ISW Series Fabric Attach

User Guide

9036850-00 Rev AA
October 2020

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

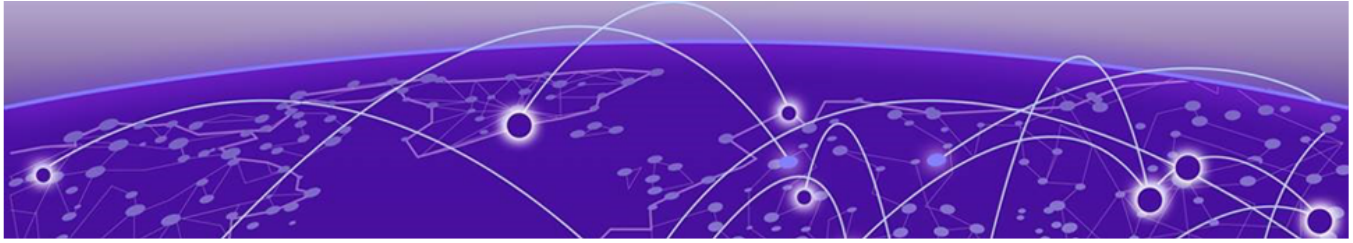
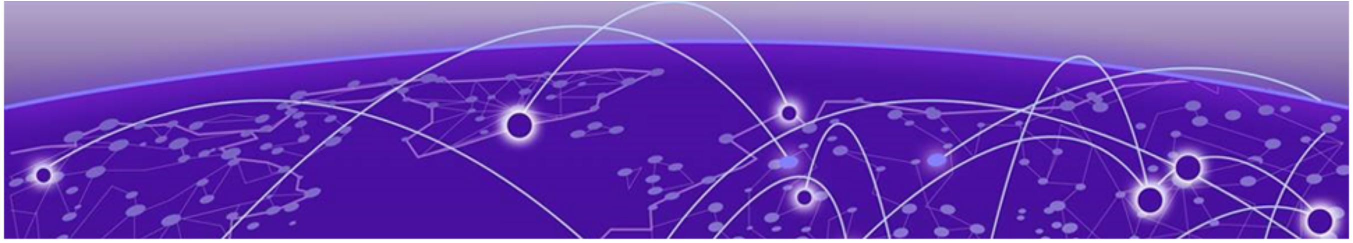


Table of Contents



Preface

This section describes the text conventions used in this document, where you can find additional information, and how you can provide feedback to us.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product.
📝	Note	Useful information or instructions.
➡	Important	Important features or instructions.

Table 1: Notes and warnings (continued)

Icon	Notice type	Alerts you to...
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, `member[member...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and software compatibility for Extreme Networks products

Extreme Optics Compatibility

Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).

3. Select the products for which you would like to receive notifications.

   Note
   You can modify your product selections or unsubscribe at any time.

4. Select **Submit**.

Providing Feedback

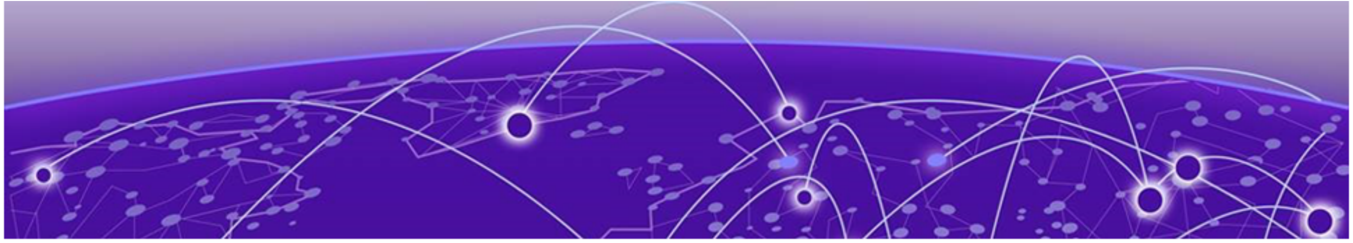
The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



Fabric Attach

The following sections provide conceptual information to help you understand and configure Fabric Attach on switch.

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 an 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.

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

  An FA Proxy device may or may not be capable of running SPB. 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. Non-FA clients without an FA agent are supported through the FA EAP support.
- 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.

FA Server, FA Proxy and FA Standalone Proxy devices use FA signaling in conjunction with Extreme Management Center Access Control in order to automate configuration of services.

The ISW only performs the functions of an FA Client.

Note
Extreme WLAN Access Points and Defender for IOT are FA Clients which initiate Fabric Attach VLAN/I-SID bindings themselves. If these are connected to an ISW, they will not be able to perform Fabric Attach VLAN/I-SID signaling because the ISW FA Client does not implement the proxy function of an FA Proxy.

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.

