Configuring Fabric Attach on Avaya Ethernet Routing Switch 3500 Series

Release 5.3.2
NN47203-505
Issue 02.02
September 2016

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the

documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document provides instructions to configure Avaya Fabric Attach on the switch.

Chapter 2: New in this document

The following sections detail what is new in *Configuring Fabric Attach on Avaya Ethernet Routing Switch 3500 Series* for this software release.

Fabric Attach Proxy support

Fabric Attach Proxy functionality is supported on ERS 3510 only. FA Proxies support I-SID/VLAN assignment definition and have the ability to advertise these assignments for possible use by an FA Server, if connectivity permits.

For more information about FA Proxy, see the following:

- Fabric Attach fundamentals on page 8
- FA Proxy I-SID-to-VLAN assignment on page 11
- FA data processing on page 12
- FA Proxy and FA Server connection maintenance on page 15
- Creating an I-SID-to-VLAN assignment on an FA proxy on page 27
- Deleting an I-SID-to-VLAN assignment on an FA Proxy on page 28
- Displaying I-SID-to-VLAN assignment information on page 26
- Configuring an I-SID/VLAN assignment on page 41

Chapter 3: Fabric Attach fundamentals

Fabric Attach (FA) extends the fabric edge to devices that do not support Shortest Path Bridging MAC (SPBM). With FA, non-SPBM devices can take advantage of full SPBM support, when support is available.

FA also decreases the configuration requirements on SPBM devices by off-loading some configuration to the attached non-SPBM devices and by automating certain configuration steps that occur most often.

FA Signaling

The FA elements communicate between themselves using FA Signaling . FA Signaling is Avaya's application level protocol that leverages standard network protocols, such as LLDP, to exchange messages and data between FA elements to orchestrate network automation.

FA Network Elements

The FA architecture involves the following FA elements:

- FA Server—An SPB capable network device connected to the fabric edge running the FA agent in FA Server mode. FA Servers receive requests to create services with specific I-SID/VLAN bindings.

  In the SPBM architecture an FA Server is a BEB. FA servers process requests for service creation from FA Proxy and/or FA Clients. An FA Server can operate in SPBM or VLAN provisioning mode.

- FA Proxy—A device running the FA agent in FA Proxy mode.

  An FA Proxy device may be capable of running SPB or not. SPB is always disabled on devices running FA Proxy. FA Proxy mode is enabled by default on devices supporting this mode.

  FA Proxies support I-SID/VLAN assignment definition and have the ability to advertise these assignments for possible use by an FA Server, if connectivity permits.

- FA Client—A non-SPB network attached device running the FA agent in FA Client mode and able to advertise ISID/VLAN binding requests for service creation to an FA Proxy or FA Server.

- FA Standalone Proxy–An FA device running the FA agent in FA Standalone Proxy mode. FA Standalone Proxy supports FA Proxy functionality in environments without an FA Server.

  An FA Standalone Proxy can be used to automate the configuration of traditional VLANs for devices connected to it, such as WLAN Access Points.

  The FA Standalone Proxy does not send provisioning requests upstream. An FA Standalone Proxy automatically accepts requests from FA clients and assumes that the upstream network has been provisioned appropriately.

FA Standalone Proxy can be used in environments where the devices upstream from the FA Standalone Proxy do not support Fabric Attach, but the devices downstream from it support Fabric Attach.

Note:

This release supports FA Proxy functionality (on ERS 3510 only) and Standalone Proxy operation.

FA agent startup and initialization

During the FA agent startup and initialization sequence, the following are restored from non-volatile memory:

- FA service status
- FA port-level settings
- external client proxy status
- message authentication status and keys for all ports
- previously configured I-SID/VLAN assignments
- Zero Touch settings
- FA Standalone Proxy settings
- extended logging support

In a stack environment, FA agent startup and initialization occurs on every unit in the stack, using the data restored from non-volatile memory.

The initialization sequence can also include operations geared towards cleaning-up settings that were previously configured in support of FA I-SID/VLAN assignments that were active on an FA Proxy or an FA Server before a system reset.

FA Element Discovery

An FA agent which controls FA functionality resides on all FA-capable devices (FA Server, FA Proxy, FA Standalone Proxy or FA Client). No agent-specific configuration is necessary.

FA Proxy and FA Server elements control FA through a global FA service setting (global SPBM setting) and through per-port settings that control the transmission of FA information using FA Signaling.

The first stage of establishing FA connectivity involves element discovery. In order for FA discovery to function, FA service and per-port settings must be enabled. Once these settings are enabled, the FA agent advertises its capabilities (FA Server, FA Proxy or FA Client) through FA Signaling. Following discovery, an FA agent is aware of all FA services currently provided by the network

elements to which it is directly connected. Based on this information, an FA Client or an FA Proxy agent can determine whether FA data (I-SID/VLAN assignments) should be exported to an FA Proxy that acts as an external client proxy or an FA Server.

Per-port settings are, by default, enabled on FA Proxies and disabled on FA Servers.

Note:

An FA Proxy can communicate with, at most, one FA Server at a time. If multiple server connections exist, the first discovered server is considered the primary server. Multiple links (trunked) to a single server are supported as long as they form a logical interface. Multiple non-trunked links are not supported and data received on non-primary ports is ignored by an FA Proxy. FA Proxies or FA Clients can connect through a LAG/MLT to two FA Servers which form a Split-LAG or SMLT pair. Connections which may create loops, to multiple servers that are not in Split-LAG or SMLT mode, are not supported.

An FA Server can communicate with multiple, different FA Proxies and FA Clients.

FA LLDP extensions

The Fabric Attach (FA) TLVs described in this section are implemented as extensions to the LLDP standard, using the flexible extension mechanism supported by the standard. These TLVs use TLV type 127 as described in the 802.1ab (LLDP) standard.

Avaya Fabric Attach Element TLV

With the Avaya FA Element TLV, FA elements advertise their FA capabilities. This data forms the basis for FA element discovery and determines the state machine used by FA entities. This information is received, processed and stored by the receiving switch so that it is immediately accessible for internal applications.

FA Element TLV data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm.

The Organizationally Specific Avaya FA Element TLV contains the following data:

- FA Element Type – indicates element capabilities
- FA Element Management VLAN – identifies the management VLAN
- FA Element System ID - unique system identifier used to support element discovery and tracking.
- FA Element State Data - supports the exchange of element state information

The FA Element TLV is included in all LLDPDUs when the FA service is enabled and when the port-level transmission flags associated with this TLV are enabled.

You can view the FA port settings but you cannot update them through the LLDP support. Use the `fa port-enable` command to update the FA port settings.

With the FA service enabled, LLDPDUs containing proprietary Avaya TLVs are transmitted on links that may or may not have Avaya components at the far end. Since the LLDP standard dictates that

unrecognized but well-formed TLVs in received LLDPDUs should be ignored, this should not cause any issues.

Note:

This behavior is different from the way other proprietary Avaya LLDP TLVs are handled. The other proprietary Avaya TLVs are only included in LLDPUs generated on links that have recognized Avaya elements, specifically Avaya telephony gear, at the far end.

Avaya FA I-SID/VLAN Assignment TLV

With the Avaya FA I-SID/VLAN Assignment TLV, an FA Proxy or FA Client distributes I-SID/VLAN assignments to the FA Server. This information is received, processed and stored by the receiving device so that it is immediately accessible for internal applications.

I-SID/VLAN Assignment TLV data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm.

I-SID/VLAN assignment requests can be accepted (activated) or rejected by an FA Server.

The FA I-SID/VLAN Assignment TLV is only included in an LLDPDU when complementary FA element devices (FA Proxy, FA Server, or FA Client) are directly connected. The associated port-level transmit flags must be enabled as well.

The Organizationally Specific Avaya FA I-SID/VLAN Assignment TLV contains the following data:

- VLAN ID – identifies the VLAN component of the I-SID-to-VLAN mapping
- I-SID – identifies the I-SID component of the I-SID-to-VLAN mapping
- Status – contains information related to the processing of the I-SID-to-VLAN mapping

Multiple I-SID/VLAN assignments may be included in a single TLV.

