zyyxpj22p
```

7.9.2.4.2 Configuring Relay Server for Afaria Server

To configure the relay server to support one or more Afaria servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

- As all relay server communications must use HTTP or HTTPS protocol, configure the Afaria server and devices to use HTTP or HTTPS.
- Set up the relay server for basic operations.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more Afaria servers. Consider these items when defining the [backend_farm] and [backend_server] sections.
   - [backend_farm]
     id – user-defined, case-sensitive value for identifying the server farm. The farm ID you define must match the farm ID you define on the Afaria Administration console ▸ *Server* ▸ *Configuration* ▸ *Relay Server* ▸ page. On the Relay Server page, the default value is “afaria”.
   - [backend_server]
     - id – define the server ID value to match the `TransmitterID` value defined in each Afaria server’s registry key `HKLM\Software\Afaria\Afaria\Server\TransmitterId`.
     - Token – the farm token you define must match the farm token you define on the Afaria Administration console ▸ *Server* ▸ *Configuration* ▸ *Relay Server* ▸ page.
2. On the ▸ *Server* ▸ *Configuration* ▸ *Relay Server* ▸ page of the Afaria Administration console, configure settings for communications between the relay server and the Afaria server component.
   - *Start the outbound enabler* – select this option to apply an automatic start-up attribute to the outbound enabler service. Afaria logging captures the outbound enabler’s restart and failure events.
   - *Farm ID* and *Farm token* – a pair of case-sensitive, ASCII text strings that your relay server uses to direct incoming client communication to your Afaria Server, either a standalone server or server farm. The combination of the strings must be unique for a given Afaria instance.

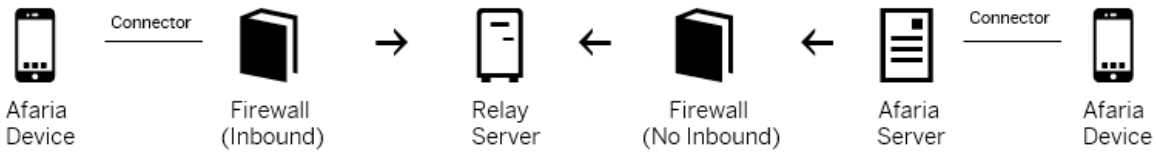
- *Farm ID* – value must match the corresponding value in your relay server's configuration file and in your device configuration settings.
- *Farm token* – value must match the corresponding value in your relay server's configuration file.

- *Server address and Server port* – the Afaria server IP address or "localhost" and HTTP port that the Afaria server is using for communications. In a server farm environment, you must enable HTTP on each Afaria server in the farm and use "localhost" rather than the IP address.
- *RS address and RS port* – the relay server IP address or fully qualified domain name and port that the outbound enabler service uses to connect to the relay server.
- *RS URL suffix* – text string used as an IIS parameter for invoking the relay server's Afaria Server Web services, as per the relay server installation instructions for creating the IIS application pool.
- *Maximum restarts* – the maximum number of times the outbound enabler attempts to start if it stops unexpectedly.
- *Client URL prefix*– text string used as an IIS parameter for invoking the relay server's Afaria client Web services, as per the relay server installation instructions for creating the IIS application pool. This value is also required as a configuration value on Afaria devices.
- *Use HTTPS* – enable the outbound enabler to communicate via SSL to the relay server.
- *Certificate path* – the path and file name on the Afaria server for the relay server's certificate file. The certificate contains the relay server's identity and public key.

3. Restart the relay server host.
4. Restart the Afaria server service.

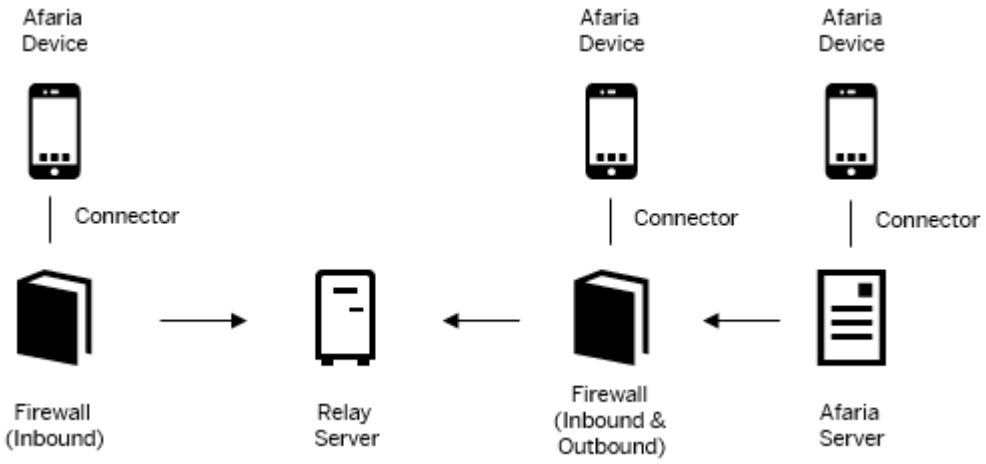
7.9.2.4.2.1 Relay Server Bypass

Even after your relay server is operational, the Afaria Server continues to support direct device connections. If it is appropriate for your environment, you may allow devices to continue to connect to the Afaria server directly, bypassing the relay server.



Bypass Relay Server—Sample 1

As the above diagram illustrates, if you have Afaria devices that are inside your organization's firewall and want to connect, you can allow these devices to make direct connections with the Afaria server using any of Afaria supported session protocols. These connections need not to pass through the firewall, so the firewall can support higher security.



Bypass Relay Server—Sample 2

As the above diagram illustrates, if you have devices that are outside your organization's firewall and want to connect, you can allow these devices to make direct connections with the Afaria server using any of Afaria supported session protocols as long as your firewall permits the traffic.

7.9.2.4.3 Configuring Relay Server for Enrollment Server

To configure the relay server to support one or more enrollment servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

- Set up the relay server for basic operations.
- Ensure that IIS is running on your enrollment servers.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more enrollment servers
   Consider this item when defining the [backend_farm] section:
   - id – user-defined, case-sensitive value for identifying the server farm.
2. Configure settings for communications between the relay server and the enrollment server component.
   a. In the Afaria Administration console, open the *Server* > *Configuration* > *Enrollment Server* page.
   b. In the Enrollment Server group, select *Use Relay Server.*
   c. In the Relay Farm ID field, enter the farm ID identifying your enrollment server farm.
   The value you enter must match the ID value you defined in the [backend_farm] section.
   d. In the relay server group, define these settings:

- If using HTTPS, select *Use HTTPS on Relay Server connections*
- *Server address* – address of the relay server
- *Client URL prefix* – IIS path to `rs_client.dll`, as defined in the machine hosting the relay server. The default value may differ from your relay server's IIS path.

e. Click *Save*.

3. Restart the relay server host.
4. (Optional) Restart the Afaria server service from the Afaria Administration console.
5. On your Afaria server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler` and import it to each machine where you installed an enrollment sever.
6. On each machine where you installed an enrollment server, launch the relay server outbound enabler from the command prompt.

7.9.2.4.4 Configuring Relay Server for Certificate Authority

To configure the Relay Server to support one or more certificate authority servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

- Set up the relay server for basic operations.
- Ensure that IIS is running on your certificate authority.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more certificate authority servers.
   Consider this item when defining the [backend_farm] section:
   - id – user-defined, case-sensitive value for identifying the server farm.
2. Configure settings for communications between the relay server and the certificate authority.
   a. In the Afaria Administration console, open the *Server* > *Configuration* > *Certificate Authority* page.
   b. Select the *Enable* check box for relay server and define these settings:
      - *Server address* – address of the relay server
      - *Farm ID* – farm ID identifying your iOS certificate authority farm.

        > **Note**
        >
        > The value you enter must match the ID value you defined in the [backend_farm] section.

      - *Device URL prefix* – IIS path to `rs_client.dll`, as defined in the machine hosting the relay server. The default value may differ from your relay server's IIS path.

c. Click *Save*.

3. Restart the relay server host.
4. (Optional) Restart the Afaria Server service from the Afaria Administration console.
5. On your Afaria Server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler` and import it to each machine where you installed a certificate authority server.
6. On each machine where you installed a certificate authority server, launch the relay server outbound enabler from the command prompt.

7.9.2.4.5 Configuring Relay Server for Access Control

To configure the relay server to support the access control filter, define the relay server configuration file, configure settings on the Afaria Administration console, and reinstall the PowerShell component of the access control filter.

Prerequisites

- Configure the relay server for basic operations.
- Configure the relay server for the SAP Afaria, regardless of whether you plan to use it for device connections.
- Install and configure the access control filter components.

Procedure

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 filter's farm ID as **`Afariafarm-IS.`**

2. On the *Server* > *Configuration* > *Access Control Server* page of the Afaria Administration console, select *Use Relay Server*, then click *Save*.
3. Reinstall the PowerShell component of the 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 filter.
4. Restart the machine on which you reinstalled the PowerShell component.
5. Restart the relay server host.

6. In the Afaria Administration console, restart the Afaria server service.

7.9.2.4.6 Configuring Relay Server for Package Server

To configure the relay server to support one or more Package Servers, define the relay server configuration file and configure settings on the Afaria Administration console.

Prerequisites

- Set up the relay server for basic operations.
- Ensure that IIS is running on your package servers.

Procedure

1. Configure the relay server configuration file `rs.config` to support one or more Package Servers. Consider this item when defining the [backend_farm] section:
   - id – user-defined, case-sensitive value for identifying the server farm.
2. Configure settings for communications between the relay server and the package server component.
   a. In the Afaria Administration console, open the *Server* > *Configuration* > *Package Server* page.
   b. In the Package Server (Direct Access) group, select *Use HTTPS on Package Server connections* and enter the server address for the package server.
   c. In the Package Server (Indirect Access) group, select *Use Relay Server* and enter the farm ID identifying your Package Server farm.
   The value you enter must match the id value you defined in the [backend_farm] section.
   d. In the Indirect Access (Relay Server) group, define these settings:
      - If using HTTPS, select *Use HTTPS on Relay Server connections.*
      - Server address – address of the relay server
      - Device URL prefix – IIS path to the relay server client virtual directory and `rs.dll`, as defined in the machine hosting the relay server.
      The default value may differ from your relay server's IIS path.
   e. Click *Save.*
3. Restart the relay server host.
4. (Optional) Restart the Afaria Server service from the Afaria Administration console.
5. On your Afaria Server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler2` and import it to each machine where you installed a Package Server.
6. On each machine, launch the relay server outbound enabler from the command prompt.

7.9.2.4.7 Launching the Relay Server Outbound Enabler

Launch the relay server outbound enabler (RSOE) from the command prompt of the server component.

Prerequisites

1. On your Afaria Server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler2.`
2. Import the folder to the machine hosting the server component.

Context

- The RSOE is the relay server's agent on a server component, such as the package server and the enrollment server. It initiates an outbound connection with the relay server.
- The executable file for the RSOE is `rsoe2.exe.`
- SAP recommends matching the versions of the RSOE and the relay server.

Procedure

1. From the command prompt of the machine hosting the server component, navigate to the `RSOutboundEnabler2` directory that you copied from the Afaria Server.
2. To launch the RSOE, use the command line:
   `rsoe2 -cr <param> -f <farm> -id <id> [options]`
   - -cr – parameters for the relay server connection.
   - -f – server component farm ID, as defined in the relay server configuration file.
   - -id – unique ID identifying the server component, as defined in the relay server configuration file.

   For a complete list of command line switches and their meanings, enter **`rsoe2`** at the command prompt and press *Enter.*

   If you include the security token when you define the [backend_server] section in the relay server configuration file, you must use the -t switch when launching the RSOE.

   When using the -cs switch, do not use "localhost" for the server address and do not use spaces in the name.

> ✤ Example
>
> This is a sample command line to launch the RSOE on a machine hosting the iOS certificate authority:
>
> **`rsoe2.exe -cr "host=www.rs.com;port=80" -cs "host= <<IP Address>>;port=80" -f CAFarmName -id CAID -t CAToken`**

Next Steps

(Optional) Install the RSOE as a Windows service.

7.9.2.4.7.1 Installing the Relay Server Outbound Enabler as a Windows Service

Install the relay server outbound enabler (RSOE) as a Windows service by running the `dbsvc.exe` service utility at the command prompt.

Prerequisites

1. On your Afaria server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler2.`
2. Import the folder to the machine hosting the server component.

Context

- Each instance of the RSOE can be installed as a Windows service.
- The RSOutboundEnabler2 folder includes `dbsvc.exe`, a service utility that installs the RSOE as a Windows service.

Procedure

On the machine hosting the server component, execute this command at a command prompt running with administrator privileges:

```
dbsvc.exe -as -s auto -sn "AfariaRSOE" -w AfariaRSOE "<<full path>>
\RSOutboundEnabler2\rsoe2.exe" @"<<full path>>\RSOutboundEnabler\rsoe.config"
```

For a complete list of the service utility's command line switches, enter **`dbsvc.exe`** at the command prompt and press *Enter.*

Results

- The command prompt displays a line confirming that the "AfariaRSOE" service was successfully created.

- The "AfariaRSOE" service is listed in the list of Windows services of the machine hosting the server component.

7.9.3 Launching the Relay Server Outbound Enabler

Launch the relay server outbound enabler (RSOE) from the command prompt of the server component.

Prerequisites

1. On your Afaria Server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler2.`
2. Import the folder to the machine hosting the server component.

Context

- The RSOE is the relay server's agent on a server component, such as the package server and the enrollment server. It initiates an outbound connection with the relay server.
- The executable file for the RSOE is `rsoe2.exe.`
- SAP recommends matching the versions of the RSOE and the relay server.

Procedure

1. From the command prompt of the machine hosting the server component, navigate to the `RSOutboundEnabler2` directory that you copied from the Afaria Server.
2. To launch the RSOE, use the command line:
   `rsoe2 -cr <param> -f <farm> -id <id> [options]`
   - -cr – parameters for the relay server connection.
   - -f – server component farm ID, as defined in the relay server configuration file.
   - -id – unique ID identifying the server component, as defined in the relay server configuration file.

   For a complete list of command line switches and their meanings, enter **`rsoe2`** at the command prompt and press *Enter*.

   If you include the security token when you define the [backend_server] section in the relay server configuration file, you must use the -t switch when launching the RSOE.

   When using the -cs switch, do not use "localhost" for the server address and do not use spaces in the name.

> ✤ Example
>
> This is a sample command line to launch the RSOE on a machine hosting the iOS certificate authority:

```
rsoe2.exe -cr "host=www.rs.com;port=80" -cs "host= <<IP Address>>;port=80" -f
CAFarmName -id CAID -t CAToken
```

Next Steps

(Optional) Install the RSOE as a Windows service.

7.9.3.1 Installing the Relay Server Outbound Enabler as a Windows Service

Install the relay server outbound enabler (RSOE) as a Windows service by running the `dbsvc.exe` service utility at the command prompt.

Prerequisites

1. On your Afaria server, copy the entire directory `<<Afaria Server Installation Directory>>\Server\bin\RSOutboundEnabler2.`
2. Import the folder to the machine hosting the server component.

Context

- Each instance of the RSOE can be installed as a Windows service.
- The RSOutboundEnabler2 folder includes `dbsvc.exe`, a service utility that installs the RSOE as a Windows service.

Procedure

On the machine hosting the server component, execute this command at a command prompt running with administrator privileges:

```
dbsvc.exe -as -s auto -sn "AfariaRSOE" -w AfariaRSOE "<<full path>>
\RSOutboundEnabler2\rsoe2.exe" @"<<full path>>\RSOutboundEnabler\rsoe.config"
```

For a complete list of the service utility's command line switches, enter **`dbsvc.exe`** at the command prompt and press *Enter.*

Results

- The command prompt displays a line confirming that the "AfariaRSOE" service was successfully created.
- The "AfariaRSOE" service is listed in the list of Windows services of the machine hosting the server component.

7.9.4 Relay Server with SSL

To configure the relay server to use SSL, you must install a trusted certificate on the server that is running the relay server's Microsoft Internet Information Services (IIS).

You can configure Afaria devices to connect securely using the relay server address and HTTPS protocol after you have installed the certificate. Connecting to the relay server with SSL ensures that the traffic from devices to the relay server is encrypted. If your Afaria Server and relay server are behind the same firewall, this configuration is all you need to secure your data.

Encrypting traffic between the relay server and the Afaria Server requires that you export the relay server's public key and copy the resulting file to the Afaria Server, then use the Afaria Administration console relay server page to enable HTTPS and specify the location of the public key file. All traffic is encrypted after you restart the Afaria Server.

7.9.5 Relay-Server-Related Logging

Relay-server-related logging allows you to retrieve connections and restart attempts occurred both on the Afaria Server and the relay server.

Context

- Afaria-side logging – captures the outbound enabler restart attempt events; it does not capture relay server start events when started by the Afaria service, as occurs when the "Start the outbound enabler" setting is selected.
- Relay-server-side logging – relay server logging captures events while relay server is active. The log is stored in the following relay server path: `<relay server installation path>\ias_relay_server\Log`.

The relay server log captures connections from the Afaria Server to the relay server and successful device connections. The log does not capture unsuccessful client connections.

Procedure

1. To retrieve logging from the relay server to the Afaria server, unselect *Start the outbound enabler* to prevent the outbound enabler from starting during the next restart.
2. Restart the Afaria Server service.
3. On the Afaria Server, open a command prompt and navigate to `<<Afaria Server Installation Directory>>\bin\RSOutboundEnabler2.`
4. Restart the outbound enabler using this single, continuous command:
   `rsoe2.exe -id <<AfariaServerID>> -f <<FarmID>> -t <<Farm token>> -cs "host=localhost;port=<<AfariaHTTPPort>>;" -cr "host=<<RelayServerIP>>;port=<<RelayServerHTTPPort>>;url_suffix=<<RsURLSuffix>>;url_prefix=<<ClientURLPrefix>>" -v <<LogVerbosity>> -o <<LogOutputPathFile>>`
   - `<<AfariaServerID>>` – the Afaria server ID value. The ID value is defined in the Afaria Server registry key HKLM\Software\Afaria\Afaria\Server\TransmitterId.
   - `<<FarmID>>` – farm ID, as stored on the Relay Server configuration page.
   - `<<Farm token>>` – farm token, as stored on the Relay Server configuration page.
   - `<<AfariaHTTPPort>>` – Afaria HTTP port, as stored on the Client Communications configuration page.
   - `<<RelayServerIP>>` – relay server IP address.
   - `<<RelayServerHTTPPort>>` – relay server HTTP port.
   - `<<RsURLSuffix>>` – RS URL suffix, as stored on the Relay Server configuration page.
   - `<<ClientURLPrefix>>` – client URL Prefix, as stored on the Relay Server configuration page.
   - `<<LogVerbosity>>` – controls the level of logging. Logs always include errors. Logs always include warning for levels 1-5.
     - 0 – no logging.
     - 1 – session-level logging.
     - 2 – request-level logging.
     - 3 – packet-level logging, terse.
     - 4 – packet-level logging, verbose.
     - 5 – transport-level logging.
   - `<<LogOutputPathFile>>` – Afaria Server path and file name for the log file.

   For a complete list of command line switches and their meanings, enter **`rsoe2`** at the command prompt and press *Enter.*

Example

This sample writes the log file to `c:\outbound.log` on the Afaria Server.

```
rsoe2.exe -id got -f AfariaFarm -t Token_00 -cs "host=localhost;port=80;" -cr
"host=10.14.229.21;port=80;url_suffix=/ias_relay_server/server/
rs.dll;url_prefix=/ias_relay_server/client/rs.dll" -v 5 -o c:\outbound.log -af
```

8 Server Configuration for Installation and Management

Server configuration properties, as defined in the server configuration page

Related Information

Configuring Afaria Server for Package Server [page 39]
Configuring Relay Server for Access Control [page 60]
Configuring the Relay Server for Certificate Authority and Enrollment Server Connections [page 37]

8.1 Selecting a Server

When multiple servers are defined for an Afaria server farm, select a server on the Server > Configuration page to change the server context for configuration and management. If the system has only one server, it is the main server, which displays on the Home page banner at all times and is the server for all operations.

Context

The server list is cached when you start a session. If one administrator makes a change to the list during a session, other administrators do not see the change until their next session.

Procedure

1. On the Home page, on the Server tile, click the *Configuration* icon to open the *Server* > *Configuration* page.
2. On the page banner, click *Server selector* to open the list.
3. Select a server.

   The server selection persists until you change it.

8.2 Showing or Hiding Servers in the Server List

To allow or disallow selection of a server in the Afaria banner bar's server list, show or hide a server. For example, hide a server that you want to take down for maintenance.

Context

You cannot hide the master server.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Server Farm*.
3. Select a server and click *Edit*.
4. Select *Visible* or *Hidden*:
   - Visible – the server appears in the server list.
   - Hidden – the server does not appear in the server list.
5. On the server row you are editing, click *Save* below the Replication Address.
6. Click *Save* at the top of the page.

8.3 Configuration for Security

Use the Security property page to configure NT, LDAP, or Active Directory user authentication, to set timeout values for user authentication and user group assignments, and to specify whether to automatically approve new, enrolling clients.

In a fresh installation of Afaria, the default directory security authentication model for devices and self-service portals is NT Domain. You can change this default after installation; to do so log in to the Afaria Administrator portal, choose the desired tenant (if you have created more than one), and access the security screen by selecting *Server* > *Configuration* > *Server* > *Security*. Change the directory security settings to match the NT domain, AD, or LDAP server.

For the greatest security level in LDAP or Active Directory environments, enable both authentication and SSL. When you enable SSL from the Security property page, you enable it only for LDAP-supported or Active Directory authentication and assignments, that is, it is not enabled for NT domains.

Related Information

Configuring NT Domain [page 124]
Configuring Active Directory [page 125]
Configuring LDAP [page 126]

8.3.1 Afaria Managed Authentication

You can set Afaria-managed authentication for the Enrollment Server and Package Server using the Enable Authentication setting on the *Server* > *Configuration* > *Server* > *Security* page in the Afaria Administration console. This setting applies to individual tenants.