The FA service is enabled by default on FA Servers and FA Proxies. It is disabled by default on FA Standalone Proxy-only devices. Per-port settings are, by default, enabled on FA Proxies and disabled on FA Servers.

Port VLAN tagging switchport updates occur when an element is discovered. When an element is deleted or expires, all updated settings are cleared and roll back to their previous values.

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 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
- Message authentication status and keys for all ports
- Previously configured I-SID/VLAN assignments
- Extended logging support

FA I-SID-to-VLAN Assignment

Each I-SID/VLAN association that is configured on an ISW FA Client creates a Customer VLAN (C-VLAN) User-Network Interface (UNI), when the assignment becomes active following acceptance by an FA Server.

Note

FA Proxy/Client devices support only C-VLAN UNIs. They do not support switched UNIs.

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/Client 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.

If the FA Proxy or FA Client has access to an FA Server, these assignments are advertised for possible use by the FA Server, using FA signaling.

All I-SID/VLAN assignments defined on an FA Proxy, as well as those received from FA Clients when client proxy operation is enabled, start in the 'pending' state. The I-SID/VLAN assignment 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 can also reject proposed I-SID/VLAN assignments. In this case, the assignment state is updated to 'rejected'. Data describing the reason for the rejection may also be available.

FA Data Processing

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/Client 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.

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.

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 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.

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/Client 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.

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.

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.

You can configure the timeout value used for FA device or binding aging with the **`fa timeout`** command. The default value is 240 seconds.

FA Proxy/Client and FA Server Connection Maintenance

An FA Proxy/Client can interact with only 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.

Primary server failure is detected using a capabilities advertisement timeout. After 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/Client and 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/Client 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. After 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/Client 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.

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.

You can configure message authentication status and authentication keys on a per-port basis.

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 interface on which the FA Client is discovered is EAP/ NEAP enabled.

For FA Clients connected behind the ISW 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.

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.

FA Zero Touch

FA Zero Touch eases the configuration process on FA-capable devices by automating specific configuration tasks required for FA functionality.

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. 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.

The ISW does not propagate the management VLAN on any of its access ports.

The ISW will automatically perform DHCP on the management VLAN it receives from the FA Server/FA Proxy, unless a static IP is configured on the same VLAN.

Automated trusted FA Client connection

The ISW will automatically QoS trust traffic received on its uplinks to the FA Proxy/FA Server.

EAP and FA

With EAP and FA, FA-capable switches or stacks can forward traffic from EAP/NEAP clients over the SPB coud. The traffic for authenticated clients is mapped to I-SIDs received from the Extreme Management Center Access Control 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.

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 the ISW FA Client, the client port becomes a member of the VLAN from the I-SID/VLAN pair. The ISW FA Client sends to the FA Server/FA Proxy the binding received from the RADIUS server.

The ISW supports the following EAP/NEAP modes:

- Port-based 802.1X: EAPoL authentication with Single-Host-Single-Authentication behavior (SHSA). This mode works with Fabric Attach RADIUS attributes.
- Single 802.1X: EAPoL authentication with Multiple-Host-Single-Authentication behavior (MHSA). This mode works with Fabric Attach RADIUS attributes.
- Multi 802.1X: EAPoL authentication with Multiple-Host-Multiple-Authentication behavior (MHMA). This mode does NOT work with Fabric Attach RADIUS attributes.
- MAC-based: RADIUS MAC authentication (NEAP) with Single-Host-Single-Authentication behavior (SHSA). This mode works with Fabric Attach RADIUS attributes.

Note

The ISW can support MHMA in the MAC-based mode, but the last assigned RADIUS FA VLAN will apply to all authorized MACs on the port.

Note

Do not use NEAP (MAC-based mode) to connect Extreme WLAN Access Point FA Clients or to provision the ISW access port with the necessary VLANs. There are two reasons for this. First, the ISW can accept only one VLAN/I-SID binding per port. Second, a WLAN Access Point bridges wireless user MACs into the same ISW authorized port and would therefore require MHSA support, which the ISW provides only in EAP Single 802.1X mode.

VSAs

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

VSAs sent from RADIUS server to switch:

- Extreme-Fabric-Attach-VLAN-ISID

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

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

  This VSA contains the value of the PVID that should be set on the port with the authenticated client.

  Note

  In the ISW FA implementation, the Fabric-Attach-VLAN-PVID attribute must always be supplied. This attribute determines what VLAN is set as access VLAN on the ISW switch port.