All I-SID/VLAN assignments defined on an FA Proxy, as well as those received from FA Clients when external client proxy support is enabled, start in the pending state. This state is updated based on feedback received from the FA Server. If an assignment is accepted by the FA Server, its state is updated to active. A server may also reject proposed I-SID/VLAN assignments. In this case, the assignment state is updated to rejected.

Avaya TLV Transmit Flags

With the transmit flags, you can choose on a port-level basis, which LLDP TLVs (including the Avaya TLV such as Call Server TLV or FA TLVs) to include in transmitted LLDPDUs, and which to exclude. These flags are independent of the configured TLV data. Therefore, even if data for a specific TLV is configured, the TLV is only included in LLDPDUs on ports for which the TLV is enabled for transmission.

By default, the transmit flags are set to enabled for non-FA Avaya TLVs (the PoE Conservation Levels TLV default depends on the devices's PoE support) on all ports. The transmit flags for the FA Element and FA I-SID/VLAN Assignment TLVs default to enabled on the switch, on all ports. The transmit flag values for the FA TLVs can only be manipulated through the FA support, with the **`fa port-enable`** ACLI command.

FA Proxy I-SID-to-VLAN assignment

Note:

The following section applies to ERS 3510 only.

Although administrators may configure I-SID-to-VLAN bindings on FA Proxies, I-SID-to-VLAN bindings are typically received by FA Proxies from FA Clients. If external client proxy support is enabled, standard processing requirements for bindings received from an FA Client are managed the same way that processing requirements for locally configured bindings are managed.

If an I-SID-to-VLAN assignment is accepted by the FA Server, the assignment state is updated to *active*. If an I-SID-to-VLAN assignment is not accepted by the FA Server, the assignment state is updated to *rejected*.

The FA Proxy receives and displays assignment status information from the FA Server for each pending I-SID-to-VLAN assignment. Possible responses include:

- Assignment accepted (2)
- Rejection: generic (3)
- Rejection: Fabric Attach resources unavailable (4)
- Rejection: VLAN invalid (6)
- Rejection: VLAN resources unavailable (8)
- Rejection: application interaction issue (9)

Note:

Data exchanges (I-SID/VLAN assignments) between an FA Proxy and an FA Server/FA Client are supported, as are exchanges between an FA Server and an FA Proxy/FA Client. FA Proxy to FA Proxy and FA Server to FA Server interactions are not supported.

FA data processing

Note:

This section is applies to ERS 3510 only.

Following discovery, an FA Proxy or FA Client transmits locally-defined I-SID/VLAN assignments through FA Signaling to an FA Server, which accepts or rejects these assignments.

The I-SID/VLAN assignment acceptance by the server can require actions to be performed by the FA agent on both the FA Proxy and the FA Server, to appropriately configure the communication channel (uplink) between the FA Proxy or FA Client and FA Server. Most actions undertaken based on assignment acceptance are undone when the I-SID/VLAN assignment is no longer needed.

I-SID/VLAN assignment rejection by the FA Server requires the FA Proxy to clean up any settings that the FA agent made related to feature operation, as well as log the rejection and any associated error type information for later analysis by an administrator. The amount of clean-up required depends on whether the port VLAN membership was established by the FA Proxy agent or by the administrator outside of the FA feature operation. An uplink port that is associated with a VLAN

because of an accepted FA Proxy I-SID/VLAN assignment, and not because of an explicit administrator port VLAN membership action, will have the port VLAN membership cleared when the related I-SID/VLAN assignment is rejected by the FA Server or deleted by the FA Proxy administrator. *The port tagging status will remain in effect regardless of I-SID/VLAN assignment status, once it has been established by the FA agent.*

VLANs that are automatically created on an FA Proxy due to I-SID/VLAN assignment acceptance are automatically deleted when bindings are rejected or deleted.

No more than a single log message is generated for a rejected I-SID/VLAN assignment, regardless of how many times the assignments have been requested and rejected. Assignments that are rejected, accepted, and later rejected result in a log message being generated for each “new” rejection (two I-SID/VLAN assignment rejection log messages are generated in this case).

FA Proxy I-SID/VLAN assignment addition actions:

- Create port-based VLAN corresponding to I-SID/VLAN assignment VLAN.
- Update port VLAN membership to include I-SID/VLAN assignment VLAN.
- Update port VLAN tagging status to ensure egress traffic is tagged.

FA Server I-SID/VLAN assignment addition actions:

- Create SPBM switched UNI VLAN corresponding to I-SID/VLAN assignment VLAN.
  - C-VLAN join operation does not initiate VLAN creation (VLAN already exists and is associated with the I-SID/VLAN binding I-SID).
- Update downlink port VLAN tagging status to ensure egress traffic is tagged. Tagging status for FA client connections is determined by the client link tagging requirements.
- Update I-SID/VLAN mapping data to ensure Shortest Path Bridging-MAC (SPBM)-switched UNI support is enabled for the I-SID/VLAN/port tuple (in other words, create switched UNI). Port VLAN membership is updated by this action.

Additional actions can be required for I-SID/VLAN binding state transitions involving FA Client-generated data. The communication channel (that is, the downlink) between the FA Client and FA Proxy must be appropriately configured. This can require actions to be performed on the switch.

FA Proxy external client proxy I-SID/VLAN assignment addition actions:

- Update downlink port VLAN membership to include I-SID/VLAN assignment VLAN.
- Update downlink port VLAN tagging status based on the FA Client state data (tagged – ‘tagAll’/ untagged – ‘untagPvidOnly’).

Each of these actions is performed by the FA Proxy and FA Server for each I-SID/VLAN assignment, unless the required data/settings have already been configured by the administrator. The successful transition from ‘pending’ to ‘active’ is gated by the successful completion of these actions. The FA agent tracks which settings have been updated based on I-SID/VLAN assignment processing (comparing them with settings established by the administrator), and cleans-up or undoes the settings that are related to I-SID/VLAN assignment support as much as possible when an assignment is no longer needed.

I-SID/VLAN assignment state transitions from ‘active’ to ‘rejected’ require complementary actions be performed by the FA Proxy and the FA Server to eliminate assignment-related settings:

FA Proxy I-SID/VLAN assignment deletion actions:

- Update uplink port VLAN membership to exclude I-SID/VLAN assignment VLAN.
- Delete port-based VLAN corresponding to I-SID/VLAN assignment VLAN. *Uplink port VLAN tagging status remains unchanged.*

FA Server I-SID/VLAN assignment deletion actions:

- Delete I-SID/VLAN/port association data to disable SPBM-switched UNI support for the I- SID/VLAN/port tuple (to delete switched UNI). This action updates port VLAN membership.
- Delete SPBM-switched UNI VLAN corresponding to I-SID/VLAN assignment VLAN.
  - Previously joined C-VLANs are not deleted.

State transitions related to FA Client-generated bindings require additional complementary actions to be performed by the FA Proxy to eliminate assignment-related settings:

FA Proxy external client proxy I-SID/VLAN assignment deletion actions:

- Update downlink port VLAN membership to exclude I-SID/VLAN assignment VLAN.
- Delete port-based VLAN corresponding to I-SID/VLAN assignment VLAN.

Note:

Downlink port VLAN tagging status remains unchanged

Assignment status data returned by the FA Server for each pending I-SID/VLAN assignment drives the FA Proxy response processing. Assignment rejections can include information to indicate the reason for the rejection.

Rejection error codes include:

- FA resources unavailable(4)–the resources that are required for the FA agent to support additional I-SID/VLAN assignments are currently exhausted. The maximum number of assignments that can be supported has been reached.
- VLAN invalid(6)–the specified VLAN can't be used to create a switched UNI at this time. The VLAN already exists and is either inactive or has an incorrect type for this application. This error is also returned if an FA Client or FA Proxy exports an bindings with an I-SID value of 0 and SPBM provisioning is enabled.
- VLAN resources unavailable(8)–the maximum number of VLANs that can be supported by the device has been reached.
- Application interaction issue(9)–a failure has been detected during FA interactions with the VLAN and/or the SPBM applications. The VLAN operations to create the required SPBM switched UNI VLAN or enable port tagging may have failed or the SPBM operation to create the switched UNI may have failed.

