altOS Server Software Release 6.1.0

Version 6.1.0 Final Release Notes

Build numbers:

- Management Server – 6.1.0-1613596712
- OTA Update Server - 2.7.0-1613685449
- Resource Server - 1.4.0-1613602124
- Cloud Messenger - 4.1.0-1613599503
- Certificate Server - 1.0.0-1613667068
- Dispatcher Service-1.3.0-1613600815
- Installer - build 1613765128

Summary Release Notes

Companion Device Operating System

This is a minor altOS Server release with support for altOS 10.1.0 system.

Certificate Server:

- New certificate service to manage device certificates.

Management Server:

- Allow selected table entries to be exported in the Device List view
- Add new policy attribute ‘Stop other containers on entry’
- Configure default recover password per container
- Make Secure Mode option ‘Cellular Nework Access’ attribute modifiable

OTA Update Server:

- Add new columns ‘created date’ and 'version' to the Schedule List view, Channel column is hidden by default.
- Change the default release name to include model + version + build number
- Enable HTTPS by default in Resources Server (S3) configuration

File Server renamed to Resource Server

Installation

- Install guide updated with instructions on adding additional tenants.
- Install scripts and instructions on Certificate Server installation.

Security Improvements

  - Web server - Remove support for TLS v1.0 and TLS v1.1
  - Web server - add security headers to prevent clickjacking and other attacks.
  - Replace SHA1 usage with SHA-256

© 2021 CIS Mobile. All rights reserved

This document is furnished under license or non-disclosure agreement and may be used or copied only in accordance with the terms of such license or non-disclosure agreement. CIS Mobile assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. Except as permitted by such license or non-disclosure agreement, no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of CIS Mobile.

Detailed Release Notes

Certificate Server

This altOS Server release contains features to support PKI integration with the client. altOS devices support PKI keys, enabling stronger authentication, message signature and verification features in the future releases.

The certificate server provides PKI features for the system. The certificate service securely stores altOS server private keys and is used to sign device certificates.

Allow selected table entries to be exported in the Device List view.

Enable selected table entries to be exported. Previously the entire table would be exported when exceuting the 'Export Devices' action on the Devices list view.

Add new policy attribute 'Stop other containers on entry'.

When enabled for a container, all other Regular and Hidden containers will be stopped upon entering the container.

Configure default recover password per container

The default recovery password or pin can now be configured via Policy. This allows the Administrator to specify a unique per container recovery password or pin in place of the previous default values used ('aaaa' and '0000').

Make Secure Mode mode, 'Cellular Nework Access' attribute modifiable

This attribute was disabled in altOS Server 5.5, and is now modifiable. Cellular network access can be enabled in Secure Mode for altOS clients v 10.1.0 and later.

Add new columns 'created date' and 'version' to the Schedule List view, Channel column is hidden by default

The Schedule List view in the OTA update server was modified to include 2 new columns and hide one column.

Change the default release name to include model + version + build number

When creating a release in the OTA update server, the default release name will be populated using information from the import file.

Enable HTTPS by default in Resources Server (S3) configuration

The default connection protocol for AWS S3 connections is set to HTTPS.

Security Improvements

The web server for all altOS servers was updated to remove support for TLS 1.0 and TLS 1.1. Addional security updates were added to prevent clickjacking and other attacks.

SHA1 is replaced with SHA-256. SHA1 was primarily used to calculate hash values for files sent from/to the server.

Bug Fixes

- No event log for password expiration.
- UI Fix: After saving resource server settings, re selecting resource server displays S3 settings.
- UI Fix: Save action on Tenant defaults page performs executes a logout user session.
- Some Icon and wallpaper files greater than 1 MB not displayed on device. Increase max size to 5MB.
- Secure mode crashed if user photo too big, max download size is 100MB.
- Enable update license for auditor role.

- After a new server install, go to Resource Server page, “An unknown error occurred” is displayed.
- UI Fix: install and go to Resource Server page. "An unknown error occurred" displayed.
- UI Fix: Test Connection button on LDAP settings view is cutoff off on small screens.
- User file pattern match is case sensitive, change to case insensitive.
- UI Fix: App configuration available options inconsistent with role permissions.
- Large backup file uploads sometimes timeout

Known Issues:

- Pattern matching in App Configurations will not match against strings containing special characters.