

Trusted Server Setup AAM, MSS, and CMM

Document #: 190

Last Update: 10/22/2013

Page: 1 of 4

Overview

This document outlines the steps for creating and maintaining an Avaya Aura Messaging, Modular Messaging MSS, or CMM Trusted Server used for Mutare applications.

AAM

The AAM must be at release 6.0 or later to use the Trusted Server/Super User feature.

Define a Trusted Server

Go to Server Settings ▶ Trusted Servers screen and add a new Trusted Server entry for Mutare.

AVAYA Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration This Server: aam6

Administration / Messaging

Messaging System (Storage) User Management Class of Service Sites Topology Storage Destinations System Policies Enhanced List Management System Mailboxes System Ports and Access User Activity Log Configuration Reports (Storage) Users Info Mailboxes Remote Users Uninitialized Mailboxes Login Failures Locked Out Users Server Information System Status (Storage) System Status (Application) Alarm Summary Voice Channels (Application) Cache Statistics (Application) Server Settings (Storage) External Hosts Trusted Servers Networked Servers Request Remote Update IMAP/SMTP Settings (Storage) General Options Mail Options IMAP/SMTP Status Telephony Settings (Application) Telephony Integration Server Settings (Application)

Edit Trusted Server

The Edit Trusted Server allows the changing or deletion of a trusted server.

Trusted Server Name	Primary	Password	
		Confirm Password	
Machine Name / IP Address	10.10.1.156	Service Name	Mutare
Minutes of Inactivity Before Alarm	0		
Access to Cross Domain Delivery	no	Special Type	(none)
LDAP Access Allowed	yes	LDAP Connection Security	No encryption required
IMAP4 Super User Access Allowed	yes	IMAP4 Super User Connection Security	Must use SSL or encrypted SASL

Back Save Delete Help

In the example above, the AAM will trust a connection coming from public IP address 10.10.1.156 if it supplies the Trusted Server Name “Primary” and the password entered.



Trusted Server Setup AAM, MSS, and CMM

Document #: 190

Last Update: 10/22/2013

Page: 2 of 4

MSS

The MSS must be at release 3.1 or later to use the Trusted Server/Super User feature.

Define a Trusted Server

Go to Messaging Administration ► Trusted Servers screen and add a new Trusted Server entry for Mutare.

The screenshot shows the 'Add Trusted Server' configuration page in the Avaya Modular Messaging Administration web interface. The page is displayed in a Windows Internet Explorer browser window. The navigation menu on the left includes categories like Messaging Administration, Server Administration, IMAP/SMTP Administration, Server Information, and Utilities. The main form contains the following fields:

Trusted Server Name	EVM	Password	****
		Confirm Password	****
Machine Name / IP Address	10.1.1.100	Service Name	Super User
Minutes of Inactivity Before Alarm	0	Default Community	1
Access to Cross Domain Delivery	no	Special Type	(none)
LDAP Access Allowed	yes	LDAP Connection Security	No encryption required
IMAP4 Super User Access Allowed	yes	IMAP4 Super User Connection Security	Must use SSL or encrypted SASL

At the bottom of the form, there are 'Save', 'Back', and 'Help' buttons. A 'Page Status' message at the bottom indicates: 'One or more fields have been changed. Data shown is unsaved.'

In the example above, the MSS will trust a connection coming from public IP address 10.1.1.100 if it supplies the Trusted Server Name "mutare" and password shown here.



Trusted Server Setup AAM, MSS, and CMM

Document #: 190

Last Update: 10/22/2013

Page: 3 of 4

CMM

The Avaya CM must be at release 5.2 and have the CMM configured to use the Trusted Server feature.

Define a Trusted Server

Go to Server Administration ▶ Trusted Servers screen and add a new Trusted Server entry for Mutare.

The screenshot shows the 'Edit Trusted Server' configuration page in the Avaya Communication System Manager. The page title is 'Edit Trusted Server' and it includes a description: 'The Edit Trusted Server allows the changing or deletion of a trusted server.' The configuration is presented in a table-like form with the following fields:

Trusted Server Name	merak	Password	<input type="text"/>
		Confirm Password	<input type="text"/>
IP Address	192.168.1.48	Service Name	Mutare
Minutes of Inactivity Before Alarm	0	Default Community	1
Access to Cross Domain Delivery	no		
LDAP Access Allowed	yes	LDAP Connection Security	No encryption required
IMAP4 Super User Access Allowed	yes	IMAP4 Super User Connection Security	Must use SSL

At the bottom of the form are buttons for 'Back', 'Save', 'Delete', and 'Help'. The left sidebar contains a navigation menu with categories like 'Administration / Messaging', 'Server Administration', and 'IMAP/SMTTP Administration'.

In the example above, the CMM will trust a connection coming from public IP address 192.168.1.48 if it supplies the Trusted Server Name "merak" and password shown here.



Trusted Server Setup AAM, MSS, and CMM

Document #: 190

Last Update: 10/22/2013

Page: 4 of 4

AAM, MSS, & CMM

Fill out the three fields in yellow with the values you selected for your system. Phone or email them to the Mutare project manager who sent this document.

Field	Notes	Your Values
Trusted Server Name	“mutare”. If the application is installed on a dedicated server, you might want to enter a name that identifies the server.	
Password	You may wish to phone this value to Mutare.	
Machine Name/IP Address	Public IP Address where Mutare application is installed	
Service Name	Change to “Super User” or “Mutare”. Value is not important.	
Minutes of Inactivity	default to 0	0
Access to Cross Domain Delivery	default to no	no
Default Community	Default is “1”	1
Special Type (This value is only used on the AAM and MSS. Not used for CMM.)	Default is (none)	(none)
LDAP Access Allowed	Used for Sync applications.	Yes
LDAP Connection Security	Default is “No encryption required”.	No encryption required
IMAP4 Super User Access Allowed	Used to allow IMAP access to mailboxes without passwords.	Yes
IMAP4 Connection Security	Default is “Must use SSL or encrypted SASL”	Must use SSL or encrypted SASL