As with the actions initiated to support an assignment addition, actions related to assignment deletion are performed only if the targeted data was created during the I-SID/VLAN assignment addition phase. Previously-existing configuration data is not changed. No artifacts are left behind to indicate that automated operations have taken place, following an addition or deletion sequence. This goal may not always be achievable but all attempts are made to satisfy this requirement.

In addition to explicit I-SID/VLAN assignment state transitions, several events can occur that initiate assignment deletion processing. These include:

- I-SID/VLAN assignment timeout–A “last updated” timestamp is associated with all active assignments on the FA Server. When this value is not updated for a predetermined amount of time, the I-SID/VLAN assignment is considered obsolete. Obsolete assignment data and related settings are removed by the FA server agent. The timeout duration value allows FA Server settings to be maintained if temporary connectivity issues are encountered.

  I-SID/VLAN binding timeout is also performed by an FA Proxy when it is providing client proxy services and FA Client data is present. Processing similar to that performed by the FA Server related to data aging is supported.
- I-SID/VLAN assignment list updates–The current I-SID/VLAN assignment list is advertised by an FA Proxy at regular intervals (dictated by FA Signaling). During processing of this data, an FA Server must handle list updates and delete assignments from previous advertisements that are no longer present. Though these entries would be processed appropriately when they timeout, the FA agent attempts to update the data in real-time and initiates deletion immediately upon detection of this condition.
- FA Server inactivity timeout–If primary FA Server advertisements are not received for a predetermined amount of time, the I-SID/VLAN assignments accepted by the server are considered rejected. I-SID/VLAN assignment data is defaulted (reverts to the ‘pending’ state) and related settings are removed by the FA Proxy agent. The timeout duration value has been chosen to allow FA Proxy settings to be maintained if temporary connectivity issues are encountered.

FA Proxy and FA Server connection maintenance

Note:

This section applies to ERS 3510 only.

An FA Proxy can only interact with one FA Server at a time. If multiple server connections exist, the first discovered server is considered the primary server. All other servers discovered after this point in time are considered alternates. Typically only a single FA Server is discovered. If multiple servers are discovered, an indication is logged to identify this situation in case it is not intended. I-SID/VLAN assignment data is only exchanged between the FA Proxy and the primary FA Server.

When using LACP for uplink/downlink trunk, ports should be aggregated into a trunk and the LACP key should explicitly be associated with a MLT ID through the LACP Key/MLT ID mapping table.

Primary server failure is detected using a capabilities advertisement timeout. Once a predefined period of time without an FA Server advertisement from the current primary server expires, the primary server becomes undefined. Any FA Proxy I-SID/VLAN assignments previously accepted by the server are defaulted (reset to the ‘pending’ state) and related settings are cleared. An informational message (primary server lost) is logged when this transition occurs. I-SID/VLAN assignment data is not advertised until a new primary FA Server is selected. The same algorithm used at startup to select an initial primary server is used to select a new primary server.

FA Proxy/FA Server connectivity using Multi-link Trunking (MLT), Distributed Multi-Link Trunking (DMLT) or Split Multi-Link Trunking (SMLT) connections is supported.

Multiple links associated with the same trunk are treated as a single logical connection. The FA agent reconciles any issues related to MLT, DMLT and SMLT server connectivity and recognizes server uniqueness in the presence of (potentially) multiple capabilities advertisements (that is, FA Signaling received on multiple ports generated by the same server).

In MLT, DMLT and SMLT environments, FA Signaling is generated and received on all links connecting the FA Proxy and FA Server. An FA Proxy receiving an FA Server advertisement determines if a primary FA Server has been selected. If not, the FA Element System ID associated with an advertising FA Server is saved and primary server selection is completed. Once a primary server has been selected, system ID data associated with FA Server advertisements received on other ports is compared against the primary server data. If the system ID values are not the same, an error indication is logged. In all cases, the FA Proxy only generates FA Signaling containing I-SID/VLAN assignment data on the interfaces associated with the primary FA Server.

Note:

The FA Element System ID is structured such that the same system ID is generated on all links associated with a trunk connection between an FA Proxy and an FA Server even in an SMLT scenario where different physical devices are acting as a single logical entity.

In an SMLT environment, an FA Server takes additional actions to ensure that data is synchronized on both SMLT aggregation peers. In this configuration, the FA Server that receives and accepts advertised FA I-SID/VLAN assignments is responsible for generating messages that are sent across the Inter-Switch Trunk (IST) to inform the partner aggregation switch about FA settings that have been configured (for example, SPBM switched UNI VLAN). Similar actions are required when I-SID/VLAN assignments are deactivated.

Agent Stacking functionality

The FA agent is able to function in both standalone and stacked configurations. In a stack, the base unit FA agent acts as the master and pushes its configuration settings to all non-base units (NBUs), to synchronize data across all units. FA agents are active on all units and are able to process stack events as well as data distribution messages.

On an FA Proxy, connections to the primary FA Server can exist on any unit in the stack. When the unit with the active FA Proxy-to-FA primary server interface leaves the stack, any I-SID-to-VLAN assignments accepted by the server are aged-out. I-SID-to-VLAN assignment data is restored to the default *pending* state and related settings are removed by the FA Proxy agent.

FA message authentication and integrity protection

In order to secure the FA communication in terms of data integrity and authenticity, a keyed-hash message authentication code transmitted with FA TLV data is used to protect all FA signaling exchanges. The standard HMAC-SHA256 algorithm is used to calculate the message authentication code (digest) involving a cryptographic hash function (SHA-256) in combination with a shared secret key. The key is symmetric (known by both source and destination parties). By default, FA message

authentication is enabled and a default key is defined to provide secure communication out-of-the-box.

When FA message authentication is enabled, the FA key (default or configured) is used to generate a Hash-based Message Authentication Code (HMAC) digest that is included in all FA TLVs (the FA Element TLV and the FA I-SID/VLAN Assignment TLV).. Upon receipt, the HMAC digest is recomputed for the TLV data and compared against the digest included in the TLV. If the digests are the same, the data is valid. If not, the data is considered invalid and is ignored.

The FA secure communication setting (enabled/disabled) and the symmetric key data are maintained across resets and restored during FA initialization.

Multiple authentication key support provides support for authentication using multiple keys, a user-defined key and a default key. Key usage can be restricted. Only the user-defined key (strict key-mode) or both the user-defined key followed if necessary by the default key (standard key-mode) can be used for authenticating messages. By default, only the user-defined key (strict key-mode) is used for authentication.

Message authentication status, authentication key and key-mode settings are maintained on a per-port basis.

Information related to authentication failures is passed to the EAP/NEAP agent for forwarding to a FA policy server for potential processing when the following criteria are met:

- the interface on which the FA Client is discovered is EAP/NEAP enabled
- the automated FA Client Port Mode Zero Touch option is enabled for FA Client element type

FA Client ingress interface, element type, authentication status, and related key information can be provided for additional upstream client processing.

FA Clients

FA Clients connect to an FA Proxy through standard, non MAC-in-MAC access ports, advertising configured I-SID/VLAN requests to the FA Server. In this scenario, the FA Proxy acts as a client proxy for the FA Client by passing I-SID/VLAN binding requests to a discovered FA Server and returning assignment status information to the FA Client. FA Clients can connect directly to an FA Server, as well.

Note:

External client proxy support must be enabled on an FA Proxy switch before FA client data is accepted by the FA Proxy. By default, external client proxy support is enabled on an FA Proxy.

I-SID/VLAN bindings received from an FA Client by an FA Proxy acting as a proxy for external clients are processed in much the same way locally administered assignments are processed. FA Proxy response processing takes care of VLAN creation and updates VLAN membership*and tagging of the FA Server uplink port if necessary*.