Disable Afaria-managed authentication for the Enrollment Server and Package Server by turning off the Enable Authentication setting on the Afaria Administration console for the devices that are associated with the tenant.

8.3.2 Configuring NT Domain

Configure NT domain settings to support user authentication and assignments.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Security*.
3. Select *NT Domain* as the directory type.
4. Specify the NT default authentication and NT assignment domains.

   If you are using NT for authentication and assignments, you can change the NT domain against which users are verified. If you did not specify any domain when you installed the server, users automatically authenticate against the local computer. Separate the multiple domains with commas.
5. Select *Automatically approve new device* to automatically approve new devices.

   Approved devices, when connected to the Afaria Server, receive group profiles and system files.
6. Select *Enable authentication* for either NT or SSL communication between your server and devices.
7. Specify the length of time a cookie is valid by setting an authentication time out value.

   You can also set an automatic renewal period during which a cookie is nearing it's expiration date, if the user connects to the server during the specified time period, the cookie is automatically renewed.
8. In the Assignment section, specify the length of time that user-group-assignment cookies remain valid.
9. Click *Save* at the top of the page.

8.3.3 Configuring Active Directory

Configure Active Directory (AD) domain settings to support user authentication and assignments.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Security*.
3. Select *Active Directory* as the directory type.
4. In the *Directory Server* area, enter or select the directory settings:
   - Server Address – enter the Active Directory server address as either a fully qualified domain name, such as afaria.mycompany.com, or as an IP address.
   - Use SSL – enable SSL communication between the Afaria Server and the Active Directory server.
   - User – enter the user ID for the Active Directory account the Afaria Server service uses to communicate with the Active Directory server. Consider the following about AD users:
     Users that are added to the AD Users container implicitly are not displayed as users when viewing the members from the Group editor. However, policies assigned to implicit users will be deployed successfully.
     Deleting a user from AD does not disable the user in the groups list. The AD monitor only receives notifications that users have been deleted when they have been disabled.
   - Password – enter the password for the Active Directory account the Afaria Server service uses to communicate with the Active Directory server.
   - Search Root for User – specifies the node where the search begins.
   - Class Name for Users – identifies the type of user object selected.
5. In the *Client* area, select *Automatically approve new device* to automatically approve new devices.

   Approved devices, when connected to the Afaria Server, receive group profiles and system files.
6. (Optional) Select *Stop device management when directory user record is disabled* .

   If the user is disabled in Active Directory, Afaria will:
   - For Android:
     - Remove NitroDesk data – removes all configuration and user data associated with the NitroDesk.
     - Block access control for email – sets the access control for email policy to block.
     - Unapprove device – sets the device state to unapproved.
   - For iOS:
     - Remove MDM – removes Afaria Mobile Device Management (MDM) control from the device.
     - Block access control for email – sets the access control for email policy to block.
     - Unapprove device – sets the device state to unapproved.

   > **i Note**
   >
   > Enabling this option starts a one-time process during which the Afaria Server synchronizes some information with the configured Active Directory server. For directory servers with a large number of user records, the process may take a few hours to complete.
7. In the *User Data Attribute* area, enter and select the User Data settings:

- User Name Attribute – the server uses the User Name Attribute you selected for the user ID to verify the user.

  > **i Note**
  >
  > If the non-default class name for users or user name attributes are manually entered, they will not be added to the default dropdown selection list.

  > **i Note**
  >
  > If the directory server changes, the existing groups with the assigned users will not be removed. The users will need to be removed manually.

- Certificate Common Name – the LDAP property that provides the identity of the certificate.
  If the Common Name of the user's certificate needs to be different than the authenticated username, then the administrators can specify the LDAP Property to query. The common name of the retrieve certificate is set to the queried value.

8. In the *Client Session* area, do the following:
   1. Select *Enable authentication* for either NT or SSL communication between your server and devices.
   2. Specify the length of time a cookie is valid by setting an authentication time out value.
      You can also set an automatic renewal period during which a cookie is nearing it's expiration date, if the user connects to the server during the specified time period, the cookie is automatically renewed.
   3. In the Assignment section, specify the length of time that user-group-assignment cookies remain valid.
9. Click *Save* at the top of the page.

   > **i Note**
   >
   > To monitor the changes in the Active Directory object data using DirSync control, the user account must have the Replicating Directory Changes permission on the domain naming context. To grant the Replicating Directory Changes permission to a user account or group, you must modify the permissions on the directory partition object.

   See *Afaria Installation Guide* for basic rights for Active Directory user.

8.3.4 Configuring LDAP

Configure LDAP domain settings to support user authentication and assignments.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Security*.
3. Select *LDAP-based* as the directory type.
4. In the *Directory Server* area, enter or select the directory settings:

- Server Address – enter the LDAP server address as either a fully qualified domain name, such as afaria.mycompany.com, or as an IP address.
- Use SSL – enable SSL communication between the Afaria server and the LDAP server.
- User – enter the user ID for the LDAP account the Afaria server uses to communicate with the LDAP server.
- Password – enter the password for the user ID.
- Search Root for User – specifies the node where the search begins.
- Class Name for Users – identifies the type of user object selected.
- Server Type – select *Microsoft Active Directory*.
- Select *Support OU membership* to support authentication against organizational units only, or you can select *Support OU and group membership* to support authentication against both organizational units and groups.

5. In the *Client* area, select *Automatically approve new device* to automatically approve new devices.

   Approved devices, when connected to the Afaria Server, receive group profiles and system files.
6. In the *User Data Attribute* area, enter and select the User Data settings:
   - User Name Attribute – the server uses the User Name Attribute you selected for the user ID to verify the user.

     > **i Note**
     >
     > If the non-default class name for users or user name attributes are manually entered, they will not be added to the default dropdown selection list.

   - Certificate Common Name – the LDAP property that provides the identity of the certificate.
     If the Common Name of the user's certificate needs to be different than the authenticated user name, then the administrators can specify the LDAP Property to query. The common name of the retrieve certificate is set to the queried value.
7. In the *Client Session* area, do the following:
   1. Select *Enable authentication* for either NT or SSL communication between your server and clients.
   2. Specify the length of time a cookie is valid by setting an authentication time out value.
   3. Set an automatic renewal period during which a cookie is nearing it's expiration date
      If the user connects to the server during the specified time period, the cookie is automatically renewed.
   4. In the Assignment section, specify the length of time that user-group-assignment cookies remain valid.
8. Click *Save* at the top of the page.

8.4 Configuration for Schedules

Schedules enable you to set specific tasks, such as updating channel content or refreshing dynamic groups, to perform automatically at specific times, days, and for a specified length of time. You have the ability to edit schedule settings, enable or disable schedules, and run schedules on demand.

8.4.1 Editing a Schedule

Edit a schedule's start and end times, how long and often it runs, and set it to retry to run after failing by changing the settings for each individually listed schedule.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Schedule*.
3. Select one of the listed schedules.
4. Click *Edit connection rule*.
5. Select the type of schedule from the drop-down menu.
6. Click the tabs to edit the settings:
   - Rate – set the start time and how many days the schedule runs.
   - Range – select a start and end date for the schedule.
   - Repeat – select how often the schedule repeats.
   - Retry – select how many times and how often the schedule tries after failing to run.
   - Randomize – not applicable.
7. Click *Save*.

8.4.2 Enabling or Disabling Schedules

Manually enable or disable schedules to temporarily or permanently start or stop the task each schedule is set to perform. By default, iOS schedules are disabled after installation.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Schedule*.

3. Select one or multiple schedules.
4. Click *Enable* or *Disable*.
    - Enable – starts running the schedule according to the saved settings.
    - Disable – stops running the schedule according to the saved settings.

8.4.3 Running a Schedule on Demand

Manually run a schedule as needed, without changing the schedule's normal run time.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Schedule*.
3. Select one of the listed schedules.
4. Click *Run Now*.

Results

The selected schedule runs, and the *Last Run* column is updated.

8.5 Configuration for Logging

Configure the type, detail level, and cleanup frequency for Afaria server-side logging.

8.5.1 Configuring Log Options

Configure the Afaria server-side logging options by type and detail level. By default, all logs are enabled.

Procedure

1. On the Server page, on the left toolbar, click *Configuration* > *Server* > *Log Option*.
2. Click *Disable every log below* to disable all logging options or select logs to enable in different areas:

- Message log – records information, warning, and error messages specific to the server.
- Replication log – records replication-specific information, warning and error messages.
- Session log – records information about past sessions, such as the channel involved, the end time and duration, the user and computer information, and the session event status.
- Session event detail – records log details at the object level pertaining to File Transfers or Sessions.
- Device action log – records information about actions occurring on the devices.
- Alert log – enables the server to log both raised events and closed alerts on your server.

Administrative actions performed by the user is recorded in system logs. The user or role executing the action is recorded in the log entries by the logged in user.

3. Click *Save*.

8.5.2 Configuring and Running Log Cleanup

Specify how often the SAP Afaria server deletes log files. You can also delete log files by running the log cleanup process when required.

Procedure

1. On the Server page, on the left toolbar, click *Configuration* > *Server* > *Log Cleanup*.
2. Perform one of the following tasks:
   a. To enable log cleanup, select the *Enable* check box and specify the age (in days) at which the SAP Afaria server deletes the log files in the *Number of days* field.
   b. To disable log cleanup, clear the *Enable* check box.
   c. To restore log cleanup default settings, click *Reset to defaults*.
3. Click *Save*.
4. To run log cleanup outside of the scheduled time, click *Configuration* > *Server* > *Schedule* from the menu, select Log Cleanup from the list, and then click *Run Now* at the top of the page.

8.6 Configuring for Outbound Notifications

Outbound notifications for iOS devices are treated differently from those of non-iOS devices.

8.6.1 Configuring Apple Notification Throttling

Notifications sent to iOS devices are managed in the Afaria Administration console according to the Apple notification throttling settings in Afaria. iOS notifications are throttled, which means that they manage the load placed on the Afaria system by distributing over a period of time, the number of APNS notifications sent to

devices. The Apple Notification Throttling settings affect only the notification sent to devices through the APNs, as an indirect mechanism that controls the number of concurrent iOS device connections to the Afaria system. Actual device connections are affected by a number of additional factors, including the device state (locked, on, off) and network availability.

Context

Throttling Settings

The following two settings manage Apple Notification Throttling:

- *Throttling Rate* manages the maximum number of notifications successfully sent, per minute, to the APNs. For example, a setting of 50 means that Afaria sends 50 device notifications to APNS each minute until there are no notifications left to send. A value of 0 disables throttling, meaning that all notifications are sent as quickly as possible.
- Set *Throttling Scope* to "per server" to apply the same throttling rate to every active server in an Afaria server farm. If you do not set "per server", then the throttling rate applies across the entire farm, and is divided by the number of active servers in the farm. Throttling scope is ignored if the throttling rate is 0 (disabled).
  - For example, “Per server” selected: If the throttling rate is 50, and scope is per server, 5 active servers gives an aggregate throttling rate of 250. Afaria sends out 250 notifications per minute.
  - For example “Per server” not selected: If the throttling rate is 50, and scope is not per server, 5 active servers gives an aggregate throttling rate of 50. Afaria sends out 50 notifications per minute.

Device Actions

Administrator-initiated actions and user-initiated actions are independent of each other, and have separate settings that establish priority for user-initiated actions.

- *Administrator-Initiated Actions* are performed from within the Afaria Administrator or through the iOS Schedules (in Server Schedules). All administrator-initiated actions requiring iOS device notifications adhere to the throttling settings specified herein to manage the notifications sent via the APNs.
  - The default setting on a new installation is 50, indicating 50 device notifications are sent each minute.

> **i Note**
>
> Disabling throttling by setting the value to zero can potentially overload the Afaria system, depending on the number of devices being immediately notified and connecting to to the Afaria farm, relative to its load handling capability.

- *User-Initiated Actions* are performed on the device, whereupon the user is expecting a swift response.
  - The default value for the user-initiated throttling settings is zero so that notifications are not throttled, and thus sent to the APNs for immediate response to end-users.

> **i Note**
>
> Due to the general sporadic nature of user-initiated actions, disabling throttling for this queue doesn't generally cause any load problems on the Afaria server.

Procedure

1. On the *Server* page, from the left toolbar, select *Configuration*.
2. Select *Server Outbound Notification*.
3. In the *Apple Notification Throttling* area, set the values to control throttling using the guidelines described above.
4. Click *Save*.

   Changes to the Apple notification throttling settings do not require a restart of any Afaria services, however, it may take up to one minute for changes to take effect.

   Only the system tenant APNs configuration contacts Apple for all device notifications, across all tenants.

8.6.2 Configuring Outbound Notifications for Non-iOS Devices

Set the flood control level to prevent the Afaria server from being overwhelmed with incoming sessions. Use the notification retries options to control whether and how often notifications are re-sent to devices.

Procedure

1. On the Server page, from the left toolbar, click *Configuration*.
2. Select *Server* > *Outbound Notification*.
3. In the Flood control area, set the values to control the number of client notifications sent during a given time period:
   - High water – notifications stop going out when the active sessions reach this number.
   - Low water – notifications resume when the active sessions drop to this number.
   - Maximum per time period – number of active sessions that occur within the specified time period.
   - Time period in seconds – time period for the maximum per time period.
   - Max simultaneous notifications – number of notifications to group together.

   Set any of these values to zero if you don't want to use them.
4. Select *Enable Notification Retries*.
5. Set the following values:
   - Retry wait time – set the amount of time in days, hours, and minutes. The maximum values for the days, hours and minutes are 30, 23, and 59.
   - Maximum SMS retries – set the number of SMS and C2DM retries that can occur in the specified time period. The maximum value is 100.
   - Maximum IP retries – set the number of IP retries that can occur in the specified time period. The maximum value is 100.

   Set any of these values to zero if you don't want to use them.
6. Click *Save*.

The message in the popup that appears after you send an outbound notification does not indicate an error in case of a failed outbound notification. To see the actual status of an outbound message, check the server message logs.

8.7 Afaria Server for GCM

Use Firebase Cloud Messaging (FCM), formerly known as Google Cloud Messaging (GCM), to reduce SMS data usage and simplify Afaria implementation for Android devices.

FCM is the new version of GCM. Google integrated Cloud Messaging into Firebase to unify their mobile platform and to enable cross-feature integration. An active Google account is needed to utilize FCM.

To get started with FCM, create a new project or import an existing GCM project by visiting the following page: https://console.firebase.google.com .

Reference the following Knowledge Base Article for details on migrating from GCM to FCM: https://launchpad.support.sap.com/#/notes/2370587/E.

8.7.1 Configuring Firebase/Google Cloud Messaging

Configure the Afaria server to use Firebase Cloud Messaging (FCM), formerly known as Google Cloud Messaging (GCM), as an alternative to SMS notifications for Android devices.

Prerequisites

- Ensure that you have a Gmail account created on behalf of your organization.
- Obtain the required application Server key and Sender ID from Firebase.

> **i Note**
>
> The FCM Server key and Sender ID are the same as the GCM API key and Project ID respectively.

Procedure

1. On Home page Server tile, click *Configuration* to open the *Server Configuration* page.
2. Navigate to the *Component* > *Google Services* page.
3. In the GCM Server area, select *Enable GCM* to enable FCM/GCM services.
4. Enter the server address, as defined by Google.
   - For FCM, use `https://fcm.googleapis.com/fcm/send`

- For GCM, use `https://android.googleapis.com/gcm/send`

> **Note**
>
> The default URL for GCM is populated if you choose the *Reset to default* link. This URL is also valid for FCM.

5. Enter the FCM Sender ID in the *GCM Project ID* field.
6. Enter the FCM Server key in the *GCM API key* field.
7. Click *Save*.
8. Restart the Afaria Server service.
9. Connect the devices manually.

   For new devices, create a new enrollment policy with FCM/GCM enabled. The enrollment policy using FCM/GCM is applied when the user enters the enrollment code on the device. The configuration policy containing the new FCM/GCM data is pushed to the device next time an existing device connects. The device is registered with FCM/GCM when the new seed data is processed and another session is initiated to update the Afaria server with the new registration token.

Related Information

Configuring Afaria Server for Enrollment Codes [page 33]

8.8 Android for Work

Android for Work is Google's enterprise mobility management (EMM) platform that lets companies deliver a secure, productive, and rich mobile experience to their employees. SAP Afaria provides seamless support for it.

> **Note**
>
> To enroll your enterprise into Android for Work, contact SAP Support for assistance.

Android for Work offers the following benefits:

- Security and data separation – ensure business data is safe from malware and seperate from personal data, using hardware-based encryption and admin-managed policies.
- Support for both employee-owned and company-provisioned devices – users can safely use a single Android device for business and personal use, and companies can provision devices they own or configure work profiles on employee-owned devices.
- Remote management – administrators can remotely control all work-related policies, applications, and data.
- Seamless user experience – delivers a consistent experience across all devices, and lets users intuitively and effortlessly switch between work and personal applications. Business applications and personal applications appear together in the launcher and recent applications list, but business application icons are clearly distinguished by the badge icon.

> **Note**
>
> Android for Work is supported on Android devices running Lollipop. Refer to the *SAP Afaria System Requirements* for more information.

8.9 Configuration for iOS

For iOS management, enable iOS Apply Policies and iOS Device Refresh schedules that are disabled by default. Optionally, configure custom branding for the Afaria application that is installed on devices.

8.9.1 Enabling or Disabling Schedules

Manually enable or disable schedules to temporarily or permanently start or stop the task each schedule is set to perform. By default, iOS schedules are disabled after installation.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Schedule*.
3. Select one or multiple schedules.
4. Click *Enable* or *Disable*.
   - Enable – starts running the schedule according to the saved settings.
   - Disable – stops running the schedule according to the saved settings.

8.9.2 Installing a SAP Afaria Client for iOS Devices Automatically During Enrollment

You can specify the SAP Afaria Client that SAP Afaria installs automatically on devices during enrollment.

Context

If you do not install the SAP Afaria Client automatically, the user must install the client manually and SAP Afaria does not manage the client using MDM.

Procedure

1. On the *Server* page, click the *Configuration* icon.
2. Expand the *Enrollment* list and click *iOS Afaria Application*.
3. To install the SAP Afaria Client on the iOS device automatically during enrollment, select the *Install during enrollment* check box.
4. Perform one of the following actions:
   - Select *AppStore* to automatically install the SAP Afaria Client from the Apple App Store.
   - Select *Custom* and browse to the client file to automatically install a custom client.
5. Click *Save*.

8.9.3 Adding Customized Branding to the App Store Application

Customize the Afaria Administration console with your own corporate brand using a custom background image and text .

Procedure

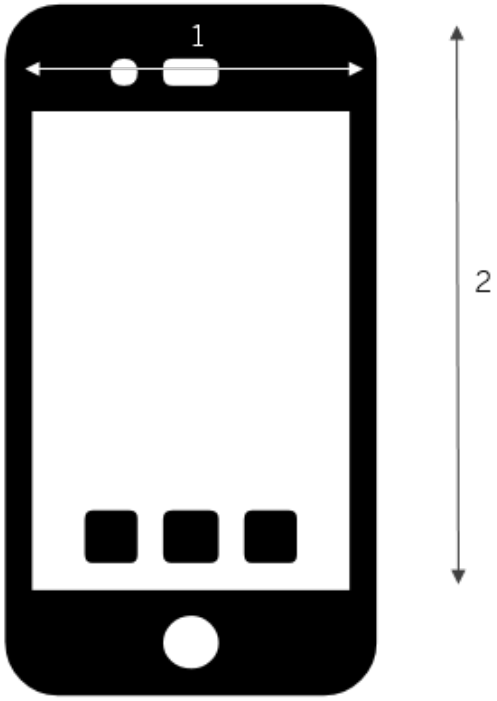
1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Component* > *iOS Branding* page.
3. Select default text or custom text for enterprise branding, and enter the text if you select the custom option.

   This text will appear on the device This text is common for all iOS device types and needs to be specified only once.
4. (Optional) Click *Language Option* to define the text in additional languages, as required, for devices in supported regions.
5. Select the device type from the type selector drop-down list next to the *Splash Screen* text label.
6. Select the default or custom image option (.JPG or .PNG) for portrait and landscape image formats.
7. (Optional) Click *Browse* and select the custom branding image.

   If you use an iPad for managing devices, the browse option does not work as there is no file system support on iOS devices.
8. Click *Save*.
   The new or the updated branding appears when Afaria Administration console is opened on the device.

8.9.3.1 iOS Branding Element Map

Branding elements on the diagram map to elements on the Apple App Store Afaria Application Home screen.



Element	Maps to... on iOS Configuration > About Branding Tab
1	Title to display on the Afaria home screen
2	Background image to display in portrait mode
N/A	Background image to display in landscape mode

8.9.3.2 Language Localization and Branding on the Afaria iOS Application

For the text on the Afaria application info page, the appearance is determined by the settings you use on the associated *Server Configuration* > *Component* > *iOS Branding* page, the languages supported on the device, and the regional settings on the device.

The Language Option link on the iOS branding page opens the multi-language branding dialog, to define branding text for supported languages.

Localization and branding results for branding page settings:

- Default text, without language branding – for devices using a regional setting for a supported language, text is localized with system-localized content. For devices using a regional setting for a unsupported language, the text is in English.
- Custom text, without language branding – all devices display custom text, regardless of regional setting.
- Default or custom text, with language branding – for devices using a regional setting for a language that has defined text in the language branding dialog, text appears as defined.

8.9.4 Configuring Payload Signing

Payload signing helps secure payloads during delivery. You can add payload signing or change the signing certificate that you added during the installation of the SAP Afaria Enrollment Server.

Context

Perform the following task for each SAP Afaria Enrollment Server. Every Enrollment Server must have the same signing certificate.

Procedure

1. Add the signing certificate to the SAP Afaria Enrollment Server.
2. Import the signing certificate to the certificate store on the SAP Afaria Enrollment Server.

3. Grant read permission for the signing certificate to the IIS_IUSRS user.
4. In the Afaria Administration console, on the *Server* > *Configuration* > *Enrollment Server* page, type the common name of the signing certificate in the *Signing certificate name* field and click *Save*.