VSAs sent from switch to RADIUS server:

- Extreme-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
- Extreme-Fabric-Attach-Client-Type

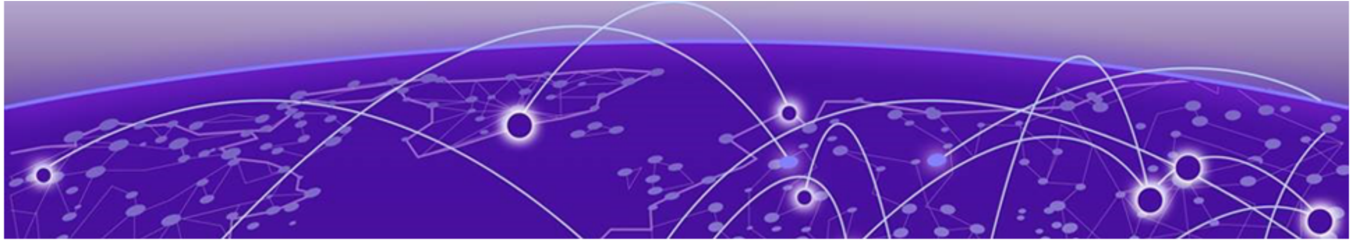
  This VSA can have the following values:
  - 1, FA Element Type Other
  - 2, FA Server
  - 3, FA Proxy
  - 4, FA Server No Authentication

    - 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]
- Fabric-Attach-Client-PSK

  This VSA can have the following values:

    - Not sent when PSK used unknown
    - 0, When Dual-key authentication is disabled
    - 10, When FA Client Failed FA TLV authentication using Default PSK
    - 11, When FA Client Passed FA TLV authentication using Default PSK
    - 100, When FA Client Failed FA TLV authentication using User Defined PSK
    - 101, When FA Client Passed FA TLV authentication using User Defined PSK
- Extreme-Fabric-Attach-Client-Id

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



CLI Commands

This chapter lists the CLI commands that pertain to Fabric Attach.

fa

Configures Fabric Attach.

Syntax

- **`default fa {assignment-timeout | authentication-key | client | discovery-timeout | message-authentication | port-enable}`**

Default

Enabled

Command Mode

Global Configuration

fa assignment-timeout

Configures Fabric Attach timeout for Fabric Attach VLAN:I-SID assignments.

Syntax

- **`fa assignment-timeout {45-480 seconds}`**

Default

240 seconds

Command Mode

Global Configuration

fa authentication-key

Configures Fabric Attach authentication key.

Syntax

- **`fa authentication-key {interface} {key}`**

Default

Extreme secret key

Command Mode

Global Configuration

fa client

Enables Fabric Attach client.

Syntax

- **`fa client`**

Default

None

Command Mode

Global Configuration

fa debuglevel

Enables Fabric Attach debugging.

Syntax

- **`fa debuglevel {1-5}`**

Default

None

Command Mode

Global Configuration

fa discovery-timeout

Configures Fabric Attach timeout for Fabric Attach neighbor elements.

Syntax

- **`fa discovery-timeout {45-480 seconds}`**

Default

240 seconds

Command Mode

Global Configuration

fa extended-logging

Enables Fabric Attach extended logging

Syntax

- **`fa extended-logging`**

Default

None

Command Mode

Global Configuration

fa message-authentication

Enables Fabric Attach message authentication.

Syntax

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

Command Parameters

key-mode <strict | standard>

Specifies the Authentication key usage setting.

Default

Enabled

Command Mode

Global Configuration

fa port-enable

Enables the Fabric Attach operation for each port.

Syntax

- **`fa port-enable <LINE>`**

Command Parameters

<LINE>

Enables the Fabric Attach operation for each port.

Default

Enabled

Command Mode

Global Configuration

show fa

Displays Fabric Attach specific settings.

Syntax

- **`show fa {agent | assignment <1-16777214> | elements [auth-status {auth-fail | auth-pass | not-auth}] [client-type <6-17>] [element-type {client | proxy | server}] [LINE] | i-sid <1-16777214> | interface | port-enable {disabled-auth | disabled-port | enabled-auth | enabled-port | LINE} | statistics [summary | <LINE>] }`**

Command Parameters

<LINE>

List of ports

agent

Displays the Fabric Attach agent status.

assignment <1-16777214>

Displays Fabric Attach configured UNIs.

auth-status {auth-fail | auth-pass | not-auth}

Displays only specified authorized status.

client-type

Displays only the specified client type.

disabled-auth

Displays only disabled authorized ports.

disabled-port

Displays only disabled ports.

elements

Displays discovered Fabric Attach elements.

element-type

Displays only the specified element type.

enabled-auth

Displays only enabled authorized ports.

enabled-port

Displays only enabled ports.

interface

Displays Fabric Attach port settings.

i-sid <1-16777214>

Displays the Fabric Attach configured user-to-network interface (UNIs).

port-enable <LINE>

Displays the Fabric Attach port settings.

statistics

Displays the FA summary and per-port statistics counters.

summary

Displays Fabric Attach summary statistics.

Default

None

Command Mode

User Executive