If the I-SID/VLAN client assignment is rejected by the FA Server, the FA Proxy performs any required clean-up tasks and also logs the rejection and any associated error type information for later analysis by an administrator.

Note:

A user assigned to Fail Open VLAN is not removed from I-SID/VLAN bindings using MHSA mode when the RADIUS server becomes unreachable.

FA Zero Touch

FA Zero Touch eases the configuration process on FA-capable devices by automating specific configuration tasks required for FA functionality. For situations when you prefer or require manual configuration of the settings affected by Zero Touch, feature control is provided.

Fabric Attach must be enabled in order for Zero Touch to function. You must manually configure which FA Clients to associate with a Zero Touch option that automates tasks based on FA Clients discovery.

When base Zero Touch functionality is enabled, FA Proxy and FA Client devices can acquire management VLAN data from the connected FA Server or FA Proxy and use it to facilitate manageability and network configuration. When the feature is enabled, base Zero Touch auto-attach operation extracts management VLAN data from the primary FA Server advertisements and potentially uses this data to update the in-use management VLAN. This information can be cascaded to FA Clients, as well.

If the management VLAN being replaced was originally learned by the FA Proxy from FA Element TLV data pushed by the FA Server, the port membership of the now obsolete management VLAN is migrated to the new management VLAN automatically. If there is any user intervention during this automated process (for example, the Zero Touch auto-attach status is modified or the device management VLAN is manually updated) the obsolete management VLAN data remains as is.

Base ZT auto-attach support also transitions the connection between an FA Proxy and an FA Server to *Trusted* if it doesn't already support trusted QoS traffic processing. If the uplink (FA Proxy) or downlink (FA Server) interface is not already associated with a QoS Trusted interface group, a new QoS Trusted interface group ('FaTrustedIfcs') is created if necessary, and the interface is assigned to the interface group. FA Proxy or FA Server connection termination causes the QoS interface group associations to revert to their previous setting, or the default setting if prior setting data is not available.

By default, base Zero Touch support is enabled.

In addition to base Zero Touch functionality, you can configure the following Zero Touch options on an FA device:

IP Address Source Mode Update

When this option is enabled, IP address source mode is updated on the FA Proxy device (receiver) to *DHCP-When-Needed* and initiates DHCP-based IP address acquisition if an IP address is not manually configured.

IP address source mode update only occurs during base Zero Touch processing when a new management VLAN is processed if this option is enabled.

Automated trusted FA Client connection

When this option is enabled, the FA agent examines the list of discovered FA Clients and updates the QoS interface class assignment to 'Trusted' for certain client types, if the interface is not already associated with a 'Trusted' interface class.

QoS interface class assignment data that is updated by FA when an FA Client is discovered resets to the previous QoS interface class assignment when the FA Client information expires. FA Proxy or FA Server connection termination causes the QoS interface group associations to revert to their previous settings, or to default setting if prior setting data is not available. A system reset also causes the QoS interface class assignment for FA-updated interfaces to revert to the previous setting.

All FA updates to QoS settings are dynamic, with the exception of the creation of an FA Trusted QoS interface group ('FaTrustedIfcs').

QoS interface class data is updated based on the discovery and deletion (based on aging) of the following FA Client types:

- Wireless Access Point Type 1
- Wireless Access Point Type 2
- Switch
- Router
- IP Phone
- IP Camera
- IP Video
- Security Device
- Virtual Switch
- Server Endpoint
- ONA SDN
- ONA SPB-over-IP

Automated configuration only applies to FA-enabled ports.

Automated FA Client Port Mode

When this option is enabled and FA Clients are present, the EAP settings for the interface on which the client is discovered, are automatically updated based on the FA Client type. If the FA Clients of the appropriate type are deemed no longer valid (when element aging causes the FA Client to be deleted from the discovered elements list), the EAP port settings revert to the previous state. This is applicable for FA Proxy and FA Server devices.

Automated configuration only applies to FA-enabled ports.

The following FA Client types are supported:

- Wireless Access Point Type 1
- Wireless Access Point Type 2
- Switch
- Router
- IP Phone
- IP Camera
- IP Video
- Security Device
- Virtual Switch
- Server Endpoint
- ONA SDN
- ONA SPB-over-IP

Automated PVID FA Client Port Mode

Enabling this option initiates automatic port PVID, port management VLAN membership and port tagging mode update, based on the type of discovered FA Clients. This is applicable for FA Proxy and FA Server devices. Automated configuration is only applied to FA-enabled ports.

The port tagging mode is updated based on the specified link VLAN tagging requirements signaled by the FA Client in the FA Element TLV state field. The port tagging mode is set to *tagAll* for a tagged link and *untagPvidOnly* for a link carrying both tagged and untagged traffic.

Data updated by Automated PVID FA Client Port Mode when an FA Client is discovered resets to the previous value when the FA Client information expires.

The following FA Client types are supported:

- Wireless Access Point Type 1
- Wireless Access Point Type 2
- Switch
- Router
- IP Phone
- IP Camera
- IP Video
- Security Device
- Virtual Switch
- Server Endpoint
- ONA SDN
- ONA SPB-over-IP

Note:

The `auto-port-mode-fa-client` option is incompatible with the `auto-pvid-mode-fa-client` option. You cannot enable these Zero Touch options for a client type at the same time.

FA Standalone Proxy

FA Standalone Proxy introduces FA Proxy functionality in environments without an FA Server. Regardless of whether the FA Standalone Proxy upstream device is a non-Avaya component or an Avaya device on which FA Server functionality is not available, FA Standalone Proxy operation supports standard FA Proxy processing as if an FA Server has been discovered.

Note:

In FA Standalone Proxy mode, I-SID values are not specified and are implicitly 0. Only bindings with an I-SID value equal to 0 are accepted for processing.

In FA Standalone Proxy mode you must provide the FA Server uplink information, which is typically gathered through FA Server discovery. Once you provide this information, FA Standalone Proxy mode operates as if an FA Server has been discovered and is accepting I-SID/VLAN binding requests. The binding clean-up is similar to an FA Server timeout event, and occurs when the static uplink is deleted and when FA Standalone Proxy operation is disabled.

Note:

No interactions with an FA Server are supported in FA Standalone Proxy mode.

Note:

This release supports FA Proxy functionality (on ERS 3510 only) and Standalone Proxy operation.

Note:

Before creating static uplink over a LAG, it`s highly recommended to manually bind LACP-key to an MLT-ID.

When using LACP for uplink trunk, ports should be aggregated into trunk.

EAP and FA

With EAP and FA, FA-capable switches or stacks can forward traffic from EAP/NEAP clients over the SPB cloud. The traffic for authenticated clients is mapped to I-SIDs received from the Avaya Identity Engines RADIUS server.

You must configure the desired bindings for EAP/NEAP clients on the RADIUS server. When confirming the authentication request, the RADIUS server also sends the corresponding binding for the EAP/NEAP client.

In MHSA and MHMV modes, the VLAN from the I-SID/VLAN binding received from the RADIUS server is automatically created if it is not already present.

The following VLAN types are automatically created:

- port-based VLANs, if the EAP/NEAP client is connected via an FA Proxy
- Switched UNI VLANs, if the EAP/NEAP client is connected via an FA Server

After an EAP/NEAP client is disconnected, the switch cleans-up the binding associated with the client, if no other EAP/NEAP client on that port uses it.

When an EAP/NEAP client successfully authenticates on an FA Proxy, the client port becomes a member of the VLAN from the I-SID/VLAN pair. The FA Proxy sends to the FA Server the binding received from the RADIUS server. If the FA Server rejects all the bindings, the client is disconnected. EAP clients are moved from AUTHENTICATED state to HELD state.

Note:

In case of a rejected binding, a delay of up to 30 seconds may exist from the time the client authenticates on the FA Proxy until the FA Server rejection response is received by the FA Proxy. Therefore, EAP client traffic may flow for up to 30 seconds until dropped.

On an FA Server, when an EAP/NEAP device is authenticated and an FA binding is received from the RADIUS server, a switched-UNI is created. This is automatically cleaned-up when the client is disconnected.