8.10 Configuration for Device Activity Collection

You can configure the SAP Afaria Server to collect data about device activity.

No additional server components are required, but you must configure the SAP Afaria Server and devices for device activity collection. Use the Afaria Administration console to configure device activity settings on a tenant-by-tenant basis.

8.10.1 Preparing Devices for Activity Collection

Prepare the device for activity collection by installing the SAP Afaria client and enabling Location Services.

Procedure

1. Install the SAP Afaria client on the device and enroll in SAP Afaria device management.
2. During the application installation, authorize and enable Location Services.

   On iOS devices, the SAP Afaria client must continuously run for device activity to be able to monitor activities. Enabling Location Services for SAP Afaria keeps the SAP Afaria client continuously running in the background.

8.10.2 Device Activity Collection Considerations

Afaria Device Activity data collection allows you to collect various types of data from enrolled devices and use it for monitoring and report purposes.

> **i** Note
>
> Device activity data collection is disabled by default.

Starting data collection:

- If user authorization is required, device activity data collection begins after the user accepts device activity enrollment. The user response (accept or decline) is sent back to the Afaria server and appears in the Opt-in column of the Subscribers view.
- If user authorization is not required, device activity data collection begins after you enable device activity collection; restart the Afaria server service; and the device connects to the server.

- A device retains its device activity collection preference (accept or decline) when it changes tenant. However, if the user has previously declined and you move the device to a tenant where user acceptance of device activity is not required, device activity collection begins without further user notification.

Ongoing data collection:

- Device activity data is associated with a subscriber. If a device has an SIM, the subscriber is identified by the SIM IMSI or ICCID. Device activity data moves with the SIM from device to device.
- On iOS devices, device activity data collection stops automatically if the user turns off location services for more than 10 minutes.

8.10.3 Device Activity Collection Frequency

Data collection frequency settings indicate when Afaria collects device activity data from enrolled devices.

The frequency of data collection varies by device type.

- For iOS devices, Afaria collects device activity data once a day between 2:00 a.m. and 3:00 a.m. (client local time).
- For Android devices, Afaria collects device activity data at the frequency based on the schedule settings defined in the configuration policy.
- For Windows Phone devices, a background service enabled for the Afaria application, runs along with other scheduled operating system tasks and collects device activity data. This background task runs approximately every 20 minutes and sends the device coordinates to the Afaria server.

8.10.4 Collecting Device Activity Data

Use the Afaria Administration console to configure SAP Afaria to collect device activity data.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Device Activity*.
3. On the *General Settings* tab, perform the following tasks:
   a. Select *Enable Activity Collection*.
   b. To collect phone numbers that make calls to devices, select *Collect Remote Party Phone Numbers*.
   c. To collect location data from devices, select *Collect Subscriber Location Information*.
   d. To prompt users to allow SAP Afaria to collect device activity data, select *Prompt Subscriber for Activity Enrollment.*
   e. Type the message that devices display when prompting users to allow the collection of device activity data.

   If you select *Prompt Subscriber for Activity Enrollment*, data collection begins when the user accepts the device activity collection prompt on the device.

4. To prompt users to accept device activity collection, select *Prompt Subscriber for Activity Enrollment*.
   For Windows Phone devices, this option applies only if you select Collect Subscriber Location Information.
5. In the *Enrollment Notification* field, type the message that devices display when prompting users to accept device activity collection.
6. Click *Save*.
7. Click *Restart Server*.

8.10.5 Stopping Device Activity Collection

Stop the SAP Afaria Server from collecting device activity data.

Procedure

1. In the Afaria Administration console, on the *Server* page, select *Configuration* > *Component* > *Device Activity*.
2. On the *General Settings* tab, unselect *Enable Activity Collection*.
3. Save changes.
4. Click *Restart Server* to restart the SAP Afaria Server service.
   After you restart the server, device activity data collection stops for each device connecting to the server.

8.10.6 Reprompting for Device Activity Enrollment

Reprompt users and resend the Device Activity enrollment notifications to those who have previously accepted or declined enrollment.

Prerequisites

Before you set up the reprompt, verify that *Prompt Subscriber for Activity Enrollment* is selected on the Device Activity General Settings tab on the *Server* > *Configuration* > *Component* > *Device Activity* page.

Procedure

1. On the Device page, select *Activity List*.
2. Navigate the Activity views, select *Subscribers view*, and click *Select*.

3. Select a subscriber and click *Reprompt* to resend the notification.

   The Opt In column in the Subscribers view indicates which users have accepted or declined enrollment.

   The user receives either the default enrollment notification or the custom notification you set up on the Device Activity General Settings page.

8.10.7 Subscriber Data Collected by Device Type

Definitions of subscriber data, such as IMSI, ICCID, and MSISDN, collected by each device type.

Subscriber Data	iOS	Android	Windows Phone	Definitions
IMSI		X		International Mobile Subscriber Identity, conforming to International Telecommunication Union (ITU) standard.
ICCID	X			Integrated Circuit Card Identifier, conforming to International Telecommunication Union (ITU) standard.
Cell ID		X		Last reported cell ID. On CDMA networks, the Base Station ID (BID).
Current Afaria Client ID	X	X	X	SAP Afaria client global unique identifier (GUID).
Current Device ID	X	X		iOS – Unique Device Identifier (UDID), Wi-Fi MAC Address. Android - International Mobile Equipment Identity (IMEI).
MSISDN		X		Mobile Subscriber Integrated Services Digital Network Number which is the literal phone number as reported by the device. Not all SIM cards, specifically in Europe, are preprogrammed with an MSISDN.
Home MCC	X	X	X	Home network Mobile Country Code.
Home MNC	X	X	X	Home network Mobile Network Code.
Activity Last Collected	X	X	X	Date on which Device Activity data was last posted on the server by the device.
Last MCC	X	X		Last reported Mobile Country Code (MCC).
Last MNC	X	X		Last reported Mobile Network Code (MNC). On CDMA networks, the network System Identifier (SID).
Latitude	X	X	X	Last reported approximate latitude, based on crowd-sourced Wi-Fi hotspot and mobile cell tower location.

Subscriber Data	iOS	Android	Windows Phone	Definitions
Longitude	X	X	X	Last reported approximate longitude, based on crowd-sourced Wi-Fi hotspot and mobile cell tower location.
Location Last Determined	X	X	X	Date and time of the last location change.
Opt In	X	X	X	User answer to request for Device Activity Enrollment (accepted/declined).
Roaming Change Date	X	X		Date and time of the last roaming state change.
Status of Location Services	X	X	X	Status of Location Services on the device (enabled or disabled).

8.10.8 Removing Device Activity Data for a Subscriber

Remove all device activity data related to a subscriber.

Procedure

1. On the Device page, on the left toolbar, click *Device List*.
2. Select a subscriber.
3. On the top toolbar, click *Delete*.
4. Select *Device Activity*.
   All device activity data collected for the subscriber is deleted, regardless of when it was collected.

8.10.9 Device Activity Calls by Device Type

Definitions of voice call details collected by each device type, for example, Cell ID and MCC.

Voice Call Details	iOS	Android	Definitions
Remote Party		X	Remote party phone number.
Start Time	X	X	Start time of the call event.
End Time	X	X	End time of the call event. End Time does not appear in data views and reports.

Voice

Call

Details	iOS	Android	Definitions
Duration	X	X	Duration of call event.
Call Direction	X	X	Outbound or inbound call.
Cell ID		X	Mobile cell ID at the start of connection. On CDMA networks, the Base Station ID (BID) at the start of the connection.
Roaming State	X	X	Roaming status.
Latitude	X	X	Latitude generated at the start of a call.
Longitude	X	X	Longitude generated at the start of a call.
MCC	X	X	Mobile Country Code of the network on which the call event occurred.
MNC	X	X	Mobile Network Code of the network on which the call event occurred.

8.10.10 Device Activity Data Connections Details by Device Type

Definitions of data connection details collected by device type, for example, Bearer Type and MNC.

Data Connection Details	iOS	Android	Definitions
Start Time	X	X	Start time of the call event
End Time	X	X	End time of the call event. End Time does not appear in data views and reports.
Duration	X	X	Duration of call event.
Bearer Type	X	X	Network type, such as CMDA, GSM and Wi-Fi, at the start of the connection.
Connection Name		X	Network name.
Access Point Name		X	Access Point Name.
Cell ID		X	Mobile cell ID at the start of connection. On CDMA networks, the Base Station ID (BID) at the start of the connection.
Roaming State	X	X	Roaming status.
Latitude	X	X	Latitude generated at the start of the connection.
Longitude	X	X	Longitude generated at the start of the connection.

Data Connection Details	iOS	Android	Definitions
MCC	X	X	Mobile Country Code of the network on which the connection occurred.
MNC	X	X	Mobile Network Code of the network on which the connection occurred.
Sent	X	X	Number of bytes transmitted.
Received	X	X	Number of bytes received.

8.10.11 Device Activity Messages by Device Type

Definitions of message details collected by each device type, for example, cell ID and Type. Device Activity messages are not supported on iOS devices.

Message Details	iOS	Android	Definitions
Remote Party		X	Remote party phone number.
Start Time		X	Start time of the call event.
Message Direction		X	Outbound or inbound message.
Type		X	SMS or MMS.
Cell ID		X	Mobile cell ID at the start of connection. On CDMA networks, the Base Station ID (BID) at the time the message is sent.
Roaming State		X	Roaming status.
Latitude		X	Latitude generated when message is initiated/received.
Longitude		X	Longitude generated when message is initiated or received.
MCC		X	Mobile Country Code of the network on which the message occurred.
MNC		X	Mobile Network Code of the network on which the message occurred.

8.10.12 Configuring General Device Activity Settings

Enable and configure device activity data collection by configuring the Afaria Administration console.

Procedure

1. In the Afaria Administration console, on the *Server* page, select *Configuration* > *Component* > *Device Activity*.

2. On the General Settings tab, select *Enable Activity Collection*.
   If you do not want to start data collection at the next service restart, unselect *Enable Activity Collection*.
3. (Optional) To collect the phone numbers of remote devices, select *Collect Remote Party Phone Numbers*.
   This option is not applicable for Windows Phone devices.
4. (Optional) Select *Collect Subscriber Location Information*.
5. (Optional) Select *Prompt Subscriber for Activity Enrollment* and compose the enrollment notification for users to view on their devices.
   When device activity collection is enabled the first time, actual data collection begins after you restart the SAP Afaria Server service and the device successfully connects to the server.

8.10.13 Configuring Device Activity Settings for Roaming

Configure Afaria Device Activity International Roaming settings to notify users that their devices are in an international roaming state and additional charges may apply.

Context

You do not need to configure device activity settings to restart the Afaria server service unless you want to initiate device activity data collection.

Procedure

1. In the Afaria Administration console, on the Server page, select *Configuration* > *Component* > *Device Activity*.
2. On the General Settings tab, select *Enable Activity Collection*.
   If device activity is enabled, a notification appears on the device every time the device enters international roaming.
3. On the Roaming Settings tab:
   a. Select *Enable Roaming Notification*.
      This option is not applicable for Windows Phone devices.
   b. (Optional) Customize notification content.
   c. (Optional) To reduce the number of notifications when close to a roaming boundary, set the length of time a device must be in roaming status before a user receives a notification.
   d. Save changes.
   e. If you do not want to begin or resume device activity data collection at the next service restart, return to the General Settings tab and unselect *Enable Activity Collection*.

8.10.14 Configuring Device Activity Settings for Data Views

Customize how SAP Afaria Device Activity data appears in Data Views.

Procedure

1. In the Afaria Administration console, on the *Server* page, select *Configuration* > *Component* > *Device Activity*.
2. On the Data Views tab:
   a. In the Accounting Period area, set the start day in the month of the current and previous accounting periods.
   b. In the Threshold area, set the threshold fields for each type of activity in the local network while in a roaming state.
   c. In the Roaming Network area, set the percentage threshold value for each type of activity occurring in the local network while in a roaming state.
3. Save changes.

Example

Example: Enterprise mobile plan with prepaid activities for each subscriber each accounting period

Your enterprise mobile plan includes these prepaid activities, for each accounting period and for each subscriber:

- Local network:
  - 1000MB for data
  - 700 outgoing messages
  - Unlimited outgoing local calls
  - Unlimited incoming calls and messages
- Roaming:
  - 400MB for data
  - 500 messages (both outgoing and incoming)
  - 300 minutes for calls (both outgoing and incoming)

Set the threshold field for each activity accordingly. For example, enter 700 in the Number of Outgoing Messages field in the Local Network area; and “0” in the Total Outgoing Calls field in the Local Network. Incoming calls and messages in the local network are usually unlimited prepaid activities. As a result, you do not need to set thresholds for those activities. The Roaming Network views show the percentage of the prepaid activities for each subscriber during the current or previous accounting period.

For example, if a subscriber has sent 350 messages while in the local network, the Msg Out % column of the Message Threshold Summary view shows 50%.

To flag subscribers who are about to exceed the prepaid activities allowed by your enterprise mobile plan, set the percentage value for each activity to 95%.

The Exceed Threshold Summary view lists all subscribers who have exceeded 95% for any of the prepaid activities. A subscriber who has exceeded the percentage threshold for one kind activity but not for all

others, continues to appear in the Exceed Threshold Summary view. The Activity threshold views show the percentage of the prepaid activities that each subscriber has carried on during either the current or previous accounting period. For example, if a subscriber has sent 350 messages while in the local network, the Msg Out % column of the Message Threshold Summary view shows 50%.

8.10.15 Enabling Device Activity Cleanup

You can use the Afaria Administration console to configure how the SAP Afaria Server removes old device activity data.

Procedure

1. In the Afaria Administration console, on the Server page, select *Configuration* > *Component* > *Device Activity*.
2. On the Cleanup Settings tab:
   a. Select *Enable Activity Cleanup*.
   b. (Optional) Set the number of days to keep device activity data before it is removed from your system.

   When device activity cleanup is enabled, the SAP Afaria Server automatically removes old device activity data at the time of the default schedule (12:00 a.m. every day) or at the time specified in your custom device activity cleanup schedule.

8.10.16 Customizing Device Activity Cleanup Schedule

Customize the date and time at which the SAP Afaria Server deletes old device activity data.

Context

The device activity cleanup schedule applies to all tenants with device activity cleanup enabled.

Procedure

1. In the Afaria Administration console, on the Server page, select *Configuration* > *Server* > *Schedule*.
2. Click *Edit connection rule* to open the Schedule Editor.
3. Specify your schedule settings.

4. (Optional) On the *Range* tab, specify a date range for the schedule.
5. (Optional) On the *Rate* and *Repeat* tabs, set the schedule to run on a recurring basis.
6. Click *Save*.
   When Activity Cleanup is enabled, SAP Afaria removes old device activity data at the time and frequency you have set in your schedule.

8.10.17 Latitude and Longitude Definitions

Definitions for longitude and latitude data collection values.

Latitude and Longitude columns appear in the Location view in the device activity data view.

Value	Definition
<longitude > <latitude>	Last retrieved approximate longitude and latitude of the device, based on crowd-sourced Wi-Fi hotspot and mobile cell tower location. Level of accuracy varies by device type. For iOS and Android, accuracy requested is 1km (0.62 miles).
Unknown	The location of the device is temporarily unknown.
Disabled	Location services are disabled on the device.
Not Collected	Collection of subscriber location information is disabled on the Device Activity General Settings tab of the Afaria Administration console.
Unsupported	The device does not support location services.

8.11 Configuration for Alerts

Alerts increase the visibility of system event that may require your attention.

8.11.1 Acknowledging an Alert

Acknowledge an alert raised to inform others that the alert has been noticed and is being worked on.

Context

Acknowledging an alert does not close it; acknowledging lets others know that steps are being taken to resolve the alert. Acknowledging the alert stops any response that was defined for the alert, such as paging or sending e-mail to a contact.

Procedure

1. On the Server > Alert page, select *Raised Alert* tab to view the list of alerts raised.
2. Select the alert and click *Acknowledge* on the top toolbar.
3. In the confirmation dialog box, click *Yes, Continue* to acknowledge the alert.
   The state of the alert changes from Unacknowledged to Acknowledged.

8.11.2 Deleting an Alert

Delete an alert to remove it from the list of raised alerts when no further action is required on the alert. You can delete either an acknowledged alert or an unacknowledged alert.

Procedure

1. On the *Server* > *Alert* page, select *Raised Alert* tab to view the list of alerts raised.
2. Select the alert and click *Delete* in the top toolbar.
3. (Optional) In the Server alert > Delete raised alert dialog box, enter any comments you have about deleting the alert.
4. Click *OK*.
   The alert is deleted from the raised alerts list. The deleted alert details are available in the Alerts Log.

8.11.3 Viewing Pending Alerts

View alerts for which at least one associated event has occurred.

Context

Alerts having multiple associated events can cause pending alerts, when any one of the events associated with the alert occurs.

Procedure

1. On the *Server* > *Alert* page, select *Pending Alert* tab to view the list of alerts that are pending.
2. (Optional) To view additional details related to a pending alert, select the alert and click *Inspect* on the top toolbar.

8.11.4 Creating an Alert Definition

Create an alert to define the events and actions related to the alert.

Prerequisites

Before creating an alert, create alert contacts, configure alert response addresses for messages to contacts and for sending SNMP traps to IP addresses.

Context

No alerts will appear on the Raised Alerts page until you have defined and enabled them.

Procedure

1. On the *Server* > *Alert* page, select *Defined Alert* tab to view the list of alerts defined.
2. On the top toolbar, click *New* to open the Add alert dialog.
3. On the Alert properties page, define an alert's general properties, such as name and priority, and enable the alert, if required.
4. On the Assigned events page, assign events that raise the alert by selecting one or more events from the Available events list and click *Add*.

   You can specify any combination of system-defined and user-defined events to trigger an alert.

   You can remove an event from the Assigned events list by selecting it in the Assigned events list box and clicking *Remove*.
5. On the Alert response page, indicate how you want the server to respond when an alert is raised.

   You can select any of the following options:
   - To contact a person, select the contact name and specify the message to deliver to e-mail or pager.
   - To send an SNMP trap to a server, select *Send SNMP trap*.
   - To run an executable file, browse and select the file.
6. (Optional) On the Alert threshold page, specify the number of times an event or set of events must occur during a certain time period to raise an alert.

   Select Unlimited to raise the alert if the number is met, without regard to the time period.
7. (Optional) On the Alert response repeat interval page, specify how often you want the system to repeat the response until the alert is acknowledged and the number of times to repeat the response.
8. Click *Save*.

8.11.5 Creating a Contact for Alerts

Create a contact who is responsible for handling raised alerts.

Procedure

1. On the *Server* > *Alert* page, select *Defined Contact* tab to view the list of contacts.
2. Click *New* in the top toolbar.
3. Enter the contact details such as name, pager or mobile number, and e-mail address.
4. Click *Save*.

8.11.6 Configuring an Alert Response

Configure an alert response to designate the mail server where your contacts reside or the IP address where you can forward SNMP traps.

Context

You can configure alert responses from any of the following pages: Defined Alert, Defined Event, or Defined Contact.

Procedure

1. On the *Server* > *Alert* page, select *Defined Alert*, *Defined Event*, or *Defined Contact* tab.
2. Click *Configure alert response* on the top toolbar.
3. In the Server Alert > Configure alert response dialog box, specify a host name for the mail server, or enter an IP address for forwarding SNMP traps.
4. Click *OK*.

8.11.7 Viewing Defined Events

View the system-defined and user-defined events on the system.

Context

Defined Events page displays the event details such as event name, description, and the component associated with the event. A component indicates a general category for grouping events based on a functional area of the product.

Procedure

1. On the *Server* > *Alert* page, select *Defined Event* tab to view the list of alerts.
2. (Optional) To view the alert associated with an event, select the event and click *Inspect assigned alert* on the top toolbar.

8.11.8 Creating a New Event for Configuring an Alert

Create custom events to trigger alerts in the system.

Context

You can define events that work alone or together with other system-defined events to trigger an alert on your system. Any event you define on your server appears as "User-defined."

Procedure

1. On the *Server* > *Alert* page, select *Defined Events* tab to view the list of alerts defined.
2. Click *New* in the top toolbar.
3. Enter the event details such as a unique event name and description.

   The component field displays the default value "User-Defined." You cannot edit this value.
4. Click *Save*.

8.12 Configuration for Session Policies

For session policies, the Afaria Administration console lets you define system-wide parameters, such as bandwidth throttling, file compression, file differencing, failed session cleanup, and session authentication.

If you change any values, you must stop and restart the SAP Afaria server for the changes to take effect.

8.12.1 Configuring Bandwidth Throttling

Configure bandwidth throttling to increase or decrease the communications rate allowing device users to run other network applications more effectively when they communicate with the Afaria server.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Communication* > *Bandwidth Throttling*.
3. Select *Enable bandwidth throttling* and its associated settings to enable bandwidth throttling on the server.
   - Enable calibration – select to modify configuration parameters without having to stop and restart the server service in order for changes to take effect. Enabling calibration also causes the server to log bandwidth throttling information to the Messages log at the end of a session.
   - Enable event logging – select to enable bandwidth throttling events to associate with alert definitions.

   In a server farm, enable throttling on all servers.
4. Select a configuration using the drop-down menu in *Configurations* or create a new configuration by clicking *New*.

   Using a bandwidth configuration set at 14.6 Kbps, in conjunction with 10-minute or greater channel delivery segmentation criteria, may result in dropped connections.
5. In Client throughput, specify the minimum and maximum throughput rate by entering numerical values in the fields.
6. In Throttle down, specify percentages and times by entering numerical values in the Threshold, Wait time, and Percent fields.

   > ⚠ Caution
   >
   > If you enter a value of 0 (zero) in the Percent field, bandwidth throttling never occurs.
7. Click *Save*.

8.12.2 Configuring for File Compression

Compress session channel files to reduce connection times for sessions that include file transfers.

Context

> **i** Note
>
> Android devices do not support compression.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Communication* > *Compression*.