Access Points authentication

In MHSA mode, the switch also supports NEAP authentication for Access Points. Because Access Points cannot authenticate via EAP, the MHSA mode was improved as follows:

- MHSA now allows the first connected client to be a NEAP client. For each MAC seen on the port, the switch sends an Access Request to the RADIUS Server. After the first successful authentication, a configured number of auto-learned clients are granted access, as in previous MHSA behavior.
- a new option, 'no-limit', is available for configuring the switch to support an unlimited number of NEAP auto-learned clients. You can use this option when an Access Point connected to the switch supports an indeterminate number of devices.

  Previously, after the first successful EAP authentication, the switch allowed only a limited number of auto-learned NEAP clients.

  When the 'no-limit' option is enabled, the port forwards the traffic from all the devices on that port, without limiting their number. When the Access Point disconnects, the switch clears the mac-address-table for that port and blocks again all traffic. By default, the 'no-limit' option is disabled.

Note:

EAP ports configured in MHSA mode with AP detected as an FA client will not be added to the Fail Open VLAN.

VSAs

The following is a list of VSAs added to support EAP FA functionality:

VSAs sent from RADIUS server to switch:

- Avaya-Fabric-Attach-VLAN-ISID

  This VSA consists of a (VLAN, I-SID) pair.

  Multiple (VLAN, I-SID) pairs are processed only in MHSA mode.

- Avaya-Auto-VLAN-Create

  If this VSA is set to TRUE, the VLANs received in all (VLAN, I-SID) pairs will be automatically created if they do not exist. This VSA is processed only in MHSA and MHMV modes.

- Avaya-Fabric-Attach-VLAN-PVID

  This VSA contains the value of the PVID that should be set on the port with the authenticated client. The Avaya-Fabric-Attach-VLAN-PVID VSA is processed only in MHSA mode.

VSAs sent from switch to RADIUS server:

- Avaya-Fabric-Attach-Mode

  This VSA can have the following values:

  - 0 or not sent, when Switch is assumed to have no concept of SPB/AutoProv
  - 1, when the switch is an FA Server in VLAN provision mode
  - 2, when the switch is an FA Server in SPBM mode
  - 3, when the switch is an FA Proxy with the connected FA Server in VLAN provision mode
  - 4, when the switch is an FA Proxy with the connected FA Server in SPBM mode
  - 5 , when the switch is a FA Standalone Proxy

- Avaya-Fabric-Attach-Client-Type

  This VSA can have the following values:

  - 1, FA Element Type Other
  - 2, FA Server
  - 3, FA Proxy
  - 4, FA Server No Authentication
  - 5, FA Proxy No Authentication
  - 6, FA Client – Wireless AP Type 1 [clients direct network attachment]
  - 7, FA Client – Wireless Ap Type 2 [clients tunneled to controller]

- Avaya-Fabric-Attach-Client-Id

  This VSA contains the MAC address of the FA client, exported via FA Signaling.

Chapter 4: Fabric Attach configuration using the Avaya Command Line Interface

This section provides procedural information you can use to configure Fabric Attach (FA) using the Avaya Command Line Interface (ACLI).

Displaying FA-specific settings

Use this procedure to display the FA configuration status.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display the FA configuration status, enter the following command:

   ```
   show fa agent
   ```

Example

This example shows sample output for the **`show fa agent`** command in FA Proxy mode.

```
Switch(config)#show fa agent

Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Proxy
Fabric Attach Zero Touch Status: Enabled
Fabric Attach Auto Provision Setting: Proxy
Fabric Attach Provision Mode: Disabled
Fabric Attach Client Proxy Status: Enabled
Fabric Attach Standalone Proxy Status: Disabled
Fabric Attach Agent Timeout: 240 seconds
Fabric Attach Extended Logging Status: Disabled
Fabric Attach Primary Server Id: <none>
Fabric Attach Primary Server Descr: <none>

Switch
```

This example shows sample output for the **`show fa agent`** command in FA Proxy Standalone mode.

```
Switch(config)#show fa agent
```

```
Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Proxy
Fabric Attach Zero Touch Status: Enabled
Fabric Attach Provision Mode: Legacy
Fabric Attach Client Proxy Status: Enabled
Fabric Attach Standalone Proxy Status: Disabled
Fabric Attach Agent Timeout: 240 seconds
Fabric Attach Extended Logging Status: Disabled

Switch(config)#
```

Displaying Fabric Attach elements

Use this procedure to display discovered Fabric Attach elements.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display the discovered FA elements, enter the following:

   ```
   show fa elements [<portlist> | trunk <trunknumber> | element-type
   {server | proxy | client} | auth-status  {auth-pass | auth-fail |
   not-auth} | client-type <6-17>]
   ```

Example

The following example displays sample output for the `show fa elements` command.

```
================================================================================
Fabric Attach Discovered Elements
================================================================================
UNIT/                MGMT                                              ELEM ASGN
PORT    TYPE         VLAN  STATE  SYSTEM ID                            AUTH AUTH
--------------------------------------------------------------------------------
1/5     Server       1234  T / S  6c:fa:58:dc:fc:00:00:00:01:05     AP   AP
1/36    Client       1     U / D  fc:a8:41:fa:f8:00:00:00:00:24     AP   N
================================================================================
                    Fabric Attach Authentication Detail
================================================================================
UNIT/                      ELEM OPER                ASGN OPER
PORT   EXPANDED TYPE       AUTH STATUS              AUTH STATUS
--------------------------------------------------------------------------------
1/5    Server (Auth)       successAuth              successAuth
1/36   Switch              successAuth              none
State Legend: (Tagging/AutoConfig)
T=Tagged, U=Untagged, D=Disabled, S=Spbm, V=Vlan, I=Invalid
Auth Legend:
AP=Authentication Pass, AF=Authentication Fail, NA=Not Authenticated, N=None
--------------------------------------------------------------------------------
2 out of 2 total number of Fabric Attach discovered elements displayed
--------------------------------------------------------------------------------
```

Field	Definition
State	FA Element TLV state field data
Elem Auth	FA Element TLV authentication status
Asgn Auth	FA I-SID/VLAN Assignment TLV authentication status
Elem Oper Auth Status	FA Element TLV authentication status detail data
Asgn Oper Auth Status	FA I-SID/VLAN Assignment TLV authentication status detail data

Variable Definitions

The following table describes the parameters for the `show fa elements` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to display discovered FA elements.
trunk <trunknumber>	Specifies a trunk number for which to display discovered FA elements.
auth-status {auth-pass | auth-fail | not-auth}	Displays only specified authorized status FA elements.
element-type {server | proxy | client}	Displays only specified element type.
client-type <6-17>	Displays only specified client type.

Displaying I-SID-to-VLAN assignment information

Use this procedure to display information about I-SID-to-VLAN assignments.

This procedure applies to ERS 3510 only.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display I-SID-to-VLAN assignment information on an FA Proxy, enter the following commands:

   ```
   show fa i-sid [<1-16777214>]
   ```

   ```
   show i-sid [<1-16777214>]
   ```

   OR

   ```
   show fa assignment [<1-16777214>]
   ```

   ```
   show i-sid [<1-16777214>]
   ```

Example

The following example displays sample output for the **show fa i-sid** command.

```
Switch(config)#show fa i-sid

 I-SID    VLAN     Source       Status
--------  ----  -------------  --------
500       5     Proxy          Active
501       25    Client         Active
600       6     Proxy, Client  Active
13849     138   Proxy          Rejected (VLAN invalid)
16000000  1000  Proxy          Rejected (application interaction issue)
```

Variable definitions

The following table describes the parameters for the **show fa i-sid [<1–16777214>]** or **show fa assignment [<1–16777214>]** command.

Variable	Value
[<1-16777214>]	Specifies the Fabric Attach I-SID for which to display I-SID-to-VLAN assignment information. Values range from 1 to 16777214. If you do not specify a I-SID value, the switch displays information for all configured I-SID-to-VLAN assignments.