3. Configure and manage the compression cache.
   - Size – specify the percentage of disk space allocated.
   - Remove files from compression cache if the source file is not found during a compression refresh – select to delete files from the list of files that Afaria attempts to cache when Afaria cannot find the file during a refresh action.
     It is recommended that you store your cached files locally when using this option in order to prevent occurrences of network access outages from unintentionally causing Afaria to delete files that you would prefer to keep.
   - Show – select to view the list of files or add files to the compression cache.
   - Refresh – select to reload the files in the list.

   > **i** Note
   >
   > Adding files to compression and differencing caches can be a slow process.
4. Click *Save*.

8.12.3 Configuring File Differencing

Use file differencing to maintain different versions of files that you frequently send to Afaria devices, which reduces connection times for sessions that include the stored files.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Communication* > *Differencing*.
3. Configure and manage the differencing cache.
   - Size – specify the percentage of disk space allocated.
   - Remove files from differencing cache if the source file was not found during a differencing refresh – select to delete files from the list of files that Afaria attempts to cache when Afaria cannot find the file during a refresh action.
     It is recommended that you store your cached files locally when using this option in order to prevent occurrences of network access outages from unintentionally causing Afaria to delete files that you would prefer to keep.
   - Show – select to view the list of files or add files to the differencing cache.
   - Refresh – select to reload the files in the list.
4. Click *Save*.

8.12.4 Configuring Failed Session Cleanup

Configure the automatic cleanup to recover sessions that were interrupted, or force a channel to restart from the beginning by configuring the manual cleanup.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Failed Session Cleanup*.
3. Set the Automatic Cleanup by entering a numeric value and choosing the unit of time from the drop-down menu.
4. If a channel continues to fail, use the Manual Cleanup by clicking *Show List*.
   a. Select a channel and click *Delete*.
   b. Click *Save*.
      The channel restarts during the next session.
5. Click *Save*.

8.12.5 Configuring Authentication and Assignments for Sessions

For running session channels with user authentication and group validation security, configure user authentication and user group assignment timeouts.

Context

On the *Server* > *Configuration* > *Security* page, the Device Approval and Domain areas are used for other tasks.

A typical timeout value for both authentication and assignments is 30 days.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Server* > *Security*.
3. In the Authentication area, select *Enable authentication* to enable authentication for session channels.
4. (Windows and Windows Mobile only.) To specify the amount of time an authentication cookie is valid, set the Authentication Timeout and Auto renew period.
5. In the Assignment area, specify the amount of time the user group assignments cookie remains valid, by setting the Assignment Timeout.
6. Click *Save*.

8.12.6 Configuring User Defined Field

Define or remove user defined fields in your Afaria database.

Procedure

1. On the Server page, on the left toolbar, click *Configuration* > *Server* > *User Defined Field*.
2. Click *Add column*.
3. Enter the column name and select the type:
   - Integer
   - Float – a floating point decimal)
   - Date/Time

- Varchar – a variable length string

4. Click *OK*.
5. To delete a user defined field, select one and click *Delete selected column*.
6. Click *Yes, Continue*.

9 Session Channel Reference

Session channels are selected in session policies and let you to perform a variety of scripted tasks on Afaria devices.

Create session channels using the Afaria Channel Administrator, then select them in session policies. In addition to sending and retrieving files, you can perform system tasks such as disk maintenance, registry updates, and script execution. You can also utilize control flow logic to condition task execution.

Device types supported are:

- Windows Mobile Professional
- Windows Mobile Standard
- Windows
- Android

9.1 Afaria Channel Administrator

From the Afaria server desktop, click *Start* > *Programs* > *Afaria* > *Afaria Channel Administrator* to create and publish session channels for selection in session policies.

9.2 Create or Edit a Session Manager Channel

Create or edit session channels to provide custom, systems-management channels that send and receive data, execute programs, and more, during a session between the device and a server.

- Create a channel – on the toolbar click *File* > *New Channel* > *Session Manager Channel* to launch the channel wizard. The wizard guides you through the channel creation process, and then opens the channel editor.
- Edit a channel – in the left pane, right-click a channel and click *Edit* to open the channel editor

To deploy a channel to devices, publish it, add it to a session policy, and link the policy to a group.

9.3 Session Manager Channel Editor

The Session Manager Channel Editor opens when you create or edit a Session Manager channel. The editor uses a tri-pane window view that includes a channel tree, a results page, and a toolbar to allow you to create or edit a channel.

9.4 Assignments View – Default View

Assignments view is the default view when you create or edit a Session Manager channel. It displays any worklist and sendlist objects associated with the selected channel. Select any channel in the channel tree to open the Channels view. The channel you are creating or editing is in edit mode, while any channel listed in the "Other channels" folder is in read-only mode.

The assignments view contains worklist and sendlist objects associated with the selected channel.

- Worklist – perform file and directory management, notifications, and system registry management tasks.
- Sendlist – worklists that are optimized for file transfer. Much of the session processing happens before the connection occurs, so using a sendlist can result in shorter connection times. Sendlists are very limited in the events that are available however, and should only be used when you only want to send files to a client.

9.5 Filter the View

Assignments view allows you to the view to include all worklist and sendlist objects, sendlists only, or worklists only. Filter the view by selecting a filter from the View drop-down list.

9.6 Channels View

Channels view displays all defined Session Manager channels. Select the Session Manager Channels item in the left pane of the editor to open the Channels view. The results pane lists all the Session Manager channels.

9.7 Events View

Worklists and sendlists contain events. When you select a worklist or sendlist in the left pane of the editor, Events view displays in the right pane, with the adjacent event list. This view lists all of the events contained in the selected object. Objects that do not contain any events appear blank. Events listed define the task order and details associated with that object.

The event list displays all Session Manager events. For worklists, all events in the event list are valid selections and display in full color. For sendlists, only events that are valid for sendlists display in full color and are available for use.

9.8 Create a New Worklist or Sendlist for a Channel

After you create the session channel, you'll define instructions to execute during a connection with a client or as part of a session. These instructions are called worklist or sendlist objects.

- Worklist – perform file and directory management, notifications, and system registry management tasks.
- Sendlist – worklists that are optimized for file transfer. Much of the session processing happens before the connection occurs, so using a sendlist can result in shorter connection times. Sendlists are very limited in the events that are available however, and should only be used when you only want to send files to a client.

> **i** Note
>
> The worklists and sendlists that you create and edit are objects that are independent from the session channel to which they're assigned, and therefore can be assigned to multiple channels for multiple device types. As independent objects, any change that you make to an object in one channel affects all other channels that include the same object assignment.

To add an object to a channel, click the *New worklist* or *New sendlist* button on the button bar. Their respective dialog boxes appear.

Enter the object's name and then click *OK*. The new object appears as a channel member in the left pane of the editor.

Any new worklist or sendlist object that you create is automatically assigned to the channel selected in the left pane of the editor. In addition, the new object is added to a master list of existing worklists and sendlists in the *Select objects* dialog box.

Existing worklists and sendlists can also be copied to create new worklists and sendlists. Save the duplicate with a new name, then modify its content using the Events view.

9.9 Assign a Worklist or Sendlist to your Channel

When you create a new worklist or sendlist, Session Manager automatically assigns it to your channel, but you can also assign any other Session Manager worklist and sendlist to your channel.

To assign an object from another channel to your channel, open the assignments view for your channel and click the Assign link to open the Select objects dialog box.

The Select objects dialog box displays all existing worklist and sendlist objects (up to a maximum of 5000) that are not currently assigned to your channel. You can assign any of these objects to your channel.

The View drop-down allows you to control the objects that display in the list. Display items from which you can choose include all worklist and sendlist objects, sendlists only, or worklists only.

To include a worklist or sendlist object in a channel, click the object name and then click OK, or double-click the object. To assign all objects at once, click the All objects link and then click OK. To assign multiple objects simultaneously, click the first object, press and hold *Ctrl* or *Shift* and then select the additional objects. The Select objects dialog box closes and the objects are added to Assignments for object view.

To clear a selected object, click anywhere on the dialog box.

9.10 Unassign Objects from your Channel

To unassign an object from your channel, select it in the assignments view and then click the Unassign link. Session Manager removes it from the view and returns it to the Select objects dialog box where it remains available for future assignments.

9.11 Add Events to a Worklist or Sendlist

Worklist and sendlist objects use events to perform actions during communication between the server and client. Afaria executes valid events and creates corresponding log entries. Invalid events are ignored and not captured in resulting logs.

There are several types of events. Some are valid for worklist objects only, while others are valid for both worklist and sendlist objects.

All events are categorized by the following function types:

- File/disk operations – events perform file-level data exchange, administration, and information gathering on the server and client.
- Variable – events manipulate placeholders whose contents you control and perform system registry tasks. You can use the predefined Session Manager variables or create your own user-defined variables. User-defined variables can be used in all worklists and sendlists contained within an individual channel.
- Session control – events govern how Session Manager structures and progresses through an object's list of events. These events include conditional statements and events that stop the worklist or sendlist, session, and connection.
- Miscellaneous – events display save file and message dialog boxes, execute programs, send commands to other computers, and run events in an external file.

To add an event to a worklist or sendlist, select the object in the left pane of the editor. Any event associated with that object displays in Events view. In the right pane, locate and then double-click the event to add and open the details dialog box for you to specify instructions for the event. The fields and options in the dialog box vary depending upon the event selected. You can also use Copy and Paste commands to copy events from one object to another.

> **i Note**
>
> The worklists and sendlists that you create and edit are objects that are independent from the channel to which they're assigned, and therefore can be assigned to multiple channels for multiple device types. As independent objects, any change that you make to an object in one channel affects all other channels that include the same object assignment.

> **i Note**
>
> Afaria does not validate events that you add to an object by using a Paste command. Adding invalid events to a sendlist object may have unpredictable results.

When the event is completely defined, click *OK* to close the Event details dialog box. The new event appears in the specified location in Events view.

Session Manager Channel Editor includes visual cues that you can use to flag or color events.

9.12 Display or Hide Event Flags

Flags are used to indicate that a special behavior is associated with an event. You can choose to display or hide event flags in Events view.

To display or hide event flags, open the event's context menu and choose *Show flags*. The event shifts to the right and any flag appears to the left of the event.

9.13 Set Event Colors

Session Manager allows you to define custom colors for different event types so that you can quickly determine the types of events in a worklist or sendlist.

To set event colors, open the event's context menu and choose *Set colors*. The Set colors dialog box appears. Click the Category drop-down arrow and select the type of category to which you want to assign a color; choices include: Client events, Comments, Control events, Get File from Client, Send File to Client, and server events. Click *New color* to access the standard Windows Color palette through which you select a predefined color or define a custom color to assign to the selected event type. When you click *OK* your color selection displays in the Sample box. Click *OK* to return to Events view. All events of the specified type display in the selected color.

9.14 Define Event Properties

Almost every event that you add to a worklist or sendlist opens its respective Event details dialog box. Use the fields and available options to set event parameters. Fields and options vary depending upon the event you add.

The following areas are common to most Event details dialog boxes:

- General event definition – basic event statement that may use directory and file names, variables, and wildcards.
- File comparison and transfer options – parameters for file handling.

- Options – parameters for additional file handling, conditional operation, and execution requirements.
- Execute – indicates whether the target for the event is the Afaria Server or the Afaria Client.
- Status – indicates whether the event is executed or ignored. You may want to disable events until you have them completely defined.

> **i Note**
>
> Simple events, like the IF event, will not open the Event details dialog box; however, once the event is added to your worklist or sendlist, you can access the dialog box by double-clicking the event in Events view.

9.15 Using Directory and File Names in Events

Many Session Manager events use path or file names as properties. However, filing systems and naming conventions vary on the clients, based upon operating system design of the device type. The sample text provided for most events represent DOS conventions.

Consider the following additional items when you use events that require directory or file names:

- Default paths – events that require a drive or path for a file name use the following default values:
  - Server – the predefined variable `<ServerInstallDir>` is the default installation path for Afaria Server, `C:\Program Files\Afaria`.
  - Client – the predefined variable `<ClientInstallDir>` is the default directory for Afaria Client, `C:\Program Files\AClient`.

  UNC – clients or servers on platforms using operating systems that support using Uniform Naming Conventions (UNC) paths may do so for directory and file names. Source files on a drive other than the local computer (server) must include UNC paths.

> **i Note**
>
> Refer to your device type's operating system reference documentation to gain understanding about its file and storage conventions.

9.16 Using Variables in Events

Variables in events are placeholders for different event parameters. Session Manager replaces the variable placeholders with the appropriate information when the event executes. Variables are always enclosed in "<>" characters and are not case sensitive. In other words, <time> is the same as <Time>.

To add a variable to an event specific field, place your cursor in the appropriate filed and the click the Show variables link on the Event details dialog box. In the Session variables box, double-clicking the variable adds it to the event, but you can also enter the variable in the appropriate fields.

> **i Note**
>
> When running an individual channel or a channel set in an Afaria session, if you create more than 256 variables in that session you will see the following error message:

> "Not enough storage is available to process this command"
>
> You may find it helpful to break up channels that create several variables into separate sessions.

The following table presents the four types of variables, as well as their respective format, description, and example.

Event Variable Types

Type	Format	Example	Description
Predefined variables	<variable>	<time>	Variables that are defined by Session Manager and display in the Session variables box.
User-defined session variables	<%variable>	<%MyVar>	Variables created using the Set Variable event. These are available to every worklist or sendlist in the channel in which they were created, but not across sessions.
Environment variables	<$variable>	<$TMP>	Variables that are system-defined values defined on the Environment property page in Control Panel.
Variable modifiers	<!modifier< variable >>	<!Drive<%MyVar>>	Modifiers that extract information from variables and parse a path.

9.17 Using Wildcards in Events

Wildcards are reserved characters that perform a task on multiple files with similar names or extensions. Instead of individually selecting many files and directories, a wildcard can reference these files or directories as a group. Afaria wildcards have the same behavior as those in the DOS and Windows operating systems.

The question mark (?) and asterisk (*) are two reserved characters used as wildcards for directory and file names.

- Use the question mark to represent a single character that a group of files or directories has in common.
- The asterisk represents one or more characters that files or directories have in common.

9.18 Event File Comparison and Transfer Properties

The File comparison and transfer options and Options group boxes in the Event details dialog box let you define the circumstances under which events execute.

Not all options are valid for all events. Valid options appear in solid or black text; inactive options appear dimmed. The following table lists most options and descriptions that appear on the Event details dialog box.

Event File Comparison and Transfer Properties

Property	Description
Check: If destination does not exist	Checks to determine if the target destination exists
Check: If source is newer	Checks a file to determine if the source file date stamp is newer than the destination file date stamp
Check: If source is different	Checks a file to determine if the source file date stamp is different than the destination file date stamp
Transfer: Always	Transfers a file regardless of source and destination date stamp
Transfer: If destination does not exist	Transfers a file even if the target destination does not exist
Transfer: If source is newer	Transfers a file if the source file date stamp is newer than the destination file date stamp
Transfer: If source is different	Transfers a file if the source file date stamp is different than the destination file date stamp
Use version information	Instructs the server to use file version differences to transfer files
Check/Send	Used with the Send File to Client event, compares a file at the client to a file on the server and then sends the file to the target (This option is used when you want to send the file to the staging area on the client, but also check the file in another location.)
Use safe transfer	Creates a destination file only when the file has been successfully transferred This option instructs the server to use a temporary file until the file transfer completes, and once complete, the server renames the temporary file to the destination file name. In unsuccessful transfers the temporary file remains hidden so that the transfer can continue if a retry is executed. Safe transfer ensures that no file corruption occurs because of an incomplete file transfer.
Turn compression off	Instructs the server to not compress files during transfer to the client.

Event File Comparison and Transfer Properties

Property	Description
Use file differencing	Instructs the server on how to use the differencing cache for sending files to the client. If a delta for a file exists in the Afaria Server's differencing cache for the file specified in the SENDFILE event, the file is sent from the differencing cache regardless of the "use file differencing" attribute setting. Use file differencing, enabled – Enabling this attribute will cause new file differencing deltas to be created and added to the differencing cache as part of the SENDFILE event execution. Use file differencing, disabled – Disabling this attribute does not create and add new file differencing deltas to the differencing cache as part of the SENDFILE event execution. Any existing file differencing delta files in the file differencing cache are used by the SENDFILE event.
Apply to directory only	Used with the Set File Attributes event to modifies directory attributes instead of file attributes

9.19 Event Options Properties

The File comparison and transfer options and Options group boxes in the Event details dialog box let you define the circumstances under which events execute.

Not all options are valid for all events. Valid options appear in solid or black text; inactive options appear dimmed. The following table lists most options and descriptions that appear on the Event details dialog box.

Options	Description
Delete after [-]	Deletes the source file after the file has been transferred
Make target path	Establishes a target path for the event and creates directories when necessary
Ignore hidden files	Instructs the server to ignore hidden files
Include subdirectories/subkeys	Includes subdirectories/registry key with the event
Conditional – True (&)	Executes the event only if the previously executed event was successful
Conditional – False (|)	Executes the event only if the previous event failed or was a "no execute"
Execution: Normal	Executes the event without special instructions

Options	Description
Execution: Not required for successful session [x]	Indicates that this event does not have to execute successfully for the server to log the session as successful
Execution: Channel critical event [+]	Terminates the Session Manager channel if this event fails
Execution: Session critical event [*]	Ends the session if this event fails

> **i** Note
>
> The condition status returned is based on the last event that executes. If an event is skipped, then no status is returned. A failure is an event that executes but does not finish successfully. Events that do not execute because of conditional options are not considered failures and do not terminate the session.

9.20 Import or Export Events

Session Manager allows you to import events that have been saved to a file into an existing worklist or sendlist, as well as export an event from a worklist of sendlist to a file in another location.

9.21 Import an Event

Select the object into which you want to import an event, then click Import events on the button bar.

The Open dialog box appears. (You can also right-click the event and choose Import events on the shortcut menu.) Navigate to the directory that contains the file that you want to import; the file will have an .evf extension. Select the file and then click Open. Session Manager adds the events from the imported file to the list of events in Events view.

> **i** Note
>
> Afaria does not validate events that you import into an object. Adding invalid events to a sendlist object may have unpredictable results.

9.22 Export an Event

To export an event from a worklist or sendlist to a file in another location, select the object that contains the event you want to export to file. In Events view, select the event to export then click Export events. The Save As

dialog box appears. (You can also right-click the event and choose Export events on the shortcut menu.) Navigate to the directory in which you want to export the selected event. In the File Name field, enter the name for the file and then click Save. Session Manager exports the file to the specified directory. You can choose to import this file to the same worklist or sendlist or another worklist or sendlist at a future time.

9.23 Optimize Channel Sessions

Although your channels sessions may be functional, you may want to fine-tune them to increase resource efficiency and decrease session completion time. You may find that the following methods optimize your channel's worklist and sendlist performance, and reduce connection time between the server and client.

Use the following strategies to optimize your channels:

- Use pre-processing tasks when possible
- Streamline remaining tasks
- Create worklist efficiencies

9.24 Pre-Processing Tasks

The single most important step that you can take to ensure that Session Manager processes events quickly and efficiently is to preprocess as much data as possible.

Preprocessing means that any task that can be performed on the client by the client should be completed before a session begins. Preprocessing should be used any time an event can be eliminated in this manner.

9.25 Streamline Remaining Tasks

The second class of session optimization is through optimization of the events that cannot be preprocessed.

- Use sendlists when possible. The best way to optimize events is to use sendlists whenever possible. The client checks an entire sendlist at one time. A worklist that includes a Send File to Client event typically has other events before or after the event, which forces Session Manager to perform multiple checks.
- Wildcards increase efficiency. Another way to ensure that processing occurs once, instead of many times, is through the use of wildcards. While an event with wildcards is expanded into several events at runtime, it's still faster than explicitly naming each file. With a wildcard, file status of the affected files can be checked at once in a manner similar to that for sendlists.
- File Status. Don't use the File Status event to check a file that's being transferred. Instead, use File Status to check for the existence of a flagged file.
- Conditional checks. Use the Set Variable event to avoid multiple File Status events and other conditional checks at the client. The first time a condition is checked, create a variable using the Set Variable event and reference that variable in subsequent worklists and sendlists. The Set Variable event does not send a command to the client and it can be used throughout the entire session.

9.26 Create Worklist Efficiencies

An efficient worklist has as few events as possible. In general, a worklist that has fewer events runs faster than a worklist that has more. Smaller worklists also use less memory and disk space.

- Comments. Each Comment event can include up to 251 characters, which may be several lines of text. Instead of creating five one-line Comment events, it's much more efficient to create one Comment event that contains five lines of text.
- Conditional attributes with event. Worklist events provide a Conditional True (&) and Conditional False (|) attribute. When enabled, the event executes based on the result of the last event, for example, an If true statement (containing a single event) can be replaced by the use of the Conditional true attribute, reducing the number of events required to complete the tasks.
- Delete after (-). Worklist events also provide a Delete after (-) attribute, which deletes the source file on the server or client after the file has been processed, for example, instead of using two events to get and delete a file at the client, you can accomplish the same task by using the Delete after (-) attribute.

9.27 Session Manager Events

Use events to perform actions during communication between the server and the device.

Afaria includes the following event types:

- File/disk operations – file-level data exchange, administration, and information gathering on the server and client.
- Variable use – manipulate placeholders for content you control and perform system registry tasks. You can use the predefined Session Manager variables or create your own user-defined variables All worklists and sendlists contained within an individual channel can use user-defined variables.
- Session control – govern how Session Manager structures and progresses through an object's list of events. Includes conditional statements and events that stop the worklist or sendlist, session, and connection.
- Miscellaneous – actions such as using a message dialog box, inserting events from other work objects, and executing programs.

> **i Note**
>
> Not all events are viable for all types of devices even though the Session Manager Channel Editor allows you to add any event to any worklist.

> **i Note**
>
> All Afaria session event parameters are subject to a 256-character maximum length requirement.

9.28 Windows Clients and Afaria Events

Afaria Windows devices are supported for many of the Afaria features. As is the nature of device management in general, and Afaria components in particular, successful operations depend in part on your understanding of how the Windows device is designed to operate in the Afaria environment.

See topic *Windows OS Variations and Afaria Operations*.

9.29 Session Event Summary

Events run on the server or a device. Some events may not support all device types.

The summary tables compare each Afaria event and its attributes to the Afaria server and each of the Afaria session devices to indicate whether the event is supported.

Key:

- Server – Afaria server
- WIN – Windows
- WM Std – Windows Mobile Standard
- WM Pro – Windows Mobile Professional
- Android – Android

9.29.1 File/Disk Operations Events Summary

Session manager events let you build worklists and sendlists.

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
Append File	—	Yes	Yes	Yes	Yes	Yes
	Delete after (-)	Yes	Yes	Yes	Yes	Yes
	Make target path	Yes	Yes	Yes	Yes	Yes
	Include subdirectories	Yes	Yes	Yes	Yes	Yes
	Conditional	Yes	Yes	Yes	Yes	Yes
	Execution: Normal	Yes	Yes	Yes	Yes	Yes
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	Yes

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	Yes
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	Yes
Check File	—	Yes	Yes	Yes	Yes	No
	Check: If destination does not exist	Yes	Yes	Yes	Yes	No
	Check: If source is newer	Yes	Yes	Yes	Yes	No
	Check: If source is different	Yes	Yes	Yes	Yes	No
	Use version information	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Check Volume	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Copy File	—	Yes	Yes	Yes	Yes	No
	Make target path	Yes	Yes	Yes	Yes	No
	Ignore hidden files	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Include subdirectories	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Delete File	—	Yes	Yes	Yes	Yes	Yes
	Ignore hidden files	Yes	Yes	Yes	Yes	Yes
	Include subdirectories	Yes	Yes	Yes	Yes	Yes
	Conditional	Yes	Yes	Yes	Yes	Yes
	Execution: Normal	Yes	Yes	Yes	Yes	Yes
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	Yes
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	Yes
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	Yes
Directory Listing	—	Yes	Yes	Yes	Yes	No
	Make target path	Yes	Yes	Yes	Yes	No
	Ignore hidden files	Yes	Yes	Yes	Yes	No
	Include subdirectories	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
File Status	—	Yes	Yes	Yes	Yes	Yes
	Ignore hidden files	Yes	Yes	Yes	Yes	Yes
	Conditional	Yes	Yes	Yes	Yes	Yes
	Execution: Normal	Yes	Yes	Yes	Yes	Yes
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	Yes
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	Yes
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	Yes
Find File	—	Yes	Yes	Yes	Yes	No
	Ignore hidden files	Yes	Yes	Yes	Yes	No
	Include subdirectories	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Get File from Client	—	Yes	Yes	Yes	Yes	Yes
	Transfer: Always	Yes	Yes	Yes	Yes	Yes
	Transfer: If destination does not exist	Yes	Yes	Yes	Yes	Yes
	Transfer: If source is newer	Yes	Yes	Yes	Yes	Yes

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Transfer: If source is different	Yes	Yes	Yes	Yes	Yes
	Use version information	Yes	Yes	No	No	No
	Use safe transfer	Yes	Yes	Yes	Yes	Yes
	Turn compression off	Yes	Yes	Yes	Yes	Yes
	Use file differencing	Yes	Yes	Yes	Yes	Yes
	Delete after [-]	Yes	Yes	Yes	Yes	Yes
	Make target path	Yes	Yes	Yes	Yes	Yes
	Ignore hidden files	Yes	Yes	Yes	Yes	Yes
	Conditional	Yes	Yes	Yes	Yes	Yes
	Execution: Normal	Yes	Yes	Yes	Yes	Yes
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	Yes
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	Yes
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	Yes
Make Directory	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Remove Directory	—	Yes	Yes	Yes	Yes	No
	Include subdirectories	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Rename File	—	Yes	Yes	Yes	Yes	Yes
	Make target path	Yes	Yes	Yes	Yes	Yes
	Ignore hidden files	Yes	Yes	Yes	Yes	Yes
	Include subdirectories	Yes	Yes	Yes	Yes	Yes
	Conditional	Yes	Yes	Yes	Yes	Yes
	Execution: Normal	Yes	Yes	Yes	Yes	Yes
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	Yes
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	Yes
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	Yes
Send File to Client	—	Yes	Yes	Yes	Yes	Yes
	Transfer: Always	Yes	Yes	Yes	Yes	Yes
	Transfer: If destination does not exist	Yes	Yes	Yes	Yes	Yes
	Transfer: If source is newer	Yes	Yes	Yes	Yes	Yes
	Transfer: If source is different	Yes	Yes	Yes	Yes	Yes
	Use version information	Yes	Yes	No	No	No
	Check/Send	Yes	Yes	Yes	Yes	Yes
	Use safe transfer	Yes	Yes	Yes	Yes	Yes

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Turn compression off	Yes	Yes	Yes	Yes	Yes
	Use file differencing	Yes	Yes	Yes	Yes	Yes
	Delete after [-]	Yes	Yes	Yes	Yes	Yes
	Make target path	Yes	Yes	Yes	Yes	Yes
	Ignore hidden files	Yes	Yes	Yes	Yes	Yes
	Include subdirectories	Yes	Yes	Yes	Yes	Yes
	Conditional	Yes	Yes	Yes	Yes	Yes
	Execution: Normal	Yes	Yes	Yes	Yes	Yes
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	Yes
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	Yes
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	Yes
Set Client Time	—	No	Yes	No	No	No
	Conditional	-	Yes	-	-	No
	Execution: Normal	-	Yes	-	-	No
	Execution: Not required for successful session [x]	-	Yes	-	-	No
	Execution: Channel critical event [+]	-	Yes	-	-	No
	Execution: Session critical event [*]	-	Yes	-	-	No
Set File Attributes	—	Yes	Yes	Yes	Yes	No
	Read Only	Yes	Yes	Yes	Yes	No
	System	Yes	Yes	Yes	Yes	No
	Hidden	Yes	Yes	Yes	Yes	No
	Archive	Yes	Yes	Yes	Yes	No
	Normal	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Apply to directory only	Yes	Yes	No	No	No
	Ignore hidden files	Yes	Yes	Yes	Yes	No
	Include subdirectories	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Wait for File to Exist	—	Yes	Yes	Yes	Yes	No
	Delete after (-)	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No

9.29.2 Variable Events Summary

Session manager events let you build worklists and sendlists.

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
Create Registry Key	—	Yes	Yes	Yes	Yes	No
	Make target path	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Delete Registry Key	—	Yes	Yes	Yes	Yes	No
	Include subkeys	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Delete Registry Value	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Delete Variable File	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Get Database Field	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Get Registry Value	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Get Script Variable	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Increment Variable	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Read Variable File	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Release Script	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Run Script Function	—	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Search Registry	—	Yes	Yes	Yes	Yes	No
	Include subkeys	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Set Database Field	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Set Registry Value	—	Yes	Yes	Yes	Yes	No
	Make target path	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Set Script Variable	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Set Variable	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Test Variable	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Update Variable File	—	Yes	Yes	Yes	Yes	No
	Make target path	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No

9.29.3 Session Control Events Summary

Session manager events let you build worklists and sendlists.

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
Comment	—	Yes	Yes	Yes	Yes	No
Disconnect	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Else	—	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
End If	—	Yes	Yes	Yes	Yes	No
End Quota	—	Yes	Yes	Yes	Yes	No
End Repeat	—	Yes	Yes	Yes	Yes	No
End Session	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
End Work Object	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
If	—	Yes	Yes	Yes	Yes	No
Quota	—	Yes	Yes	Yes	Yes	No
Repeat	—	Yes	Yes	Yes	Yes	No

9.29.4 Miscellaneous Events Summary

Session manager events let you build worklists and sendlists.

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
Append Channel	—	Yes	No	No	No	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Delete after (-)	No	-	-	-	No
	Make target path	No	-	-	-	No
	Include subdirectories	No	-	-	-	No
	Conditional	No	-	-	-	No
	Execution: Normal	Yes	-	-	-	No
	Execution: Not required for successful session [x]	Yes	-	-	-	No
	Execution: Channel critical event [+]	Yes	-	-	-	No
	Execution: Session critical event [*]	Yes	-	-	-	No
Check Memory	—	No	Yes	Yes	Yes	No
	Conditional	-	Yes	Yes	Yes	No
	Execution: Normal	-	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	-	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	-	Yes	Yes	Yes	No
	Execution: Session critical event [*]	-	Yes	Yes	Yes	No
Check Speed	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
End Impersonation	—	No	Yes	No	No	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
Execute Program	—	Yes	Yes	Yes	Yes	No
	Queued	Yes	No	No	No	No
	Do not wait	Yes	Yes	Yes	Yes	No
	Wait until completed	Yes	Yes	Yes	Yes	No
	Wait for < > mm:ss	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Impersonate User	—	No	Yes	No	No	No
	Conditional	-	Yes	-	-	No
	Execution: Normal	-	Yes	-	-	No
	Execution: Not required for successful session [x]	-	Yes	-	-	No
	Execution: Channel critical event [+]	-	Yes	-	-	No
	Execution: Session critical event [*]	-	Yes	-	-	No
Insert Channel	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Insert Worklist	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Load Script	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Message	—	Yes	Yes	Yes	Yes	Yes
	Conditional	Yes	Yes	Yes	Yes	Yes
	Execution: Normal	Yes	Yes	Yes	Yes	Yes
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	Yes
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	Yes
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	Yes
Notify Program	—	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Raise Event	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Reboot Client	—	No	Yes	Yes	Yes	No
	Conditional	-	Yes	Yes	Yes	No
	Execution: Normal	-	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	-	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	-	Yes	Yes	Yes	No
	Execution: Session critical event [*]	-	Yes	Yes	Yes	No
Set Bandwidth Throttling Config	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No

Event	Attribute	Server	WIN	WM Std	WM Pro	Android
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No
Test Group Membership	—	Yes	Yes	Yes	Yes	No
	Conditional	Yes	Yes	Yes	Yes	No
	Execution: Normal	Yes	Yes	Yes	Yes	No
	Execution: Not required for successful session [x]	Yes	Yes	Yes	Yes	No
	Execution: Channel critical event [+]	Yes	Yes	Yes	Yes	No
	Execution: Session critical event [*]	Yes	Yes	Yes	Yes	No

9.30 Session Manager Event Detail

Afaria events including their syntax and supported options.

9.30.1 Append Channel Event

The Append Channel event appends a channel or channel set to the end of a client's channel queue.

The channel runs during the current session if the session does not have cause to terminate before execution. If the session terminates before executing the channel, the channel remains in the queue for future execution.

Item	Description
Event Specific Fields	Channel or variable name – Channel or channel set name, or variable for the channel or set name to append.
Syntax	[Param 1] Channel or variable name. Example:Inventory\MyInvChannel or <%Var-Name>

Item	Description
Options	Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	A channel's name, in this context, is evaluated as its folder path plus the channel name. For example, a channel named "Hardware" stored in nested folders "Inventory \Windows" is evaluated as "Inventory\Windows\Hardware."
Returned Value	N/A

9.30.2 Append File Event

The Append File event appends the contents of one or more files to the end of another file.

Item	Description
Event Specific Fields	Source file name or wildcard. The path name, file name, or wildcard parameter for one or more files to be appended to the destination file. Click the Browse link to choose a server file, or enter the path name and file name in this field. Target file name. Specifies the name of the file to which the source file is being added. Click the Browse link to choose a file, or enter the path and file name in this field.
Syntax	[Param 1] Source file name. Example: C:\Docs*.* [Param 2] Target file name. Example: C:\DailyDocs\Daily.txt
Options	Delete after (-) Make target path Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]

Item	Description
Remarks	The Append event requires two parameters, source and destination file names. The event copies the entire contents of the source file to the end of the destination file. The destination file may or may not exist. The event fails if the source and destination are the same. For Windows clients and the server, the Append event allows both: - Append test.txt TO *.* - Append *.* TO test.txt Supports the "Make target path" option, which establishes a target path for the event and creates directories when necessary. The Append event adds disk I/O time, which is needed to process the command at the client. You may be able to save several minutes per session by letting the application do most of the heavy work and having all the data at the client ready before the session runs. When using wildcards, the "include subdirectories" option is used for the first parameter. Many source files in multiple subdirectories can be appended to a single destination file, but, a source file that is appended to a wildcard destination will not include subdirectories.
Returned Value	N/A

9.30.3 Check File Event

The Check File event compares the time, date, and file size of a server and client file, and is often used to test the state of a file before a transfer event.

Item	Worklist and Sendlist Objects
Event Specific Fields	Server file name. The drive, path, and file name of the server file to be compared with the client file. Click the Browse link to choose the server file, or enter the path and file name in this field. Client file name. Specifies the drive, path, and file name for the client file.
Syntax	[Param 1] Server file name. Example: C:\Doc\Daily.doc [Param 2] Client file name. Example: D:\Docs\ClientDaily.doc
File comparison and transfer options	Check: If destination does not exist Check: If source is newer Check: If source is different Use version information

Item	Worklist and Sendlist Objects
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.4 Check Memory Event

Use the Check Memory event to check available memory on a device.

Item	Description
Event Specific Fields	Memory device to check. The value returned (true or false) represents that the device has or does not have the specified location. Space needed. (Optional) Represents the value needed on the device type. The value that returns is true or false, representing that the device has or does not have the space needed.
Syntax	[Param 1] Type. Type values: 0 – Flash, default 1 – RAM 2 – Persistent storage 3 – Object code 4 – Transient 5 – Code stats
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	Value returned in the <CheckMemorySize> variable.

9.30.5 Check Speed Event

The Check Speed event checks the speed of the session connection.

Item	Description
Event Specific Fields	N/A
Syntax	N/A
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The <ConnectionSpeed> return value maintains accuracy for dial-up connections, but becomes distorted for LAN connections.
Returned Value	Value returned in the <ConnectionSpeed> variable, bits per second.

9.30.6 Check Volume Event

Use the Check Volume event to check a devices disk size.

Item	Description
Event Specific Fields	Volume to check. Used with the variable, the value returned (true or false) represents that the device has or does not have the specified location. Space needed. (Optional) Represents the value needed on the client device. The value that returns is true or false, representing that the device has or does not have the space needed.
Syntax	The syntax for the Windows Mobile client main storage is: \ (backslash). The syntax for the Windows Mobile client external storage card is: \SD Card or \Storage Card. (The exact syntax depends upon the name of the external storage on the specific device.)
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]

Item	Description
Remarks	This event supports disk sizes > 4 GB. Any valid path on the desired drive may be used as the volume parameter: — On NTFS drives, if the path is the name of a directory on a junction (mount) point, the returned data will be for the mounted volume, not the volume indicated by the drive letter.
Returned Value	Value returned in the <CheckDiskSize> or <VolumeSize> variable

9.30.7 Comment Event

The Comment event is a non-executable event used to add comments to a worklist or sendlist or to separate event blocks with a blank line.

Comment events are ignored at session execution time, but the comment text is displayed in Session Manager.

Item	Worklist and Sendlist Objects
Event Specific Fields	Text box. Enter the comment text (up to 251 characters, including line breaks) that you want inserted into the worklist or sendlist. The comment text may span several lines and may be longer than the display area in Events view.
Syntax	N/A
Options	N/A
Remarks	N/A
Returned Value	N/A

9.30.8 Copy File Event

The Copy File event duplicates one or more files to another file name or directory.

> **i** Note
>
> File attributes are not retained with this event.

Item	Description
Event Specific Fields	(Source) File name or wildcard. Specifies the path, file name, or wildcard parameters for one or more files to copy. Click the Browse link to choose a file if the event occurs on the server, or enter the path and file name in this field. This event is unsuccessful if the source file does not exist or if the wildcard parameter does not locate any files. (Target) File name. The path, file name, or directory for the file or directory that will receive the copied files. This value should be a file if the source field is a file, or a directory if the source field is a wildcard parameter.
Syntax	[Param 1] Source file name. Example: C:\Docs*.doc [Param 2] Target file name. Example: C:\DailyDocs*.sav
Options	Make target path Ignore hidden files Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the "Make target path" option. Target files, including any subdirectories, in the file spec that do not exist will be created. Supports the "Ignore hidden files" option, which instructs the server to ignore hidden files in events using wildcards. Supports a file exclusion mask, which appends a vertical bar, followed by a file specification to indicate the files to exclude from that operation. For example, to copy all files except .xls files from the "C:\Reports" directory, enter this command: COPY "C:\Reports*.*|*.xls" TO "D:\Backup\Reports*.*" Define multiple exclusions with multiple instances of the mask, such as "C:\Reports*.*|*.xls |*.txt". The Copy File event adds disk I/O time, which is needed to process the command at the client. You may be able to save several minutes per session by letting the application do most of the heavy work and having all the data at the client ready before the session runs.
Returned Value	N/A

9.30.9 Create Registry Key Event

The Create Registry Key event creates a new key in the registry.

Item	Description
Event Specific Fields	Root key\key1\keyN. The complete path and name of the key to be added.
Syntax	[Param 1] Registry path and key name. Example: HKLM\Software\Key
Options	Make target path Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the “Make target path” option. Target files, including any subdirectories, in the file spec that do not exist will be created. This event will fail if the parameter is not a valid registry path or if the specified key already exists. Windows CE does not ship with a registry editor but third party applications are available.
Returned Value	N/A

9.30.10 Delete File Event

The Delete File event permanently removes one or more files from the server or client.

Item	Description
Event Specific Fields	File name or wildcard. The path, file name, or wildcard parameter for one or more files to delete. Click the Browse link to set this field if the event occurs on the server, or enter the path and file name in this field.
Syntax	[Param 1]File name or wildcard. Example: D:\Docs*.doc

Item	Description
Options	Ignore hidden files Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the "Ignore hidden files" option, which instructs the server to ignore hidden files in events using wildcards. Supports a file exclusion mask, which appends a vertical bar, followed by a file specification to indicate the files to exclude from that operation. For example, to delete all files except .xls files from the "C:\Reports" directory, enter this command: DELETE "C:\Reports*.*|*.xls". Define multiple exclusions with multiple instances of the mask, such as "C:\Reports*.*|*.xls |*.txt". Don't include a drive letter on Windows CE clients. The Delete File event adds disk I/O time, which is needed to process the command at the client. You may be able to save several minutes per session by letting the application do most of the heavy work and having all the data at the client ready before the session runs.
Returned Value	N/A

9.30.11 Delete Registry Key Event

The Delete Registry Key event removes a key from the registry.

Item	Description
Event Specific Fields	Root key\key1\keyN. The complete path and name of the registry key to be deleted.
Syntax	[Param 1] Registry path. Example: HKLM\Software\Key
Options	Include subkeys Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]

Item	Description
Remarks	N/A
Returned Value	N/A

9.30.12 Delete Registry Value Event

The Delete Registry Value event removes a value from the registry.

Item	Description
Event Specific Fields	Root key\key1\keyN. The path for the registry value. [value name]. The name for the registry value.
Syntax	[Param 1] Registry path. Example: HKLM\Software\Key\Value [Param 2] Value name. Example: ValueName Leave [Param 2] blank to use the default value.
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	This event fails if the parameter is not a valid registry path or if the key from which the value would have been deleted does not exist.
Returned Value	N/A

9.30.13 Delete Variable File Event

The Delete Variable File event removes a value entry from a variable file (*.ini) on the server or client.

Item	Description
Event Specific Fields	File name. The path and file name of the file from which an entry is to be removed. Click the Browse link to choose a file, or enter the path and file name in this field. User variable name. The name of the user-defined variable for which the value entry is being removed.

Item	Description
Syntax	[Param 1] File name. Example: C:\Variables.ini [Param 2] User variable name. Example: <%[Section].VarName>
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.14 Directory Listing Event

The Directory Listing event copies the list of files in a directory into an output file on the server. The output text file has a similar format as a DOS DIR command.

Item	Description
Event Specific Fields	Server file name for output. Instructs the event to create a file at this location on the server. Enter the directory, path, and file name that will contain the directory listing. The event replaces the file if it already exists. Directory wildcard. Specifies the path or wildcard to use to get the directory listing. End the path with a backslash (\ ) to list the contents of a directory; otherwise, the event only lists the directory name.
Syntax	[Param 1] Server file name for output. Example: C:\Listings\Dirlist.txt [Param 2] Directory wildcard. Example: C:\DailyDocs*.sav

Item	Description
Options	Make target path Ignore hidden files Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the “Ignore hidden files” option, which instructs the server to ignore hidden files in events using wildcards. Supports the “Make target path” option. Target files, including any subdirectories, in the file spec that do not exist will be created. Supports a file exclusion mask, which appends a vertical bar followed by a file specification to indicate the files to exclude from that operation. For example, to perform a directory listing on all files except .xls files from the “C:\Reports” directory, enter this command:DIR LISTING “D:\Backup\Reports\List.txt” FROM “C:\Reports*.*|*.xls”. Define multiple exclusions with multiple instances of the mask, such as “C:\Reports *.*|*.xls |*.txt”.
Returned Value	N/A

9.30.15 Disconnect Event

The Disconnect event terminates the connection between the client and server, but all remaining server events will execute as defined.

Remaining client events do not execute and are marked with a special status to indicate that the session was disconnected.

Item	Description
Event Specific Fields	N/A
Syntax	N/A
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]

Item	Description
Remarks	N/A
Returned Value	N/A

9.30.16 Else Event

The Else conditional event is used in combination with an If event to control the execution of a block of events.

Item	Description
Event Specific Fields	N/A
Syntax	If <events> Else <alternate events>
Options	N/A
Remarks	N/A
Returned Value	N/A

9.30.17 End If Event

The End If conditional event is used in combination with other If events to control the execution of a block of events. Place the End If event at the very end of each If block to end the If clause.

Item	Description
Event Specific Fields	N/A
Syntax	If <events> EndIf or If<events> Else <alternate events>Endif
Options	N/A
Remarks	N/A
Returned Value	N/A

9.30.18 End Impersonation Event

The End Impersonation event is used in combination with the Impersonate User Event [page 213] to control the execution of a block of events.

Place the End Impersonation event at the very end of each Impersonate User block to define the end.Afaria releases the user security token that was in use for the block and reverts to the last-used token.