Creating an I-SID-to-VLAN assignment on an FA proxy

About this task

Use this procedure to create an association between an I-SID and a VLAN on an FA Proxy, when SPBM is disabled on switch.

This procedure applies to ERS 3510 only.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. To create an I-SID-to-VLAN assignment, enter the following command:

   ```
   i-sid <1–16777214> vlan <1–4094>
   ```

Result

Each FA Proxy I-SID-to-VLAN assignment creates a C-VLAN User Network Interface (UNI) when the assignment is active and accepted by an FA server.

Example

The following example creates an association between I-SID 600 and VLAN 3:

```
Switch(config)#i-sid 600 vlan 3
Switch(config)#
```

Variable definitions

The following table describes the parameters for the `i-sid <1-16777214> vlan <1-4094>` command

Variable	Value
i-sid *<1-16777214>*	Specifies the I-SID to associate with the selected VLAN. Values range from 1 to 16777214.
vlan *<1-4094>*	Specifies the VLAN to associate with the selected I-SID. Values range from 1 to 4094.

Deleting an I-SID-to-VLAN assignment on an FA Proxy

Use this procedure to remove the association between an I-SID and a VLAN on an FA Proxy.

This procedure applies to ERS 3510 only.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To remove a specific I-SID-to-VLAN assignment, enter the following command:

   ```
   no i-sid <I-SID> vlan <VLAN>
   ```

3. To remove all configured I-SID-to-VLAN assignments, enter the following command:

   ```
   default i-sid
   ```

Variable definitions

The following table describes the parameters for the `no i-sid <I-SID> vlan <VLAN>` command

Variable	Value
i-sid *<1-16777214>*	Specifies the I-SID of the specific I-SID-to-VLAN assignment to remove. Values range from 1 to 16777214.
vlan *<1-4094>*	Specifies the VLAN of the specific I-SID-to-VLAN assignment to remove. Values range from 1 to 4094.

Configuring external client proxy support

Use this procedure to enable or disable external client proxy support.

About this task

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable external client proxy support, enter either of the following commands:

   ```
   fa proxy
   ```

   OR

   ```
   default fa proxy
   ```

3. To disable external client proxy support, enter the following command:

   ```
   no fa proxy
   ```

Configuring FA on switch ports

Use this procedure to enable or disable the FA operation on one or more switch ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To configure the FA operation on switch ports, enter the following command:

   ```
   [no][default] fa port-enable [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the `[no][default] fa port-enable [<portlist>]` command.

Variable	Value
[<portlist>]	Enables the FA operation on the specified switch port or ports. If you do not specify a port, the FA operation is enabled on all switch ports.
[no]	Disables the FA operation on the specified switch port or ports. If you do not specify a port or ports, the FA operation is disabled on all switch ports.
[default]	Restores the FA operation on all switch ports to default.

Displaying switch port FA operation status

Use this procedure to display per-port FA operation status.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display FA configuration information, enter one of the following commands:

   ```
   show fa port-enable [<portlist> | enabled-port | disabled-port | enabled-auth | disabled-auth]
   ```

   OR

   ```
   show fa interface [<portlist> | enabled-port | disabled-port | enabled-auth | disabled-auth]
   ```

Example

The following example displays sample output for the `show fa port-enable` command.

```
Switch(config)#show fa port-enable

                            Service
Unit Port IfIndex Trunk Advertisement Authentication Keymode
---- ---- ------- ----- -------------------- --------------
1    1    1                 Enabled   Enabled     Strict
1    2    2                 Enabled   Enabled     Strict
1    3    3                 Enabled   Enabled     Strict
1    4    4         2       Enabled   Enabled     Standard
1    5    5         2       Enabled   Enabled     Standard
1    6    6                 Enabled   Enabled     Strict
```

Variable Definitions

The following table describes the parameters for the `show fa port-enable` or `show fa interface` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to display FA operation status. If you do not specify a port or ports, the switch displays FA operation status for all switch ports.
enabled-port	Displays only FA enabled ports.
disabled-port	Displays only FA disabled ports.
enabled-auth	Displays only authentication enabled ports.
disabled-auth	Displays only authentication disabled ports.

Configuring the FA authentication key

Use the following command to configure the FA authentication key on specified ports.

Note:

You can configure the FA authentication key only on secure images.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the FA authentication key:

   ```
   [default] fa authentication-key <portlist>
   ```

   Enter the authentication key, and then re-enter the key for confirmation. For security purposes, key data is hidden.

Variable Definitions

The following table describes the parameters for the `fa authentication-key` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to define the authentication key.

Configuring FA message authentication support

Use the following procedure to configure the FA message authentication support on specified ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the FA message authentication support:

   ```
   fa message-authentication [<PortList>] [key-mode <strict | standard>]
   ```

3. **(Optional)** Reset the FA message authentication support to default:

   ```
   default fa message-authentication
   ```

   Note:

   The default setting is *enabled*.

4. **(Optional)** Disable the FA message authentication support:

   ```
   no fa message-authentication [<PortList>]
   ```

Variable Definitions

The following table describes the parameters for the `fa message-authentication` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to enable the FA message authentication support.
key-mode <strict | standard>	Specifies the Authentication key usage setting — the user-defined authentication key (strict) or both the user-defined and default authentication keys (standard) are used for FA TLV data authentication. Default key-mode is strict.

Configuring FA VLANs

Use this procedure to create or delete FA VLANs on an FA Proxy or FA Standalone Proxy.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To create FA VLANs, enter the following command:

   ```
   fa vlan <LINE>
   ```

3. To delete FA VLANs, enter the following command:

   ```
   no fa vlan <LINE>
   ```

4. To delete all configured FA VLANs, enter the following command:

   ```
   default fa vlan
   ```

Example

The following is an example of creating an FA VLAN and verifying the configuration.

```
Switch(config)#fa vlan 6
Switch(config)#show fa vlan

VLAN           Source              Status
----  -------------------------  --------
6     Proxy                      Pending

Binding Count: 1
```

Variable Definitions

The following table describes the parameters for the `fa vlan` command.

Variable	Value
[<LINE>]	Specifies an individual VLAN ID or a range of VLAN IDs to create. A VLAN ID can range from 1 to 4094.

Displaying Fabric Attach VLAN information

Use this procedure to display Fabric Attach-specific VLAN information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display Fabric Attach VLAN information, enter the following command:

   ```
   show fa vlan [<1-4094>]
   ```

Example

The following example displays sample output for the `show fa vlan` command.

```
Switch(config)#show fa vlan

VLAN    Source      Status
----  -----------  --------
1007  Proxy        Pending
1008  Proxy        Pending
```

Enabling or disabling FA Zero Touch support

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. To enable FA Zero Touch support on an FA Proxy, FA Server, or FA Standalone Proxy, enter the following command:

   ```
   fa zero-touch
   ```

3. To disable FA Zero Touch support on an FA Proxy, FA Server, or FA Standalone Proxy, enter the following command:

   ```
   no fa zero-touch
   ```

4. To reset the FA Zero Touch support state to default, enter the following command:

   ```
   default fa zero-touch
   ```

Configuring FA Zero Touch options

Use this procedure to configure FA Zero Touch option settings..

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. To enable an FA Zero Touch option, enter the following command:

   ```
   fa zero-touch-options {{auto-port-mode-fa-client | auto-pvid-mode-
   fa-client | auto-trusted-mode-fa-client} [client-type {hint |
   <6-17>}] | ip-addr-dhcp}
   ```

Note:

The `auto-port-mode-fa-client` option is incompatible with the `auto-pvid-mode-fa-client` option. You cannot enable both of these Zero Touch options for a client type at the same time.

3. To disable a specific FA Zero Touch option, enter the following command:

   ```
   no fa zero-touch-options {{auto-port-mode-fa-client | auto-pvid-mode-fa-client | auto-trusted-mode-fa-client} | ip-addr-dhcp}
   ```

4. To clear all FA Zero Touch option settings, enter the following command:

   ```
   default fa zero-touch-options
   ```

Variable Definitions

The following table describes the parameters for the `fa zero-touch-options` command.

Variable	Value
auto-port-mode-fa-client	Automates the configuration of EAP port modes.
auto-pvid-mode-fa-client	Automates client PVID/Mgmt VLAN updates.
auto-trusted-mode-fa-client	Automates the FA Client connection default QoS treatment.
ip-addr-dhcp	Automates DHCP IP address acquisition.

Note:

Default FA client types WAP Type 1 (6) and Switch (8) are associated with the client type-specific Zero Touch options if no client-type data is provided with the CLI commands.

Displaying FA Zero Touch option settings

Use this procedure to verify the FA Zero Touch option settings.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display the FA Zero Touch option settings, enter the following command:

   ```
   show fa zero-touch-options [client-data]
   ```

Example

The following is an example of configuring and displaying FA Zero Touch options.