Item	Description
Event Specific Fields	N/A
Syntax	Impersonate User <events> End Impersonation
Options	N/A
Remarks	N/A
Returned Value	N/A

9.30.19 End Quota Event

One of two Quota events that wrap a block of file transfer events together by a specified time or byte limit in an individual session.

Using the Quota events, the server counts the time or bytes spent on the events that are wrapped by the Quota event, then stops processing the events when the defined time or byte limit is met, even if the limit is met during the middle of an individual file transmission. The next time that the client connects to the server, the server continues processing the wrapped events starting at the exact place in the events, or file, where it stopped in the previous session.

Item	Description
Server/client availability	
Event Specific Fields	N/A
Syntax	Quota <send events> End Quota
Options	N/A
Remarks	Worklist execution below the End Quota event resumes on two conditions: • The nested SEND events have completed. The flag file specified in the Quota event is created. • The quota is met or exceeded. Execution is passed to subsequent events once the last block is transferred. All necessary parameters for resuming uncompleted SEND events are set at this time.
Returned Value	N/A

9.30.20 End Repeat Event

The End Repeat conditional event is used with the Repeat event to mark the end of a Repeat block of events.

Place End Repeat events at the end of each Repeat event.

Item	Description
Event Specific Fields	N/A

Item	Description
Syntax	Repeat <events> End Repeat
Options	N/A
Remarks	N/A
Returned Value	N/A

9.30.21 End Session Event

The End Session event terminates the connection between the client and the server.

All remaining session events are marked “Not executed.” This event is useful for stopping execution in a specific condition, rather than continuing the operation.

Item	Description
Event Specific Fields	N/A
Syntax	N/A
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.22 End Work Object Event

The End Work Object event ends the currently executing worklist or sendlist.

This event terminates the connection between the client and the server when there are no more worklists and sendlists in the session. If there are more worklists and sendlists to be executed for the session, the next object in the list will be executed.

Item	Description
Event Specific Fields	N/A
Syntax	N/A

Item	Description
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.23 Execute Program Event

The Execute Program event provides similar capability as the DOS command line for running programs. This event launches the program via the information in the Command Line field.

Item	Description
Event Specific Fields	Command line. Enter the path and name of the application's executable file. Include command line options after the file name.
Syntax	[Param 1] Command line. Example: C:\WINNT\SYSTEM32\NOTEPAD.EXE
Execute options	Queued Do not wait Wait until completed Wait for < > mm:ss
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]

Item	Description
Remarks	To execute .bat files on the server, access the Services dialog box through and then stop the Server. Set the LogOn properties to allow the service to interact with desktop, then re-start the Server. To execute programs on a Windows Mobile client, you must enclose the executable within double quotation marks in the path to the parameter file that is the parameter, as in the example below “iexplore.exe”\windows\test.jpg
Returned Value	N/A

9.30.24 File Status Event

The File Status event determines whether a file exists at the specified location.

It also sets the <FileStatCount>, <FileStatVersion>, and <FileStatSize> variables. Use this event to set the conditional value to true or false, based on a file's presence. This event most often precedes a conditional event or an event with the Conditional option enabled.

To retrieve the total size of the contents of a directory using the path to the directory, such as File Status C:\temp, you must append wildcards to the end of the path, as in File Status C:\temp*.* If no wildcards are appended, then the <FileStatSize> variable returns zero.

Item	Description
Event Specific Fields	File name or wildcard. The Server attempts to locate a file at the specified path and file name. If the event occurs on the server, click the Browse link to choose the file.
Syntax	[Param 1]File name or wildcard. Example: D:\Docs*.doc
Options	Ignore hidden files Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.25 Find File Event

The Find File event locates the specified file or directory on the client or Server and sets the specified user variable to the full path for the specified file.

Item	Description
Event Specific Fields	User variable name. The user-defined variable for which the file path is being set. Starting path\file name or directory or wildcard. Enter the path and file name of the file or directory that marks the starting point for the search.
Syntax	[Param 1] User variable name. Example: <%MyVar> [Param 2] Starting path\file name or directory or wildcard. Example: C:\Winnt\Notepad.exe
Options	Ignore hidden files Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the “Ignore hidden files” option, which instructs the Server to ignore hidden files in events using wildcards. Supports the “Include subdirectories” option so that subdirectories of the [Param2] filespec will be searched. Supports a file exclusion mask, which appends a vertical bar followed by a file specification to indicate the files to exclude from that operation. For example, to find all files except .doc files with names that start with the letter “A” from the “D” drive, enter this command:FIND FILE <%FullPath> “D:*.doc|a*.doc”
Returned Value	N/A

9.30.26 Get Database Field Event

The Get Database Field event retrieves the value of a specified field in a specified table in the database.

Item	Description
Event Specific Fields	User variable name. The variable to receive the value of the database field. Variable or database field name. The variable or literal name of the field from which to retrieve the value. Table name. (Optional) The name of the database table if other than the User Defined Fields table (default). WHERE parameter. (Optional) The statement by which the system queries the table field if other than "DeviceGuid = '<ClientId>'" (default). ("DeviceGuid" represents the unique identifier for a client.)
Syntax	[Param 1] User variable name. Example: <%MyVar> [Param 2] Variable or database field name. Example: BATTLEVEL [Param 3] Table name. Example: A_INV_DEVICE [Param 4] WHERE parameter. Example: DeviceGuid = '<ClientId>'
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Handheld inventory tables may contain multiple rows for the same DeviceGuid. Only the first row in the result set based on [Param 4] will be used to read the field value. If an error occurs when attempting to "read" a field value in a database table, the system will retry once. If the retry fails, then the event fails and an error message is logged to Data views, Logs in Messages view.
Returned Value	N/A

9.30.27 Get File from Client Event

The Get File from Client event locates one or more files on the client and transfers them to the specified location on the server. File attributes are not retained with this event.

Wildcards used with this event retrieves a group of files whose names have something in common, or that are in the same directory.

> **i** Note
>
> Android devices do not support file compression.

Item	Description
Event Specific Fields	(Target) Server file name or wildcard. The path, file name, directory, or wildcard parameters for the file or directory that will receive the transferred file. Click the Browse link to choose a file or directory, or enter the path, file name, or directory in this field.
	A trailing backslash "\" will be accepted as an indication that the target is a subdirectory of the given path, as in C:\Program Files\Sample\Data\. If the target path does not include the trailing backslash, then an attempt will be made to treat the target as a directory, as if an implicit backslash. If such a target directory already exists or is created using the "Make target path" option, then transfer of one or more files to this directory should be successful. In the event that no such directory exists or is created, transfer of more than one file to the target path will fail; however, transfer of a single file to the target path will be successful, with the file assuming the name specified in the target. For example, sending C:\Daily.doc to the path C:\Program Files\Sample \Data (where Data is not the name of a directory and is not created) will result in the creation or overwriting of C:\Program Files\Sample\Data with the contents of Daily.doc. In all instances where multiple source files are targeted to a single destination file, the event is logged as an error. Selecting the "Make target path" option (explained on the next page), or the pre-existence of a designated directory will not prevent this error from occurring.
	(Source) Client file name or wildcard. Specifies the path, file name or wildcard parameters for the files to transfer.
Syntax	[Param 1] Server file name or wildcard. Example: C:\ServerDocs\Daily.doc [Param 2] File name or wildcard. Example: D:\Docs*.doc

Item	Description
File comparison and transfer options	Transfer: Always Transfer: If destination does not exist Transfer: If source is newer Transfer: If source is different Use version information Use safe transfer Turn compression off Use file differencing
Options	Delete after [-] Make target path Ignore hidden files Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the “Use safe transfer” option so that the Server does not create a destination file until it has been successfully transferred. Supports the “Make target path” option. Target files, including any subdirectories, in the file spec that do not exist will be created. Supports the “Ignore hidden files” option, which instructs the Server to ignore hidden files in events using wildcards. Supports a file exclusion mask, which appends a vertical bar followed by a file specification to indicate the files to exclude from that operation. For example, to get all files except .xls files from the “C:\Reports” directory, enter this command: GET “D:\Backup\Reports” FROM “C:\Reports*.*|*.xls”. Define multiple exclusions with multiple instances of the mask, such as “C:\Reports*.*|*.xls |*.txt”. Supports indirect files. Sets event-specific information in an ASCII file that is referenced in the event, rather than included.
Returned Value	N/A

9.30.28 Get Registry Value Event

The Get Registry Value event retrieves the value of a specified registry value on client or Server and makes it available in a specified user-defined variable.

Item	Description
Event Specific Fields	User variable name. The user-defined variable for which the registry value is being set. Root key\key1\keyN. The path for the registry value. [value name]. The name for the registry value.
Syntax	[Param 1] User variable name. Example: <%MyVar> [Param 2] Root key value. Example: HKEY_LOCAL_MACHINE\Software\Afaria\Name [Param 3] Value name. Example: ValueName Leave [Param 3] blank to use the default value.
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The system also accepts HKLM, HKCU, HKCR, and HKU as abbreviations, but it does not support binary values. This event is designed to read a string value. It will read a DWORD value, but it converts the DWORD value into a string value before including it in the session variable.
Returned Value	N/A

9.30.29 Get Script Variable Event

The Get Script Variable event retrieves the value of a global script variable.

To use this event, provide the name of the script variable, as well as the session variable name that will store the retrieved value from the client or Server.

Item	Description
Event Specific Fields	Script file name. The path and name of the file that contains the script variable. Click the Browse link to choose a file and directory, or enter the path and file name in this field. Script variable name. The name of the script variable. User variable name. The name of the session variable that will store the retrieved value.
Syntax	[Param 1] Script file name. Example: C:\Scripts\Myscript.vbs [Param 2] Script variable name. Example: MyVariable [Param 3] User variable name. Example: <%variable-name>
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The difference between running a script on the client versus the Server is that session variable support is limited to setting the variable. Client scripts cannot get the session variable. Accessing Afaria session variables through this event is not supported on the client.
Returned Value	N/A

9.30.30 If Event

The If conditional event controls the execution of a block of events in a session. A block of events begins with an If event and ends with an End If event. If the condition specified is true, then all events up to the next Else or End If event will execute.

Item	Description
Event Specific Fields	N/A
Syntax	N/A
Options	N/A

Item	Description
Remarks	Supports the following conditions: • If Previous Event FALSE • If Previous Event TRUE • If (LValue) <, <=, =, >=, > (RValue) where LValue and RValue can be session variables, numbers, or strings The <, >, <=, and >= operators in Session Manager events compare only integers or strings. The first non-numeric character terminates comparisons of integers. For example, the statement 128.46.22.8 >= 128.56.22.8 would return as "True" because the comparison stops at the decimal point (non-numeric character) following 128.
Returned Value	N/A

9.30.31 Impersonate User Event

This event uses the corresponding End Impersonation Event [page 202] to control the user context for executing a block of events in a session.

The event uses the Windows API LogonUser call with a specified Domain/Username and password to obtain a security token. The event then uses the token when calling the Windows API ImpersonateLoggedOnUser and RevertToSelf calls to execute any of the following events:

- Append event
- Check File event
- Check Volume event
- Copy File event
- Create Registry Key event
- Delete File event
- Delete Registry Key event
- Delete Registry Value event
- Delete Variable File event
- Directory Listing event
- Execute Program event
- Files Status event
- Find File event
- Get File from Client event
- Get Registry Value event
- Load Script event
- Make Directory event
- Read Variable File event
- Remove Directory event
- Rename File event
- Search Registry event
- Set File Attributes event

- Set Registry Value event
- Update Variable File event
- Wait for File to Exist event

This event has no effect on the Load Script Event [page 216], other than it uses the security token to gain access to the script file. The user context for executing the script file is not controlled by the Impersonate User event.

Afaria events that do not rely on user credentials to operate, operate as they normally would inside the Impersonate User block.

Item	Description
Event Specific Fields	User Name. User to impersonate. Password. Password associated with the user name. Confirm password. Password associated with the user name.
Syntax	[Param 1] User Name. Example: UserName or Domain\User-Name [Param 2] Password: password [Param 3] Confirm Password: password
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Event nesting is valid. Password characters display as "*". Event execution skips to the corresponding End Impersonation event when the Impersonate User event fails.
Returned Value	N/A

9.30.32 Increment Variable Event

The Increment Variable event modifies the value of the specified user variable by the specified amount (positive or negative).

Item	Description
Event Specific Fields	User variable name. The user-defined variable to be incremented by the specified amount. Amount. The positive or negative amount by which the variable is to be incremented.
Syntax	[Param 1] User variable name. Example: <%MyVar> [Param 2] Amount. Example: 100
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Increment amounts must be positive or negative whole numbers with no separator characters, such as 5000, not 5,000. The lowest number to which a variable can be incremented is -2147483648, while the highest number is 2147483647.
Returned Value	N/A

9.30.33 Insert Channel Event

The Insert Channel event allows you to insert an existing Session Manager channel into the currently selected worklist.

Item	Description
Event Specific Fields	Click the *Select Channel link* to access the Session Manager Channels dialog box. Use this dialog box to choose the Session Manager channel to insert into the worklist.
Syntax	[Param 1] Session Manager channel name. Example: \$root$\Locked Channel
Server/client availability	
Remarks	N/A
Returned Value	N/A

9.30.34 Insert Worklist Event

The Insert Worklist event allows you to insert one or more events from an external worklist file into a worklist's list of events.

Item	Description
Event Specific Fields	Worklist file name or @indirect file. The name of the file that contains the worklist file. Click the Browse link to choose the file, or enter the file name in this field. Indirect files must use the @ symbol before the file name.
Syntax	[Param 1] Worklist file name or @indirect file. Example: C:\Events\Insert.evf or @C:\Indirect\Insert.ind
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports indirect files. Sets event-specific information in an ASCII file that is referenced in the event, rather than included.
Returned Value	N/A

9.30.35 Load Script Event

The Load Script event initiates the script engine, reads the script file and parses the script text, and then connects the script to the script engine in order that the script be available for other session events.

To use this event, provide the name of the script file, as well as the script type (VBScript or JScript) to be run at the client or Server.

Item	Description
Event Specific Fields	Script file name. The path and name of the script file. Click the Browse link to choose a file and directory, or enter the path and file name in this field. Script language. The name of the script language (VBScript or JScript). **i Note** To use a script engine other than VBScript or JScript, enter the name directly in the Script language field.

Item	Description
Syntax	[Param 1] Script file name. Example: C:\Scripts\Myscript.vbs [Param 2] Script language. Example: JScript **i Note** We do not support using this event to display message box UI.
Remarks	Accessing Afaria session variables through this event is not supported on the client.
Returned Value	N/A

9.30.36 Make Directory Event

The Make Directory event creates a new client or Server directory. As part of a sendlist object, this event creates the directory only if necessary.

Item	Description
Event Specific Fields	Directory path. Specifies the path and directory name of the new directory.
Syntax	[Param 1] Directory path. Example: C:\Dir1\Dir2\Dir3
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.37 Message Event

The Message event displays a message in the status dialog at the client, or logs a message to the Messages and Session views in Data views, Logs.

Item	Description
Event Specific Fields	Message text or @indirect file. Specifies the text of the message to display, or the name of the file that contains the message text.

Item	Description
Syntax	[Param 1] Message text or @indirect file. Example: This is a message or @C:\Messages\Message.txt
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports indirect files. Sets event-specific information in an ASCII file that's referenced in the event, rather than included.
Returned Value	N/A

9.30.38 Notify Program Event

The Notify Program event sends a message to the specified named pipe or mailslot on the server.

Item	Description
Event Specific Fields	Server named pipe or mail slot. Specifies the pipe name or mailslot to be notified on the server. Notify text or @indirect file. Specifies the text of the message to send, or the name of the file that contains the message text.
Syntax	[Param 1] Server named pipe or mail slot. Example: pipe\name or mailslot\name [Param 2] Notify text or @indirect file Example: This is a notification or @C:\Notify\Notify.txt
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]

Item	Description

Remarks	Supports indirect files. Sets event-specific information in an ASCII file that's referenced in the event, rather than included.
	
	The requirements for a named pipe server that can work with the Notify event are as follows:
	
	• The named pipe must be created as bi-directional.
	• XComms.exe will open the pipe, write message data (not byte data), and will close it for each Notify event.
	• XComms.exe is expecting a Windows return code (DWORD) to come back as a response. If everything was successful, this value will be "0".
	• Pseudo-code for this event using the Windows API function names is CreateNamedPipe.
	• Loop the following as long as you want the pipe to accept information:
	  ○ ConnectNamedPipe
	  ○ ReadFile (message)
	  ○ WriteFile (return code)
	  ○ DisconnectNamedPipe

Returned Value	N/A

9.30.39 Quota Event

One of two Quota events that wrap a block of file transfer events together by a specified time or byte limit in an individual session.

Using the Quota events, the Server counts the time or bytes spent on the events that are wrapped by the Quota event, then stops processing the events when the defined time or byte limit is met, even if the limit is met during the middle of an individual file transmission. The next time that the client connects to the server, the Server continues processing the wrapped events starting at the exact place in the events, or file, where it stopped in the previous session.

> **i** Note
>
> This Quota event defines the beginning of the quota block and quota criteria, minutes and/or bytes. At least one criteria type must be specified. If both criteria are specified, the limit that is met or exceeded first will trigger the end of the block of file transfers. For example, assume that the Quota block is set for 30 seconds or 1MB. If the events within the Quota event and the End Quota event do not send 1MB in 30 seconds, then the next connection will send the rest of the file or have a connection for 30 seconds, whichever comes first.

Item	Description
Event Specific Fields	Byte limit. Specifies the size limit (for example, 1024000 or 1000k or 1m) at which you want to stop the transmission of this quota block. Time limit. Specifies the limit in minutes at which you want to stop the transmission of this quota block. Click the Enter limit link to set a limit in the Enter time limit dialog box.
Syntax	Quota <send events> End Quota
Options	N/A
Remarks	The Quota event is based on the actual amount of data being transferred, not the true file size. File compression shrinks file size depending upon file type.
Returned Value	N/A

9.30.40 Raise Event Event

The Raise Event event specifies that a particular event be visible in Home, Alerts.

Item	Description
Event Specific Fields	Event name. Specifies the event to display in the Home, Alerts. Error message. Specifies the message to appear when the event defined as the "raised event" displays in Home, Alerts.
Syntax	N/A
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.41 Read Variable File Event

The Read Variable File event sets variables by reading values from an .ini file.

Item	Description
Event Specific Fields	File name. Specifies the .ini file whose values are to be set as a user variable. User variable name. The user-defined variable whose value is to be determined by the specified .ini file.
Syntax	[Param 1] File name. Example: C:\Variables.ini [Param 2] User variable name. Examples: One variable in one section: <%[MySectionName].MySectionVar> to read MySectionVar entry in MySectionName section of the .ini file. All variables in one section: <%[MySectionName].*> to read all entries in the MySectionName section of the .ini file. The variable name format is <%[MySectionName].EntryName> where EntryName is the name on the left side of the equal sign. All variables in all sections: <%*> to read all entries in all sections of the .ini file. The variable name format is <%[MySectionName].EntryName> where SectionName is the name of the .ini file section and EntryName is the name on the left of the equal sign.
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The format for the .ini file must be: [section] variable=value for example, [386Enh] woafont=dosapp.fon ega80woa.fon=ega80woa.fon ega40woa.fon=ega40woa.fon
Returned Value	N/A

9.30.42 Reboot Client at End of Session Event

Reboots the client after a session has ended.

Item	Description
Event Specific Fields	N/A
Syntax	N/A
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The reboot occurs after the session is complete. Therefore, it is not known to the server if the reboot executes. The event is logged as successful when the task is queued with the operating system. The reboot's successful execution is subject to the device manufacturer's implementation of the reboot API. There are some circumstances in which an interactive user may be given the opportunity to cancel the reboot. For all device types and user contexts, you are advised to test the event to observe results.
Returned Value	N/A

9.30.43 Release Script Event

The Release Script event releases a specific instance of a script engine. To use this event, provide the name of the script file run at the client or server.

Item	Description
Event Specific Fields	Script file name. The path and name of the script file. Click the Browse link to choose a file and directory, or enter the path and file name in this field.
Syntax	[Param 1] Script file name. Example: C:\Scripts\Myscript.vbs

Item	Description
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Accessing session variables through this event is not supported on the client. If you do not use this event to release the script, the script engine will automatically release when the session terminates.
Returned Value	N/A

9.30.44 Remove Directory Event

The Remove Directory event deletes a client or server directory. The directory must be empty of files before it can be removed.

Item	Description
Event Specific Fields	Directory path. The path and name of the directory to be removed.
Syntax	[Param 1] Directory path. Example: C:\ServerDocs
Options	Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The "Include subdirectories" option is available for Windows and Windows Mobile clients. It removes the specified directory, as well as subdirectories as long as no files reside in those subdirectories.
Returned Value	N/A

9.30.45 Rename File Event

The Rename File event moves files or changes the name of one or more files on either the Server or client.

Item	Description
Event Specific Fields	(Source) Old file name or wildcard. Specifies one or more source files to move or rename. Click the Browse link to choose a path and file, or enter the path, file name, or wildcard parameter in this field. (Target) New file name or wildcard. Enter the path and new file name, or the wildcard when more than one file is involved. Enter a directory to move one or more files without changing their names. Click the Browse link to choose a path and file name.
Syntax	[Param 1] Old file name or wildcard. Example: C:\Old*.doc [Param 2] New file name or wildcard. Example: C:\New*.doc
Options	Make target path Ignore hidden files Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the "Make target path" option. Target files, including any subdirectories, in the file spec that do not exist will be created. Supports the "Ignore hidden files" option, which instructs the Server to ignore hidden files in events using wildcards. Supports a file exclusion mask, which appends a vertical bar followed by a file specification to indicate the files to exclude from that operation. For example, to rename all files except .xls files in the "C:\Reports" directory, enter this command: RENAME "C:\Backup\Reports*.*|*.xls" TO "C:\Reports*.*". Define multiple exclusions with multiple instances of the mask, such as "C:\Backup\Reports*.*|*.xls |*.txt".
Returned Value	N/A

9.30.46 Repeat Event

The Repeat event conditionally repeats a block of events.

A Repeat block of events begins with the Repeat event and ends with an End Repeat event.

Repeat if previous event is false allows the events to execute if the previous event failed.

Repeat if previous event is true allows the events to repeat if the previous event was successful.

Item	Description
Event Specific Fields	Maximum Timeout. The maximum amount of time the Repeat event may execute repeatedly. The value may range in minutes and seconds from 00:00 to 59:59. Inactivity Timeout. The maximum amount of time that execution of the event continues when no file transfer occurs. The value may range in minutes and seconds from 00:00 to 59:59. Max Repeats. The maximum number of iterations of this Repeat event. Select from 0 (no repeats) to 99 repetitions. Execution stops after the event has been repeated the maximum number of times.
Syntax	N/A
Options	Previous Event True Previous Event False Condition – While (LValue) <, <=, =, >=, > (RValue) where LValue and RValue can be session variables, numbers, or strings
Remarks	Supports the following conditions: • If Previous Event FALSE • If Previous Event TRUE • If (LValue) <, <=, =, >=, > (RValue) where LValue and RValue can be session variables, numbers, or strings If no limit is set for timeouts or repeats, a session could become caught in an endless loop.
	i Note If the Repeat event is used with the Previous Event TRUE option, when the session runs the event verifies that the previous event was true only one time, as if it was a Repeat If event. If the session re-runs in a loop, the event does not re-verify the previous event. If the Repeat event is used with the Previous Event FALSE option, when the session runs the event verifies that the previous event was false every time it runs, as if it was a Repeat While event .
Returned Value	N/A

9.30.47 Run Script Function Event

The Run Script Function event invokes specific scripting functions at the client or Server.

To use this event, provide the name of the script function, as well as any parameters that need to be passed in to the function.

Item	Description
Event Specific Fields	Script file name. The path and name of the file that contains the script variable. Click the Browse link to choose a file and directory, or enter the path and file name in this field. Function name. The name of the script function. User variable name. The name of the session variable that will store the retrieved value. Return user variable name. If the script function returns a value, the name of the user defined session variable on the server that will store the value.
Syntax	[Param 1] Script file name. Example: C:\Scripts\Myscript.vbs [Param 2] Function name. Example: MyFunction [Param 3] Input variables. Example: <%value1>, <%value2> or 100,200 [Param 4] Return user variable name. Example: <%MyVariable>
	i Note We do not support using this event to display message box (popup) UI.
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The parameter list is a comma separated list that contains either text values or session variables. Accessing Afaria session variables through this event is not supported on the client.
Returned Value	N/A

9.30.48 Search Registry Event

The Search Registry event searches the registry on the client or Server for the specified key or value and places the value found into the specified user-defined variable.

Item	Description
Event Specific Fields	User variable name. The user-defined variable for the registry search. Root key\key1\keyN. The path for the registry value. [value name]. The name for the registry value.
Syntax	[Param 1] User variable name. Example: <%MyVar> [Param 2] Root key value. Example: HKEY_LOCAL_MACHINE\Software\Afaria\Name [Param 3] Value name. Example: ValueName Leave [Param 3] blank to use the default value.
Options	Include subkeys Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports “Include subkeys” so that the registry is searched for any keys matching the Source filespec.
Returned Value	N/A

9.30.49 Send File to Client Event

The Send File to Client event transfers one or more Server files to a file or directory on the client.

Using wildcards with this event transfers a group of Server files whose names have something in common, or that are in the same directory.

> **i** Note
>
> Android devices do not support file compression.

Item	Worklist and Sendlist Objects
Event Specific Fields	(Source) Server file name or wildcard. Indicates which directory or files to send to the client. Enter the file name, path name, or directory on the server. Click the Browse link to choose a file, or use wildcards to send files whose names have something in common or that exist in one directory. (Target) Client file name or wildcard. Places one or more Server files in this location at the client. Specify the file name, wildcard parameter, or directory for the client files.
	i Note A trailing backslash "\" will be accepted as an indication that the target is a subdirectory of the given path, as in C:\Program Files\Sample\Data\. If the target path does not include the trailing backslash, then an attempt will be made to treat the target as a directory, as if an implicit backslash. If such a target directory already exists or is created using the "Make target path" option, then transfer of one or more files to this directory should be successful. In the event that no such directory exists or is created, transfer of more than one file to the target path will fail. However transfer of a single file to the target path will be successful, with the file assuming the name specified in the target. For example, sending C:\Daily.doc to the path C:\Program Files\Sample\Data (where Data is not the name of a directory and is not created) will result in the creation or overwriting of C:\Program Files\Sample\Data with the contents of Daily.doc. In all instances where multiple source files are targeted to a single destination file, the event is logged as an error. Selecting the "Make target path" option (explained on the next page), or the pre-existence of a designated directory will not prevent this error from occurring.
Syntax	[Param 1] Server file name or wildcard. Example: C:\ServerDocs\Daily.doc [Param 2] File name or wildcard. Example: D:\Docs*.doc
File comparison and transfer options	Transfer: Always Transfer: If destination does not exist Transfer: If source is newer Transfer: If source is different Use version information Check/Send Use safe transfer Turn compression off Use file differencing

Item	Worklist and Sendlist Objects
Options	Delete after [-] Make target path Ignore hidden files Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Maximum file size – 4 GB; to send a file send a file over 4 GB, you must divide the file into segments, each 4 GB or less in size. Supports the "Use safe transfer" option so that the Server does not create a destination file until it has been successfully transferred. Supports the "Make target path" option. Target files, including any subdirectories, in the file spec that do not exist will be created. Supports the "Ignore hidden files" option, which instructs the Server to ignore hidden files in events using wildcards. Supports a file exclusion mask, which appends a vertical bar followed by a file specification to indicate the files to exclude from that operation. For example, to get all files except .xls files from the "C:\Reports" directory, enter this command: SEND "D:\Backup\Reports" FROM "C:\Reports*.*|*.xls". Define multiple exclusions with multiple instances of the mask, such as "C:\Reports*.*|*.xls |*.txt". Supports indirect files. Sets event-specific information in an ASCII file that's referenced in the event, rather than included.
Returned Value	N/A

9.30.50 Set Bandwidth Throttling Config Event

The Set Bandwidth Throttling Config event allows you to assign a predefined bandwidth throttling configuration to a session.

Item	Description
Event Specific Fields	Configuration name. The name of the predefined bandwidth throttling configuration set on the Bandwidth throttling view in Server configuration, Properties, or a variable created using the Set Variable event. If the configuration name that you enter in this field does not exist, the software uses the Current Default Configuration defined on the Bandwidth throttling view.
Syntax	N/A
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.51 Set Client Time Event

The Set Client Time event allows you to synchronize a client's time and date with the server's time and date.

This feature is valuable for customers with clients that reside in a restricted network and cannot perform their own date and time synchronization.

Item	Description
Event Specific Fields	N/A
Syntax	N/A
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.52 Set Database Field Event

The Set Database Field event associates a value or variable to a specific user-defined field (as defined in Server configuration, Properties, User defined fields link) and then stores it in the User Defined Fields (A_USER_DEFINED) table in the database.

Item	Description
Event Specific Fields	Variable or database field name. The user-defined field name as set on the Server Configuration page for user-defined fields. Variable or value to store. The value to associate with the user-defined field name and then store in the User Defined Fields table in the database.
Syntax	[Param 1] Variable or Database field Name. Example: TotalConnections [Param 2] Variable or value to store. Example: 5
	Note The SQL statement must be syntactically correct or the database rejects it and the event fails. The following examples provide the correct syntax for each user defined field type available to the A_USER_DEFINED field table. The examples assume that the Float (decimal numbers) field name is "MyFloat"; Varchar (text strings, 255 character limit) field name is "MyVarchar"; Integer (whole numbers) field name is "MyInteger"; and Date field name is "MyDate".
	Example Float field type: [Param 1] MyFloat [Param 2] 1234.5
	Example Varchar field type: [Param 1] MyVarchar [Param 2] 'Hello World!' or [Param 2] 'Don''t forget to escape single quotation marks occurring within a string.' (Varchar field type values must be enclosed in single quotation marks. A single quotation mark within the text must also be preceded by a single quotation mark, as in "Don''t...")

Item	Description
	Example Integer field type: [Param 1] MyInteger [Param 2] 1234
	Example Date field type: [Param 1] MyDate [Param 2] GetDate()
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	When a client connects to the server, the system updates the database field (specified in [Param 1] in the User Defined Fields table) with the current value of the variable/value specified in [Param 2]. If an error occurs when attempting to "write" a field value to the table, the system will retry once. If the retry fails, then the event fails and an error message is logged to Server Logs, Messages view. If you assign a value to a field and that field is deleted via User defined fields (in Server configuration, Properties), then both the field and its value are deleted from the User Defined Fields table. Before using a field in this event, ensure that it exists in the table.
Returned Value	N/A

9.30.53 Set File Attributes Event

The Set File Attributes event sets or clears a file or a wildcard's attributes.

> **i Note**
>
> File attributes are not retained in the Copy File Event [page 195], Get File from Client Event [page 209], and Send File to Client Event [page 227]. Instead, you must use this event to define file attributes.

Item	Description
Event Specific Fields	File name or wildcard. Indicates the file or wildcard on which to set or clear the attributes.
Syntax	[Param 1] File name or wildcard. Example: C:\WINNT\system.ini

Item	Description
Options	Read only System Hidden (see Remarks) Archive Normal Apply to directory only Ignore hidden files Include subdirectories Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Returned Value	N/A

9.30.54 Set Registry Value Event

The Set Registry Value event sets a specified registry value to the string specified.

Item	Description
Event Specific Fields	Root key\key1\keyN. The path of the value to be set. Variable or value. The user-defined variable to set with the specified registry key, or the value to use. Value type. Key data type. [value name]. The name for the registry value.
Syntax	[Param 1] Root key. Example: HKEY_LOCAL_MACHINE\SoftWare\Afaria\Dir [Param 2] Variable or value. Example: C:\Temp or <%MyVar> [Param 4] Value name. Example: ValueName

Item	Description
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Converts non-string values to string values. Supports the “Make target path” option. Target files, including any subdirectories, in the file spec that do not exist will be created.
Returned Value	N/A

9.30.55 Set Script Variable Event

The Set Script Variable event allows the session to set a global script variable that can be used by the script in subsequent calls to script functions at the client or Server.

To use this event, provide the name of the script variable, as well as a value. The value can contain a session variable.

Item	Description
Event Specific Fields	Script file name. The path and name of the file that contains the script variable. Click the Browse link to choose a file and directory, or enter the path and file name in this field. Script variable name. The name of the script variable. Variable or value. The name of the variable or value.
Syntax	[Param 1] Script file name. Example: C:\Scripts\Myscript.vbs [Param 2] Script variable name. Example: MyVariable [Param 3] Variable or value. Example: C:\Temp

Item	Description
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	The difference between running a script on the client versus the Server is that session variable support is limited to setting the variable. Client scripts cannot get the session variable. Accessing Afaria session variables through this event is not supported on the client.
Returned Value	N/A

9.30.56 Set Variable Event

The Set Variable event creates user-defined variables.

After a user variable is defined, it may be used anywhere in a session, including other worklist objects. A user-defined variable does not preserve its data across sessions, except during a restart.

Item	Description
Event Specific Fields	User variable name. Specifies the name for this user-defined variable. The default value is <%VariableName>. Value or @indirect file. Sets the variable's value or specifies the name of the file that contains the value. Click Browse to choose a Server text file, or enter the path and file name of a text file. When using a file, remember to precede the path and file name with an "@".
Syntax	[Param 1] User variable name. Example: <%MyVar> [Param 2] Value or @indirect file. Example: NewValue or @C:\NewVlue.txt
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]

Item	Description
Remarks	The variable names should be unique throughout all worklists in a session. Using the Set Variable event on a previously defined variable will change the value. Although this may be needed for some applications, it can lead to unexpected results and side effects across worklists. This event works only with text (*.txt) files when referencing indirect files. Supports indirect files. Sets event-specific information in an ASCII file that's referenced in the event, rather than included.
Returned Value	N/A

9.30.57 Test Group Membership Event

The Test Group Membership event allows you to test predefined LDAP/NT or user-defined client groups by comparing the group to a known value.

The session evaluates the group and the result is compared to the specified value.

Item	Description
Event Specific Fields	Group to test. The group to evaluate. Click the Browse link to access the Assignment group browse dialog box through which you can select the group.
Syntax	[Param 1] Group to test. (Selection occurs through the Browse link.) Example: NTDGWID:development\Domain Admins\512
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A
Returned Value	N/A

9.30.58 Test Variable Event

The Test Variable event allows you to test predefined variables by comparing the variable to a known value.

The session evaluates the variable and the result is compared to the specified value.

Item	Description
Event Specific Fields	Variables and/or text. The variable or text string to evaluate and compare with the field below. This field may contain up to 260 characters. Variables and/or text. The variable or text string to compare with the value in the first field. This field may contain up to 260 characters.
Syntax	[Param 1] Variables and/or text. Example: <%MyVar> [Param 2] Variables and/or text. Example: <%MyTestVar> or TestText
Options	Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	N/A.
Returned Value	N/A

9.30.59 Update Variable File Event

The Update Variable File event allows user-defined variables to be saved to a Windows .ini file on the client and Server.

Item	Description
Event Specific Fields	File name. The path and directory of the .ini file. User variable name. The user-defined variable to be saved to the specified .ini file.
Syntax	[Param 1] File name. Example: C:\Variables.ini [Param 2] User variable name. Example: <%[MySectionName].MySectionVar>

Item	Description
	i Note To update a variable from a variable file, use any of the following examples: One variable in one section: <%[MySectionName].MySectionVar> to read MySection-Var entry in MySectionName section of the .ini file. All variables in one section: <%[MySectionName].*> to read all entries in the MySec-tionName section of the .ini file. The variable name format is <%[MySection-Name].EntryName> where EntryName is the name on the left side of the equal sign. All variables in all sections: <%*> to read all entries in all sections of the .ini file. The variable name format is <%[MySectionName].EntryName> where SectionName is the name of the .ini file section and EntryName is the name on the left of the equal sign.
Options	Make target path Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	Supports the "Make target path" option. Target files, including any subdirectories, in the file spec that do not exist will be created.
Returned Value	N/A

9.30.60 Wait for File to Exist Event

The Wait for File to Exist event instructs the session to pause until a client or server file exists, or until a specified amount of time elapses, whichever comes first.

Session Manager checks the Server every half-second and the client every second.

Item	Description
Event Specific Fields	File name. Identifies the client or Server file to locate. Click the Browse link to select a file, or enter the path and file name in this field. Wait time. Specify the time, in minutes and seconds, to wait for the file to exist. Use the keyboard and spin controls to set the delta time. Times may range from 00:00 to 59:59.

Item	Description
Syntax	[Param 1] File name or wildcard. Example: C:\Docs\Daily.doc [Param 2] Wait time. Example: 45:00
Options	Delete after (-) Conditional (True/False) Execution: Normal Execution: Not required for successful session [x] Execution: Channel critical event [+] Execution: Session critical event [*]
Remarks	You should consider using the File Status event if your wait time is close to 00:00.
Returned Value	N/A

9.31 Session Manager Variables

When an event executes, Session Manager replaces variable placeholders with the appropriate information. Variables are always enclosed in "<>" characters and are not case sensitive.

To add a variable to an event specific field, click the Show variables link on the Event details dialog box. In the Session Variables box, double-clicking the variable adds it to the event. You can also enter the variable in the appropriate fields.

Session Manager supports the following variable types:

- Predefined Session Variables
- User-Defined Session Variables
- Environment Variables
- Variable Modifiers

> ⚠ Caution
>
> When running an individual channel or a channel set in an Afaria connection, if you create more than 256 variables in that session you will see the following error message: "Not enough storage is available to process this command"

> i Note
>
> All session variables are subject to a 256-character maximum length requirement.
>
> Not all variables are supported for all types of clients, for instance <ClientWindowsDir> is not an appropriate variable to use on an Android device; however, the Session Manager Channel Editor allows you to add any variable to any worklist.

The use of Session Manager variables is reserved for Session Manager channels. Except where noted otherwise, Afaria does not support using variables as values for other components' dialog boxes and input parameters.

9.31.1 Predefined Session Variables

Session Manager includes a set of predefined session variables that you can use to insert the current time or date, client information, or Server information in an event list.

The following table lists each predefined variable, describes its function, and provides an example of its usage and a value of the variable.