```
Switch(config)#fa zero-touch-options auto-port-mode-fa-client client-type 6,14-16
Switch(config)#show fa zero-touch-options

Fabric Attach Zero Touch Options:

    ip-addr-dhcp
    auto-port-mode-fa-client
```

The following is an example of displaying client data.

```
Switch(config)#show fa zero-touch-options client-data

Zero Touch Client Data

Type            Client Name                 Applicable Zero Touch Options
----  --------------------------------  -----------------------------------
6     wap-type1                         auto-port-mode
7     wap-type2
8     switch
9     router
10    phone
11    camera
12    video
13    security-dev
14    virtual-switch                    auto-port-mode
15    srvr-endpt                        auto-port-mode
16    ona-sdn                           auto-port-mode
17    ona-spb-over-ip

Type                        Client Description                          Origin
---- ------------------------------------------------------------- --------
6    Wireless AP (Type 1)                                          Standard
7    Wireless AP (Type 2)                                          Standard
8    Switch                                                        Standard
9    Router                                                        Standard
10   IP Phone                                                      Standard
11   IP Camera                                                     Standard
12   IP Video                                                      Standard
13   Security Device                                               Standard
14   Virtual Switch                                                Standard
15   Server Endpoint                                               Standard
16   ONA (SDN)                                                     Standard
17   ONA (SpbOIp)                                                  Standard
Zero Touch Client Data

Switch(config)#
```

Configuring FA Standalone Proxy mode

Use this procedure to enable or disable the FA Standalone Proxy mode on the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. To enable FA Standalone Proxy mode, enter the following command:

   ```
   fa standalone-proxy
   ```

3. To disable FA Standalone Proxy mode, enter the following command:

   ```
   no fa standalone-proxy
   ```

4. To restore the FA Standalone Proxy mode to default, enter the following command:

   ```
   default fa standalone-proxy
   ```

   Note:

   FA Standalone Proxy mode is disabled by default on an FA Proxy.

   Note:

   ERS 3500 supports FA Standalone Proxy mode operation only.

Displaying FA uplink values

Use this procedure to display FA static uplink values used in FA Standalone Proxy mode.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display FA static uplink values, enter the following command:

   ```
   show fa uplink
   ```

Example

The following example displays sample output for the `show fa uplink` command.

```
Switch(config)#show fa uplink

Fabric Attach Static Uplinks:
    port - 0
    trunk - 8 (dynamic MLT [LAG admin key 300] - active)
```

Configuring the static uplink for FA Standalone Proxy mode

Use this procedure to specify a port or trunk to use as a static uplink associated with FA Standalone Proxy operation.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To specify a port uplink or a trunk uplink to use in FA Standalone Proxy mode, enter the following command:

   ```
   fa uplink {port <port> | trunk <trunkId>}
   ```

3. To clear static uplink data, enter the following command:

   ```
   no fa uplink
   ```

Variable Definitions

The following table describes the parameters for the `fa uplink` command.

Variable	Value
<port>	Specifies the port to use as a static uplink.
<trunkId>	Specifies the trunk ID to use as a static uplink.

Configuring Fabric Attach extended-logging

Use the following procedure to configure Fabric Attach extended-logging.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable Fabric Attach extended-logging:

   ```
   fa extended-logging
   ```

3. Disable Fabric Attach extended-logging:

   ```
   no fa extended-logging
   ```

Configuring the FA timeout

Use this procedure to configure the FA timeout. The default is 240 seconds.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To configure the FA timeout, enter the following command:

   ```
   fa timeout <45-480>
   ```

3. To reset the timeout to its default value, enter the following command:

   ```
   default fa timeout
   ```

Chapter 5: Fabric Attach configuration using Enterprise Device Manager

Use the procedures in this section to configure Fabric Attach (FA) using Enterprise Device Manager.

Configuring Fabric Attach

Use this procedure to configure Fabric Attach.

Procedure

1. From the navigation tree, select **Edit > Fabric Attach**.
2. Click the **Agent** tab.
3. To set the Auto Provision mode to FA Proxy, click **proxy** in the **AutoProvision** field.
4. To enable or disable FA Standalone Proxy mode, click **enable** or **disable** in the **StandaloneProxy** field.
5. To enable or disable external client proxy support, click **enable** or **disable** in the **ClientProxy** field.
6. Specify the port to use as a static uplink associated with FA Standalone Proxy operation in the **UplinkPort** field.
7. Specify the trunk to use as a static uplink associated with FA Standalone Proxy operation in the **UplinkTrunk** field.
8. Specify the agent timeout in the **Timeout** field.
9. To enable or disable extended logging, click **enable** or **disable** in the **ExtendedLogging** field.
10. To enable or disable Zero Touch support, click **enable** or **disable** in the **ZeroTouchService** field.
11. To enable Zero Touch options, select the appropriate checkbox in the **OptionFlags** field.
12. Click **Apply**.

Variable definitions

Use the data in the following table to use the **Agent** tab.

Variable	Value
Service	Displays the service status.
ElementType	Displays the element type.
ProvisionMode	Displays the provision mode status
AutoProvision	Displays the Auto Provision mode.
StandaloneProxy	Specifies whether FA Standalone Proxy mode is enabled or disabled. The default is disabled.
ClientProxy	Specifies whether external client proxy is enabled or disabled. The default is enabled.
UplinkPort	Specifies the port to use as a static uplink associated with FA Standalone Proxy operation.
UplinkTrunk	Specifies the trunk to use as a static uplink associated with FA Standalone Proxy operation.
Timeout	Specifies the agent timeout in seconds. The default value is 240 seconds.
ExtendedLogging	Specifies whether extended logging is enabled or disabled. The default is disabled.
ZeroTouchService	Specifies whether Zero Touch support is enabled or disabled. The default is enabled.
OptionFlags	Specifies the option flags for Zero Touch: • **ipAddrDhcp**— automates DHCP IP address acquisition. The default is enabled. • **autoPortModeFaClient** — automates the configuration of EAP port modes • **autoTrustedModeFaClient**— automates the FA Client connection default QoS treatment • **autoPvidModeFaClient** — automates client PVID/Mgmt VLAN updates

Configuring an I-SID/VLAN assignment

Use the following procedure to configure an I-SID/VLAN assignment on an FA Proxy.

This procedure applies to ERS 3510 only.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit**.
2. Click **Fabric Attach**.

3. In the work area, click the **I-SID** tab.
4. Click **Insert**.
5. Specify an I-SID in the **Isid** field.
6. Specify a VLAN in the **Vlan** field.
7. Click **Insert**.

Variable definitions

Use the data in the following table to use the **I-SID** tab.

Name	Description
Isid	Specifies the I-SID to associate with a VLAN.
Vlan	Specifies the VLAN to associate with an I-SID.
State	Indicates the state of the VLAN/I-SID assignment.
Source	Indicates the source of the VLAN/I-SID assignment.

Configuring per-port FA settings

Use the following procedure to enable or disable FA Signaling or to configure FA message authentication.

Procedure

1. From the navigation tree, select **Edit**.
2. In the Edit tree, double-click **Fabric Attach**.
3. On the work area, click the **Ports** tab.
4. To enable or disable the transmission of FA information in FA Signaling, select **enabled** or **disabled** in the **State** field for a specific port or ports.
5. To enable or disable message authentication, select **enabled** or **disabled** in the **MsgAuthStatus** field for a specific port or ports.
6. To configure the authentication key, enter an alphanumeric string of up to 32 characters in the **MsgAuthKey** field for a specific port or ports.
7. To configure the authentication key usage, select **strict** or **standard** in the **MsgAuthKeymode** field for a specific port or ports.
8. Click **Apply**.

Variable Definition

Variable	Value
IfIndex	Indicates the interface for which to configure FA operation and message authentication.
State	Enables or disables FA operation on the interface.
MsgAuthKey	Configures the authentication key for the specified interface.
MsgAuthStatus	Enables or disables FA message authentication on the interface.
MsgAuthKeymode	Specifies the Authentication key usage setting — the user-defined authentication key (strict) or both the user-defined and default authentication keys (standard) are used for FA TLV data authentication. Default key-mode is strict.

Displaying Fabric Attach elements

Use the following procedure to view discovered FA elements.

Procedure

1. In the navigation tree, expand the following folders: **Configuration>Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **Elements** tab.

Variable definitions

Use the data in the following table to use the **Elements** tab.

Name	Description
Ifindex	Indicates the interface through which the FA element was discovered.
Type	Indicates the FA element type.
Vlan	Indicates the management VLAN advertised by the FA element.
Id	Indicates the FA Element System ID, which is the unique system identifier used for connection management and limited device state distribution.

Table continues…

Name	Description
State	Indicates the state flag data associated with the discovered FA element.
Auth	Indicates the authentication status for the discovered element.
OperAuthStatus	Displays FA Element TLV authentication status detail data.
AsgnsAuth	Indicates FA I-SID/VLAN Assignment TLV authentication status.
AsgnsOperAuthStatus	Displays FA I-SID/VLAN Assignment TLV authentication status detail data.

Automating configurations for FA Clients

Use the following procedure to automate configurations for specific types of FA Clients.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **Zero Touch Client** tab.
4. To automate configurations for a specific FA Client type, double-click the corresponding **OptionFlags** field, select the appropriate check-box and click **Ok**.
5. Click **Apply**.

Variable definitions

Use the data in the following table to use the **Zero Touch Client** tab.

Name	Description
Type	Indicates the FA Client type ID.
Descr	Indicates the FA Client type.
OptionFlags	Opens the **OptionFlags** dialog box to specify the automated configurations for an FA Client type. • autoPortModeFaClient: Automates the configuration of EAP port modes. • autoTrustedModeFaClient: Automates the FA Client connection default QoS treatment. • autoPvidModeFaClient: Automates client PVID/Mgmt VLAN updates.

Table continues…

Name	Description
Disable all	Clears all options.
Select all	Selects all available options.
Ok	Confirms the selected options.
Close	Closes the **OptionFlags**dialog box.

Chapter 6: Related Resources

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Documentation

See *Documentation Reference for Avaya Ethernet Routing Switch 3500 Series*, NN47203-101 for a list of the documentation for this product.

For more information about new features of the switch and important information about the latest release, see *Release Notes for Avaya Ethernet Routing Switch 3500 Series*, NN47203-400.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 3500 Series*, NN47203-504.

For the current documentation, see the Avaya Support website: www.avaya.com/support.

Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
8D00020E	Stackable ERS and VSP Products Virtual Campus Offering

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.

3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Subscribing to e-notifications

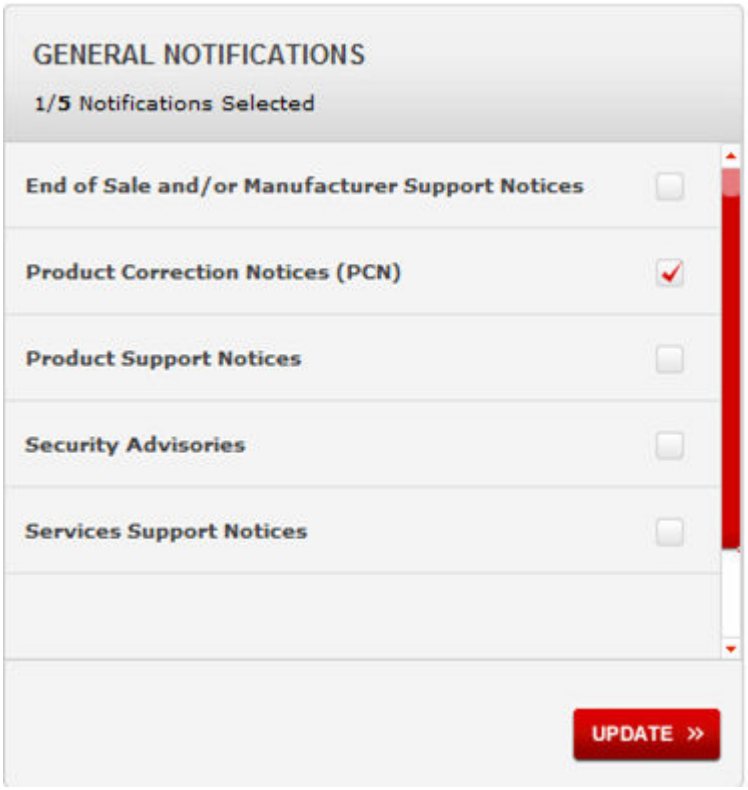
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

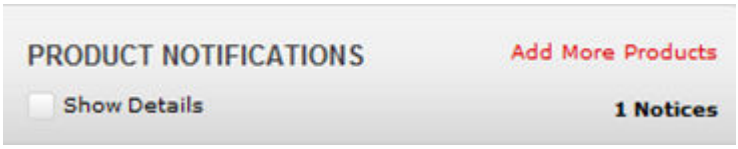
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

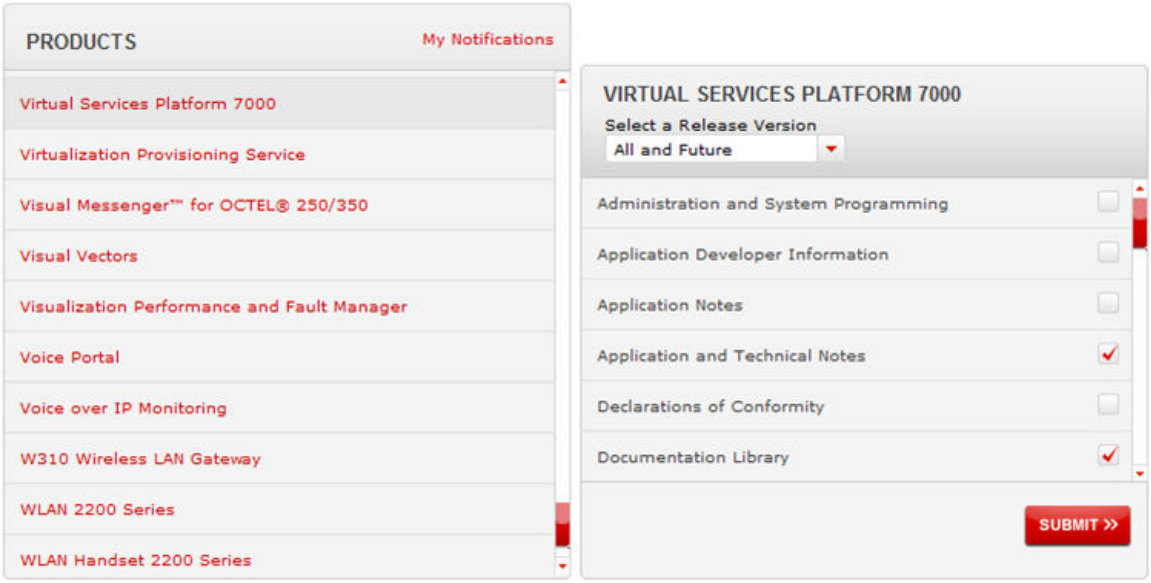
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.