Variable	Description	Sample use or sample value
<%UserDefined>	Contains or holds the value of the specified user-defined variable	Value of Variable: Value (varies)
<AuthenticatedUser>	Indicates whether or not Authentication is turned on, returning either "0" or "1" where "1" indicates Authentication is turned on	Value of Variable: 1
<ChannelName>	Indicates the name of the channel	Set Variable: <%CurrentChannel><ChannelName> Value of Variable: Channel name
<ChannelViewer>	Indicates whether the Channel Viewer UI initiated the session, returning either "1" or "0" where "1" indicates that Channel Viewer initiated the session	If <ChannelViewer> = 1 Value of Variable: 1
<CheckDiskSize>	The disk free space available value, in bytes, as determined by running the Check Volume event, handled as unsigned 64-bit integers	If <CheckDiskSize> <= 1000000 Value of Variable: 900900
<CheckMemorySize>	Used with the Check Memory event, returns a value, in bytes, that represents the available amount of memory on the handheld client; handled as unsigned 64-bit integers	If <ClientMemorySize> <= 1200000 Value of Variable: 10017792
<ClientAllUsersDesktopDir>	Returns the desktop folder for "all users" in operating systems that use the convention	Client File Status: <ClientAllUsersDesktopDir> Value of Variable: C:\Documents and Settings\All Users Desktop
<ClientBuild>	The version of the client build	Set Variable: <ClientBuild> Value of Variable: 5240

Variable	Description	Sample use or sample value
<ClientChannelDir>	The directory of the client computer where channel files are located	Client File Status: <ClientChannelDir> Value of Variable: C:\Program Files\AClient\data\VB\49\
<ClientCommonFilesDir>	The Windows Common Files directory on the client computer	Client File Status: <ClientCommonFilesDir> Value of Variable: C:\Program Files\Common Files
<ClientDataDir>	The directory of the client where the client data files are located	Client File location: <ClientDataDir> Value of Variable: C:\Program Files\AClient\Data
<ClientDomainName>	The name of the domain to which the user is logged on, or if the user is not logged on to a domain this variable will contain the user's computer name	Server Message: <ClientDomainName>finished session Value of Variable: Domain name
<ClientID>	The Windows GUID string associated with the client.	Server Message: Client's ID is <ClientID> Value of Variable: {267D64EC-90B1-420b-AE49-BA7221FBFAF1}
<ClientInstallDir>	The name of the install directory on the client	Client File Status: <ClientInstallDir>\1.txt Value of Variable: C:\Program Files\AClient
<ClientIPAddress>	The client's IP address displayed in dotted decimal notation. This variable applies to Windows 32 clinets only.	Server Message: Could not complete session with <ClientIPAddress> Value of Variable: 192.49.5.104
<ClientMachineName>	The computer name of the client computer	Test Variable: <ClientMachineName> <ServerMachineName> Value of Variable: Machine2
<ClientMemorySize>	Used with the Check Memory event, returns a value, in bytes, that represents the total amount of memory on the handheld client; handled as unsigned 64-bit integers	If <ClientMemorySize> <= 1400000 Value of Variable: 1290342
<ClientOS>	The operating system on the client computer	Server Message: Client's operating system is <ClientOS> Value of Variable: Windows 2003
<ClientOSServicePack>	If the client computer runs an operating system service pack, returns the level; otherwise returns nothing	<ClientOSServicePack> Value of Variable: 6
<ClientOSShell>	Used to return the device type for the client; returns nothing for Windows CE clients	<ClientOSShell> Windows Mobile 6 Professional

Variable	Description	Sample use or sample value
<ClientOSVersion>	The version of the operating system on the client computer	Set Variable: <%ClientSpec><ClientOS> <ClientOSVersion> Value of Variable: 6.0.1381
<ClientProcessor>	Used to determine the processor for the specific client	<ClientProcessor> Example value of Variable: StrongArm
<ClientProgramFilesDir>	The Program Files directory on the client computer	Client Check Volume <ClientProgramFilesDir> var.ini Value of Variable: C:\Program Files
<ClientRasUserName>	If the handheld client connects to the server via a modem, returns the user's User Name, otherwise returns nothing	<ClientRasUserName> Value of Variable: Name
<ClientTempFilesDir>	The temporary files directory on the client computer	Client File Status: <ClientTempFilesDir>*.x00 Value of Variable: C:\Temp
<ClientTypeCategory>	The number assigned to a category type, as defined in table A_CLIENT_CATEGORY_NAME_MAP	<ClientTypeCategory> Sample value: 7 Value of variable: -1 Windows -2 Windows Mobile Professional -4 Java -7 Windows Mobile Standard -8 iOS -9 OMA DM -10 Android
<ClientTypeCategoryName>	The name of the type of device as defined in table A_CLIENT_CATEGORY_NAME_MAP	<ClientTypeCategoryName> Sample value: Windows Mobile Standard Value of variable: 1 Windows 2 Windows Mobile Professional 7 Windows Mobile Standard 8 iOS 10 Android
<ClientUserName>	If the user launches the.xec file directly to initiate a session and the client service is not running, then...	Value of Variable: User name currently logged in
	...if the service is running, then...	Value of Variable: Afaria Client Service Account
	If the session is initiated through the Scheduler and the client service isn't running, then...	Value of Variable: Account under which XCScheduler.exe runs

Variable	Description	Sample use or sample value
	...if the service is running, then...	Value of Variable: Afaria Client Service Account
	...if the service is running, then...	Value of Variable: Afaria Client Service Account
<ClientVersion>	The version of the Afaria Client application on the client computer	If <ClientVersion> = 6.00 Value of Variable: 6.00
<ClientWindowsDir>	The Windows directory on the client computer	Send <ServerWindowsDir>*.* TO <ClientWindowsDir>*.* Value of Variable: C:\Winnt
<ClientWindowsSystemDir>	The Windows System directory on the client computer	Client Check File \example.dll <ClientWindowsSystemDir> \example.dll Value of Variable: C:\Winnt\System32
<ConnectionId>	The unique numeric ID (GUID) for the connection	Client Message: Your connection is <ConnectionId> Value of Variable: 88819910-61AC-11D5-B23C-0008C7592863
<ConnectionSpeed>	Used with the Check Speed event, determines the speed of a session connection in seconds; see remarks in "Check Speed Event" for limitations.	Value of Variable: Bits per second
<ConnectionType>	Determines whether the session connection is via LAN or dial-up	Value of Variable: LAN
<d>	Indicates the day of the month from 01 to 31	If <d> <= <%MiddleOfMonth> Value of Variable: 06
<date>	The numeric month, day, and year in the form specified by the Server's Regional Settings Control Panel	Set Variable: <%LongDate> Hello. It is <Date> Value of Variable: 060800
<dw>	Indicates the day of the week from 1 to 7	Server Remove Dir f:\week<dw> Value of Variable: 4
<dy>	Indicates the day of the year from 001 to 365	Server Execute c:\bin\dateset -d <dy> Value of Variable: 089
<FileStatCount>	The number of files as determined by running the File Status event	If <FileStatCount> <=10 Value of Variable: 10
<FileStatSize>	The file size value, in bytes, determined by running the File Status event; handled as unsigned 64-bit integers	If <FileStatSize> <= 1000000 Value of Variable: 1000000
<FileStatVersion>	The file version value determined by running the File Status event	If <FileStatVersion> <= 5.0.0.0 Value of Variable: 4.10.412.0

Variable	Description	Sample use or sample value
<GetFilesAttempted>	The number of files the Server attempts to get from the client, setting the counter to “0” at the beginning of each channel and never resetting	Value of Variable: 6
<GetFilesFailed>	The number of times the Server is unable to get a file from the client, setting the counter to “0” at the beginning of each channel and never resetting	Value of Variable: 3
<GetFilesNoUpdate>	The number of files the Get File from Client event checks that do not require an update, setting the counter to “0” at the beginning of each channel and never resetting	Value of Variable: 5
<GetFilesSuccessful>	The number of times the Server is successful in getting a file from the client, setting the counter to “0” at the beginning of each channel and never resetting	Value of Variable: 3
<hh>	Indicates the current 24-hour value on the server from 00 to 23	Server Message: Schedule complete at <hh>:<mm>:<ss> Value of Variable: 17
<InteractiveUserName>	If the user launches the.xec file directly to initiate a session, then...	Value of Variable: User name currently logged in
	If the session is initiated through the Scheduler, then...	Value of Variable: Account under which XCScheduler.exe runs
	If the user initiates a session through Channel Viewer, then...	Value of Variable: User name currently logged in
<m>	Indicates the month in numeric format from 01 to 12	Client Delete C:\prices\prices<m>.dat Value of Variable: 03
<mm>	Indicates the current minute value on the server from 00 to 59	Client Message: <UserName> connected at <mm> after the hour Value of Variable: 58
<ms>	Indicates the value of milliseconds from 000-999, resetting every second	Client Message: <UserName> connected at <ms> after the minute Value of Variable: 187
<SendFilesAttempted>	The number of files the Server attempts to send to the client, setting the counter to “0” at the beginning of each channel and never resetting	Value of Variable: 6

Variable	Description	Sample use or sample value
<SendFilesFailed>	The number of times the Server is unable to send a file to the client, setting the counter to "0" at the beginning of each channel and never resetting	Value of Variable: 3
<SendFilesNoUpdate>	The number of files the Send File to Client event checks that do not require an update, setting the counter to "0" at the beginning of each channel and never resetting	Value of Variable: 11
<SendFilesSuccessful>	The number of times the Server is successful in sending a file to the client, setting the counter to "0" at the beginning of each channel and never resetting	Value of Variable: 3
<ServerCommonFilesDir>	The Windows Common Files directory on the server computer	Server File Status: <ServerCommonFilesDir>\mtx0392.dir Value of Variable: C:\ProgramFiles\Common Files
<ServerFarmMasterServerID>	In multiserver environments, the id of the master server	Server ID: <ServerFarmMasterServerID>\mtx0392.dir Value of Variable: AfariaOne
<ServerID>	Indicates the unique identifier for the Server computer	Value of Variable: Name of server
<ServerInstallDir>	The name of the install directory on the server computer	Server File Status: <ServerInstallDir> Value of Variable: C:\Program Files\Afaria
<ServerIPAddress>	The Server's IP address displayed in dotted decimal notation	Client Message: You are proudly served by <ServerIPAddress> Value of Variable: 192.4.109.52
<ServerMachineName>	The computer name of the Server computer	Client Message: You are being served by <ServerMachineName> Value of Variable: Machine1
<ServerMemorySize>	Used with the Check Memory event, returns a value that represents the total amount of client memory; handled as unsigned 64-bit integers	If <ServerMemorySize> <= 4GB Value of Variable: 3GB
<ServerName>	Indicates the name of the Server	Value of Variable: Server1
<ServerOS>	The Server's operating system	Server Search Registry <%SvrOSValue> <ServerOS> Value of Variable: Windows NT
<ServerOSVersion>	The version of the Server's operating system	If <ServerOSVersion> = <ClientOSVersion> Value of Variable: 3.0.1381

Variable	Description	Sample use or sample value
<ServerProgramFilesDir>	The Program Files directory on the server computer	Server Delete <ServerProgramFilesDir>*.tmp Value of Variable: C:\Program Files
<ServerTempFilesDir>	The temporary files directory on the server computer	Server Rename <ServerTempFilesDir>*.mm0 <ServerTempFilesDir>*.m0 Value of Variable: C:\Temp
<ServerVersion>	The version of Afaria installed on the server computer	Value of Variable: 6.00
<ServerWindowsDir>	The Windows directory on the server computer	Send <ServerWindowsDir>*.bmp TO <Client-WindowsDir>*.bmp Value of Variable: C:\Winnt
<ServerWindowsSystemDir>	The Windows System directory on the server computer	Server Copy <ServerWindowsSystemDir>*.drv TO \archive\drv*.dr_ Value of Variable: C:\Winnt\System32
<SessionDuration>	The number of minutes elapsed during this session	If <SessionDuration> > <%CutoffTimeLimit> Value of Variable: 3
<SessionStartTime>	The time (in hhmmss format) when this session started	Server Message: User <UserName> starts at <SessionStartTime> Value of Variable: 010634
<ss>	Indicates the current second value on the server from 00 to 59	Server Copy D:\begin.flg TO D:\begin<ss>.flg Value of Variable: 56
<SystemTime>	The current GMT date and time of the server or client in format YYYYMMDD HH:MM	Server Message: User <UserName> starts at <SystemTime> Value of Variable: 20100912 13:34
<TenantID>	ID of the tenant, as defined in table A_TENANT	Server Message: Client's tenant id is <TenantID> Value of Variable: 10134
<TenantName>	Name of the tenant, as defined in table A_TENANT	Server Message: Client's tenant name is <Tenantname> Value of Variable: Tedco
<time>	Inserts the current 24-hour time at the Server in format hhmmss	Client Rename C:\done.flg TO \<time>.flg Value of Variable: 010634
<VolumeSize>	After executing Check Volume event, returns the total size of the checked volume; handled as unsigned 64-bit integers	If <VolumeSize> <= 4GB Value of Variable: 3GB
<y>	Indicates the exact two-digit numeric value of the year from 00 to 99	Client Rename C:\daily.log TO C:\archive \year<y>.log Value of Variable: 00

Variable	Description	Sample use or sample value
<y1>	Indicates the exact one-digit numeric value of the year from 0 to 9	Server Rename C:\date.fil TO C:\date<y1>.fil Value of Variable: 9
<y4>	Indicates the exact four-digit numeric value of the year	Server Rename C:\date.fil TO C:\date<y4>.fil Value of Variable: 2006

9.31.2 User-Defined Session Variables

User-defined session variables use the Set Variable event to create custom placeholders for any event that can use a variable.

Every worklist or sendlist in the session channel will have access to the new variable after it's defined. As a result, user-defined variables can be used as parameters in another worklist in the same Session Manager channel, but not across channels.

Worklists can reference another worklist's user-defined session variable as long as the variable has already been defined in the session. Sendlists execute before worklists in a session. This order of execution prevents sendlists from being able to use a worklist's variable. Exceptions may occur if you manipulate priorities in a channel or are running queued outbound notification channels.

User-defined session variables use the % (percent) symbol preceding the variable name, such as **<%myvariable>=**value. Examples of user-defined variables include:

<%current>=<m>/<d>/<y>	(Includes a combination of literal text and system variable.)
<%report>=@\report.txt	(Includes an indirect reference "@" to the contents of a file.)
<%path>=\\server1\data	(Includes a combination of literal text and system variable)

9.31.3 Environment Variables

Use environment variables as placeholders in event text for system defined values.

To be recognized by the Server, these environment variables must be defined on the Environment property page of the System Properties window, which you can access from Control Panel.

If variables have been changed or new variables have been defined, these values will not be recognized unless the service is stopped and restarted.

Environment variables in event text must take the form **<$variablename>**. For example, if a line in the System Environment Variables box defines the variable... **HTMLHome=Z:\SessionManagerChannelEditor\HTML\ActiveX**

then the event to copy a file to this directory would be...

```
COPY C:\Temp\File1.htm TO <$HTMLHome>\File1.htm
```

9.31.4 Variable Modifiers

Variable modifiers modify, then return values, from other variables. The following table lists the available variable modifiers.

Variable modifier	Description	Example
<!Drive<VarName>>	Extracts the drive letter from a session variable or user variable	Set Variable: <%MyVar>=C:\Dir1\FileName.doc Message: <!Drive<%MyVar>> Value of Variable: C:
<!File<VarName>>	Extracts the file name from a session variable or user variable	Set Variable: <%MyVar>=C:\Dir\FileName.doc Message: <!File<%MyVar>> Value of Variable: FileName.doc
<!NormalizeFileVersion<VarName>>	Returns a normalized version of a version number as a 4-node version statement, with each node containing 5 characters, for the benefit of a text string comparison. Each node is padded with leading zeros, as necessary. For example, comparing 3.2.2. to 3.2.10 becomes a comparison between 00003.00002.00002.00000 and 00003.00002.00010.00000.	If v<!NormalizeFileVersion<File1StatVersion>> < v<!NormalizeFileVersion<File2StatVersion>>
<!Path<VarName>>	Extracts the path from a session variable or user variable	Set Variable: <%MyVar>=C:\Dir\FileName.doc Message: <!Path<%MyVar>> Value of Variable: \Dir1\

9.32 Work Object Execution Problems and Solutions

There are several common reasons why a worklist or sendlist object may not execute.

Reason	Explanation and Solution
A worklist or sendlist is disabled	Explanation: Worklist and sendlist objects must be enabled before they can be executed. Solution: Verify that all worklist and sendlist objects assigned to the Session Manager channel are enabled. In Members view, verify that Enabled displays in the Status column for each event. If a worklist or sendlist is disabled, select the object and click Enable.
A worklist or sendlist has been deleted	Explanation: A worklist or sendlist may have been inadvertently deleted from the Session Manager channel. Solution: Verify that all necessary worklist and sendlist objects still exist. Use the Members view to display all worklist and sendlist objects associated with a selected Session Manager channel. If a worklist or sendlist is no longer a member of the channel and is unavailable in the Select objects dialog box (see following item), you must re-create the object.
A worklist or sendlist has not been assigned to the proper Session Manager channel	Explanation: A worklist or sendlist may exist but may not be assigned to the proper Session Manager channel. When you initially create a new worklist or sendlist, it is automatically added to the selected Session Manager channel. If you have copied or imported worklists and sendlists or have assigned and unassigned objects during your Session Manager channel editing, an object may have been assigned to the wrong channel or to no channel at all. Solution: Verify that all necessary worklist and sendlist objects are assigned to the proper Session Manager channels. Use the Members view to display all worklists and sendlists associated with a selected Session Manager channel. If a worklist or sendlist is not assigned to the Session Manager channel, click Assign to display the Select objects dialog box. Select the necessary worklist or sendlist from the list of existing objects and then click OK.
A worklist or sendlist priority is not properly set	Explanation: A worklist or sendlist object's priority setting determines the order in which it is executed during a session. For example, a worklist or sendlist with a priority setting of 100 will execute before a worklist or sendlist with a priority setting of 5. Solution: Verify that the proper priority setting has been assigned to the object. (If no priority is set, the object runs in the assigned order. The Select objects dialog box displays the objects in alphabetical order, but it does not have any impact on the execution order.) In Members view, verify that the object has been assigned the proper priority setting. To change an object's priority setting, right-click the object in the left pane of the editor and then choose Set Priority on the shortcut menu. In the Set <object> priority dialog box, enter the correct priority for the object and then click OK.

Reason	Explanation and Solution
A sendlist failed due to an invalid disk drive, directory, or path	Explanation: A sendlist transfers files based on the source and target drives, directories, and paths specified on the Event details dialog box. If you have specified an invalid drive, directory, or path, the event fails. Solution: Verify that the source and target drives, directories, and paths are correct. Use the Item Details dialog box to review the event details. If necessary, use the Event details dialog box to make the necessary changes, or create the necessary directory structure.
An event in a worklist or sendlist is disabled	Explanation: Each event in a worklist or sendlist must be enabled before it can be executed as part of the worklist or sendlist, even if the worklist or sendlist to which it belongs has been enabled. If you haven't enabled an event in a worklist or sendlist, that event will not execute. Solution: Verify that all events in a worklist or sendlist have been enabled. Use the Events view to display the object's events. If an event is disabled, it appears dimmed in Events view. To enable an event, right-click the event in the left pane of the editor and on the shortcut menu choose Enable, or access the Event details page for the event and select the Enabled option in the Status group box.
A worklist or sendlist object's events are not arranged in the proper order	Explanation: The order of events in the Events list is critical, as in the absence of a priority setting the arrangement of events determines the order in which the events execute. For example, if you insert the End Work Object event in the middle of the list of events, the object will end before all the events have executed. Solution: Verify that the events in a worklist or sendlist are arranged in the proper order. Use the Events view to see the order of events. To change the order of events, use the copy and paste commands in conjunction with the Insert Before and Insert After buttons to rearrange the events.
A critical event failed	Explanation: A critical event causes the session to terminate automatically if the event fails to successfully complete. If other events follow the failed critical event, they will not execute. Solution: Check the event details to determine which critical event failed. If this event is not critical, clear the Critical Event option on the Event details dialog box.
Insufficient disk space at the client	Explanation: In order for certain events such as file transfers to execute properly, there must be sufficient disk space at the client. If there isn't sufficient disk space, the event will not execute. Solution: Verify that sufficient disk space exists on the client. Use the Check Volume event to verify disk space.

Reason	Explanation and Solution
Invalid disk drive	Explanation: If the disk drive specified for the Source or Target does not exist, the event cannot be completed. Solution: Verify the correct disk is specified on the Events details dialog box. If necessary, make changes to the disk drive specified, or create the appropriate directory structure.
Variables not properly defined	Explanation: You must use the proper syntax when creating user-defined variables. For example, all user-defined variables must be enclosed in "< >" symbols and must be preceded with the "%" symbol, for example, <%variable>. Solution: Verify that you have used the proper syntax for all user-defined variables. Use the Event details dialog box to check variables. Make changes as necessary.
Conditional statements not properly resolved	Explanation: Many conditional events, such as Else statements, are used in conjunction with other events, such and End If events. Events may fail if conditional events are not properly resolved, for example an If event must be used with an Else event. Solution: Verify that all conditional events are resolved. Use the Events dialog box to display all of the events. Add additional conditional events as necessary.
Repeat event not properly defined	Explanation: Repeat events repeat actions based on the iterations and loop times that you specify. If you do not specify a loop time or do not use an End Repeat event in conjunction with the Repeat event, the event may not execute properly. Solution: Verify that all Repeat events are used in conjunction with an End Repeat event and that you have specified the proper number of iterations and loop times. Use the Event details dialog box to review the information. If necessary, add an End Repeat event to the list of events or modify the detail information on the Event Details dialog box.

> **i Note**
>
> Source files cannot be specified along paths that are mapped drives. If the source is on a drive other than the local computer (Server), then UNC paths are required.
>
> The condition status that is returned is based on the last event that executes. If an event is skipped, then no status is returned.

10 Reference

This section contains topics that provide more information about configuring Afaria.

10.1 Updating Passwords and Domain User Accounts

As needed and without reinstalling the Afaria server, change the domain user account and password associated with the Afaria server service, or the user password associated with the database.

Context

The main Afaria server and all farm servers must use the same user account name and password.

Procedure

1. Close all Afaria programs.
2. Using a command line, run the setup program (`setup.exe`) with parameters to change the service account or password.

   The setup program accepts parameters in any order. Available parameters:
   - -Maintenance – required for all commands.
   - -ServiceAccount= “name” – required if changing the user account and password associated with the Afaria server service.
   - -ServicePassword=“password” – required if changing the user account and password associated with the Afaria server service.
   - -DatabasePassword=“password” – required if changing the database user account password.
3. Allow the program to run to completion.

   The setup program runs silently, and may take several minutes to complete. You may not know when it has finished unless you watch the task list or run the setup from a batch file. To check for errors, see `C:\silent.log`.

10.2 Syntax Examples for Updating Afaria Server Password

When updating the user account and password on an Afaria server, the Afaria setup program accepts parameters in any order.

> ✤ Example
>
> Examples:
>
> - setup -Maintenance -DatabasePassword=“password”
> - setup -Maintenance -ServiceAccount=“name” -ServicePassword=“password”
> - setup -Maintenance -DatabasePassword=“password” -ServicePassword=“password2”

10.3 Addresses and Routing for SMS and SMTP Messages

Both the Afaria SMS Gateway and the SMTP server use addresses to deliver their respective messages to recipients.

Addresses are used in multiple contexts, including but not limited to:

- Notification messages to devices for message broadcasts, provisioning, or client deployment
- Alert notifications to an administrator contact
- Security commands to Afaria managed devices

10.4 SMS and SMTP Message Address Syntax

The address determines how the Afaria Server routes the message.

> ✤ Example
>
> Use this syntax to format addresses:
>
> <prefix>[<routing information>]
>
> where < > encloses a parameter value, and “[ ]” indicates an optional parameter.
>
> SMSC address requirements – your Short Message Service Center (SMSC) configuration entities may have specific address requirements for successful routing. For example, a service provider or carrier modem may require you to format all mobile numbers in their respective international format and may stipulate that the leading “+” symbol is or is not part of the requirement. It is your responsibility to understand the requirements for your SMSC entities, and it is your responsibility to create your address entries appropriately.
>
> SMSC name – the name of your SMSC entity has a direct impact on how Afaria routes Afaria-initiated messages.

Prefix		Routing Information		Examples	Afaria Routing Logic
Prefix = <mobile number>					
<prefix>	+	*null*	=	5554122212 15554122212 +15554122212 +445555121212	IF any SMS Gateway SMPP service is defined, THEN send via SMPP service, ELSE IF any SMS Gateway entity is defined, THEN send via SMS Gateway entity, ELSE discard message.
<prefix>	+	<routing information>	=	+15554122212@allcellular 5554122212@mobiletoday.com	IF <routing information> = an SMS Gateway SMPP service name, THEN send via SMPP service, ELSE IF <routing information> = an SMS Gateway modem name, THEN send via modem, IF any SMS Gateway SMPP service is defined, THEN send via SMPP service, ELSE IF any SMS Gateway entity is defined, THEN send via SMS Gateway entity, ELSE send via SMTP server.
Prefix = <recipient identifier>					
<prefix>	+	*null*	=	john.doe jdoe	Invalid, discard message.
<prefix>	+	<routing information>	=	john.doe@mobiletoday.com jdoe@allcellular jdoe@egroup.gov	Send via SMTP server.

10.5 Verifying Afaria Administrator IIS Settings

If you used a predefined virtual directory when installing Afaria Administration console instead of allowing the setup program to create one for you, or if you are having problem accessing the administration console from a browser, verify the Afaria API Server and Administrator and IIS settings.

Procedure

1. From the Windows Server where you installed the Afaria Administration console, select *Start > Administrative Tools > Internet Information Services (IIS) Management*.
2. Click the Basic Settings link on the right toolbar.
3. In the Edit Application dialog, verify that the physical path is the one you set during installation.
4. Open Default Document and verify that `default.aspx` appears in the list.
5. Open Authentication and ensure that only Windows authentication is enabled.
6. Click *Back* and click Browse on the right toolbar.

> **i** Note
>
> If you have stopped and restarted IIS at any time before opening Afaria Administration console, ensure that when you restarted IIS that the WWW Publishing Service also started. If it is not started, you can reset IIS, or you can restart it manually. This service must be running for you to open the administration console.

10.6 Changing the IIS Connection Timeout Value

Change the IIS connection timeout value to prevent the Afaria Server from disconnecting with an inactive browser user. Disconnected sessions can result in data loss.

Procedure

1. From the Afaria Server home page, select *Administrative Tools > Internet Information Services (IIS) Manager*.
2. Right-click Default Website on the left pane.
3. In the connections section, increase the timeout value to meet your needs, then click *OK*.

   When you change this value, it impacts all the Default Web Site members. Ensure you have determined an acceptable value for all sites.

10.7 Uninstalling Afaria Components

Remove Afaria software components using the Microsoft Add/Remove Programs utility.

10.7.1 Uninstalling Afaria Server

Uninstalling an Afaria Server also uninstalls the Afaria Administration console, if installed on the same server. Removing the Afaria Server deletes the software component, but preserves the Afaria database.

Procedure

1. If you are uninstalling a farm server, on the Afaria Administration console go to *Server > Configuration > Server Farm* and set the state to hidden.

   Hiding the farm server removes it from the server selector list.
2. Close all Afaria programs on the server you are uninstalling.
3. Stop all Afaria-related services.
4. Using the Microsoft Add/Remove Programs utility, select the component and remove it.

   The most common reasons for this step to fail include:
   - An Afaria program or related service is still running. Stop the programs and related services and retry the step.
   - Windows Explorer or some other program is using the Afaria installation directory. Close all programs, then restart the machine and retry the step.
   - Afaria system folders are shared with device users. Remove the share from the folder and retry this step.
5. If you are uninstalling a farm server, delete the server entry from the A_SERVER database table.

   If you do not delete this server from the database, it continues to appear on *Server > Configuration > Server Farm* page as an available server.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP