SSLi App v4.1 Release Notes

for A10 Thunder® Series and AX™ Series

1 May 2021

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks' products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:

https://www.a10networks.com/company/legal-notices/a10-virtual-patent-marking

TRADEMARKS

A10 Networks trademarks are listed at:

https://www.a10networks.com/company/legal-notices/a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

A10 NETWORKS INC. SOFTWARE LICENSE AND END USER AGREEMENT

Software for all A10 Networks products contains trade secrets of A10 Networks and its subsidiaries and Customer agrees to treat Software as confidential information.

Anyone who uses the Software does so only in compliance with the terms of the End User License Agreement (EULA), provided later in this document or available separately. Customer shall not:

1. Reverse engineer, reverse compile, reverse de-assemble, or otherwise translate the Software by any means.
2. Sub-license, rent, or lease the Software.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks location, which can be found by visiting www.a10networks.com.

Table of Contents

RELEASE NOTES FOR SSLI HARMONY APP V4.1

The SSLi Harmony Controller provides centralized SSLi service configuration and service level visibility to all managed SSLi deployments.

The SSLi Harmony App v4.1 provides an enriched coverage of multiple SSLi deployment scenarios and stand-alone features. The configuration section of this app is redesigned with intuitive interface for customers to perform SSLi deployments, to centrally manage the sites.

Overview

This chapter has the following sections:

What's New?

The SSLi Harmony App v4.1 focuses on enriched deployment and configuration support, that includes the following features:

- Migration to SSLi App v4.0 & 4.1
- More Traffic Flow Options
- SSLi Virtual Wire (vWire)
- Difference Tool for Deployment Configuration Changes

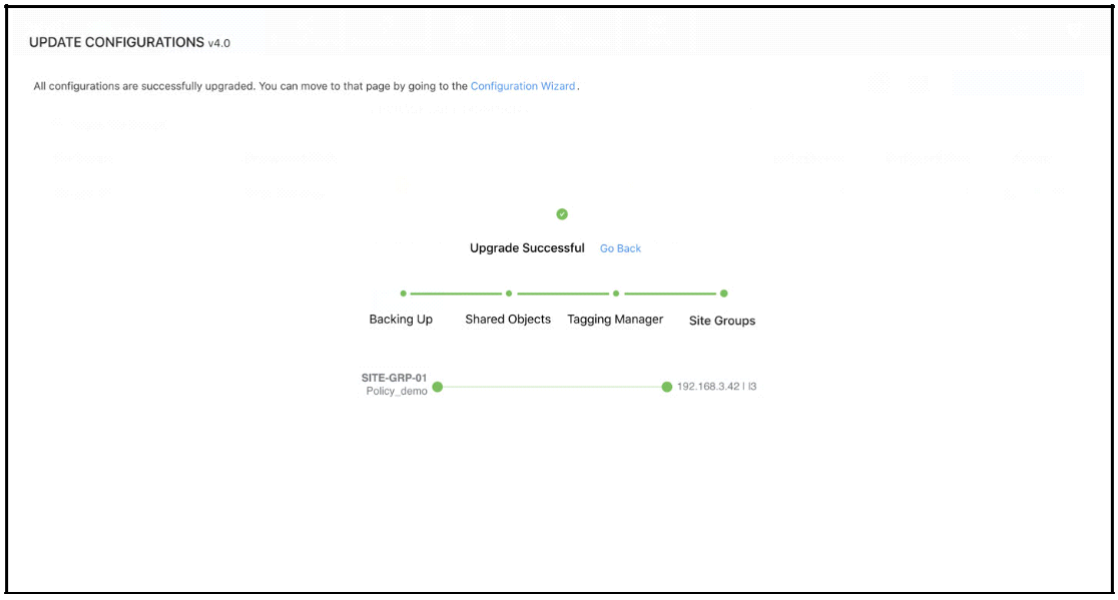
- Changes to SSLi Policy Configurations
- Additions to Shared Objects
- Enhancement to Existing Shared Objects
- Enhancement to Site Configurations
- Feature Enhancements

NOTE: For detailed information, refer *SSLi Harmony App User Guide*.

Migration to SSLi App v4.0 & 4.1

SSLi App provides users with an option to easily migrate their SSLi App v2.4 or v3.0 configurations to v4.0 & v4.1. User doesn't need to manually deploy the sites and site groups again; SSLi App recognizes and automatically migrates the SSLi configurations from previous versions.

FIGURE 1 : Migration to SSLi App v4.0 Complete



NOTE: SSLi App does not recommend direct migration from SSLi App v2.4 and v3.0 to v4.1. It is recommended to first migrate from SSLi App v2.4 or v3.0 to SSLi App v4.0 and then upgrade to SSLi App v4.1 using same steps.

More Traffic Flow Options

Previously, SSLi App v4.0 had full support for Outbound Traffic Flow. Multiple topology options were available for outbound traffic flow.

SSLi App v4.1 now provides support for the following new traffic flow options in addition to Outbound Traffic Flow:

- Inbound Traffic Flow – Inspects incoming traffic to internal networks
- Bidirectional Traffic Flow – Inspects outgoing as well as incoming traffic

User can configure any topology option for the above mentioned traffic flows through both guided and unguided mode.

FIGURE 2 : Guided Mode > Inbound Traffic Flow Topology

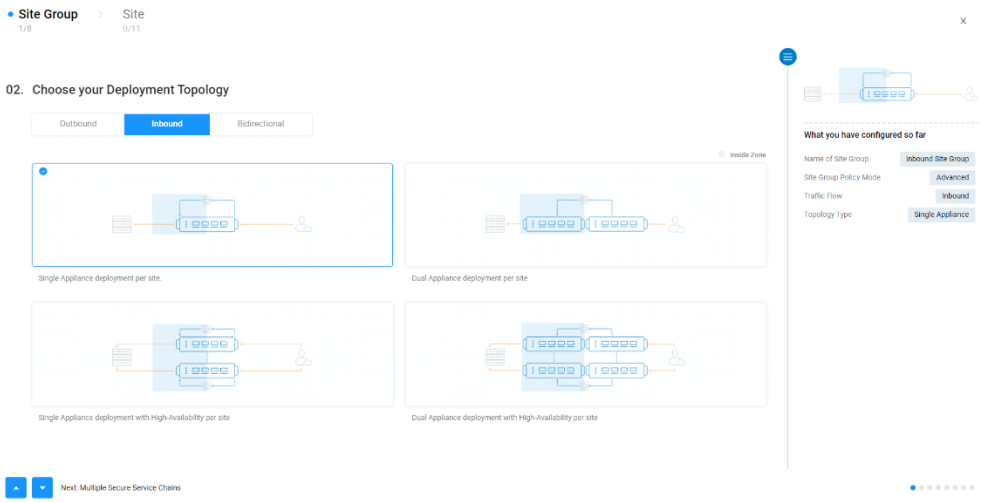
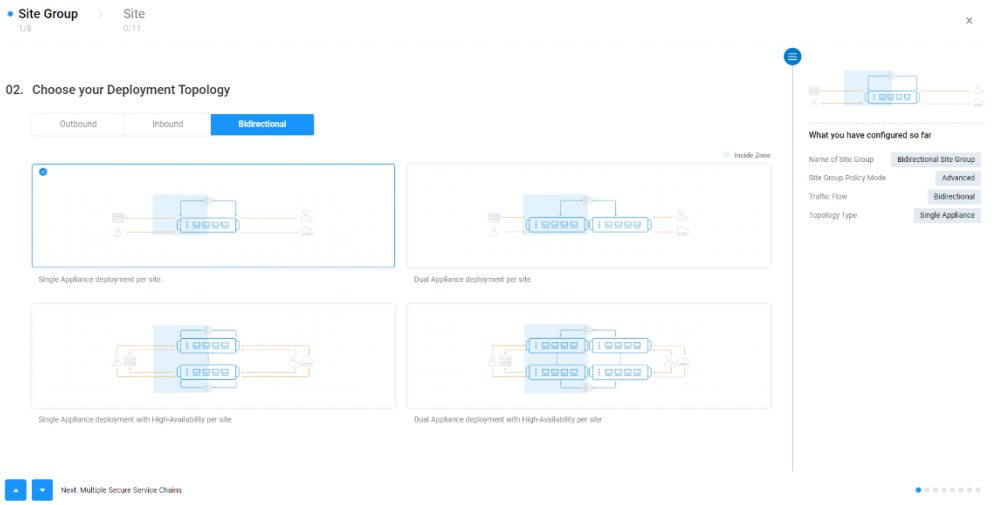


FIGURE 3 : Guided Mode > Bidirectional Traffic Flow Topology



SSLi Virtual Wire (vWire)

SSLi App v4.1 supports Virtual Wire (vWire) mode which is the recommend way to configure IPLess Topology. It considers the use case where existing implementation of IPLess can be used as it and on top of that inbound SSLi vWire or Outbound SSLi vWire can either co-exist or can be configured individually.

vWire mode is supported for all three traffic flows through guided and unguided mode.

FIGURE 4 : Guided Mode > Site Group > Select Virtual Wire Security Device

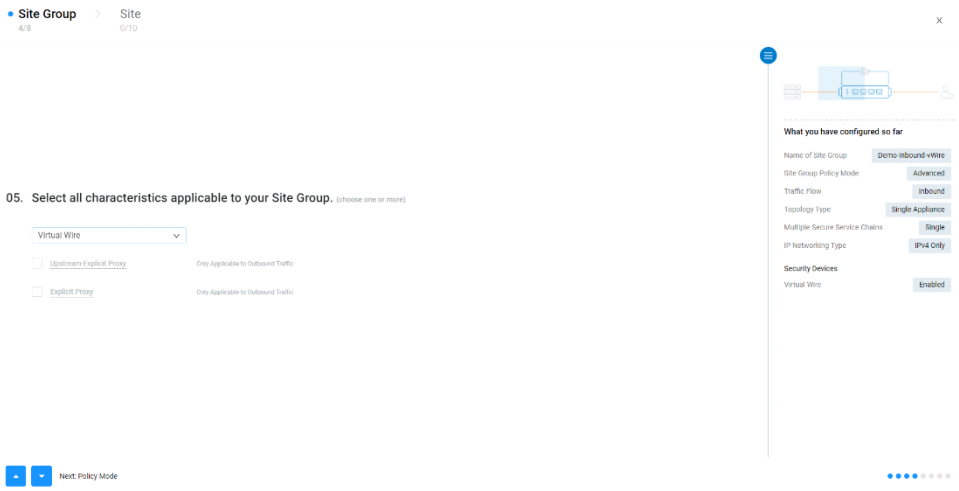
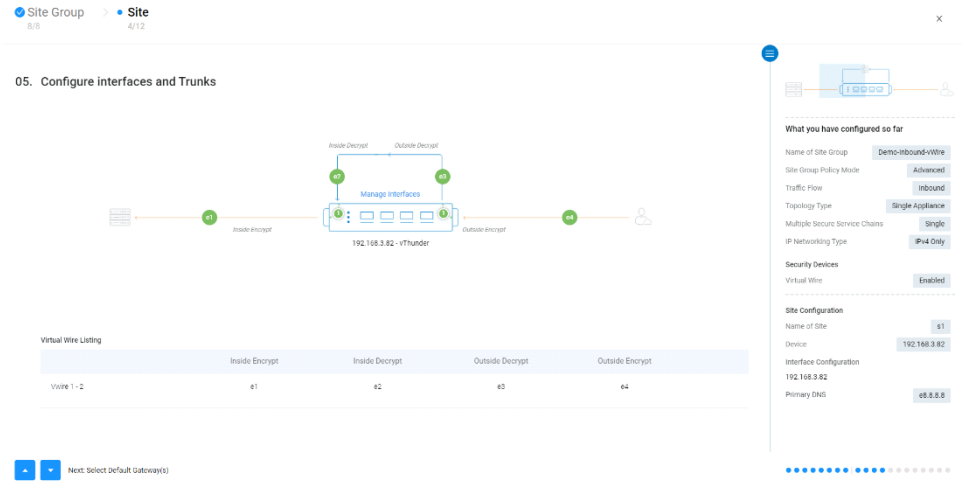


FIGURE 5 : Guided Mode > Site > Configure vWire Interfaces & Trunks

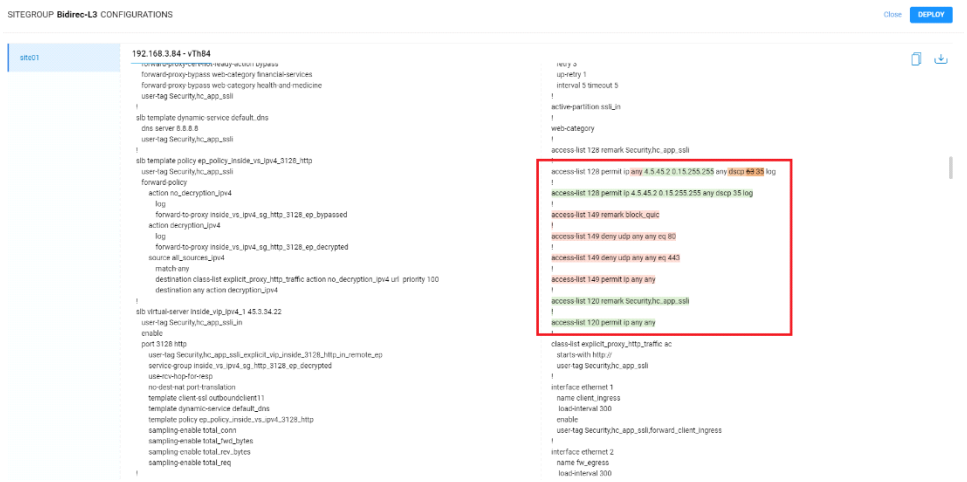


Difference Tool for Deployment Configuration Changes

The SSLi App supports Difference Tool for deployment configuration changes. Review Updates option provides side by side view of the complete configuration (to the left) and the highlighted updates (to the right). This view enables helps to know all the changes that are about to be deployed to the sites and the possible impact these changes can have. Review Updates option captures the following cases:

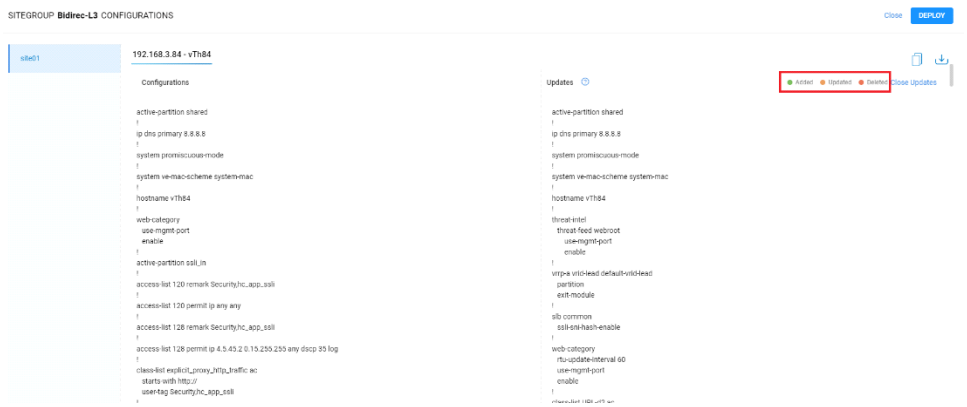
1. Highlighted Green – New configurations which will be added to the device during deployment
2. Highlighted Orange – Configurations which will be updated during deployment
3. Highlighted Red – Configurations which will be removed during deployment
4. Not Highlighted – Unchanged Configurations, configurations which will not be updated/ removed during deployment

FIGURE 6 : Review Updates



Color code indicators are added at the top of Review Updates window to guide the user what each color indicates.

FIGURE 7 : Review Update > Color Code indicators



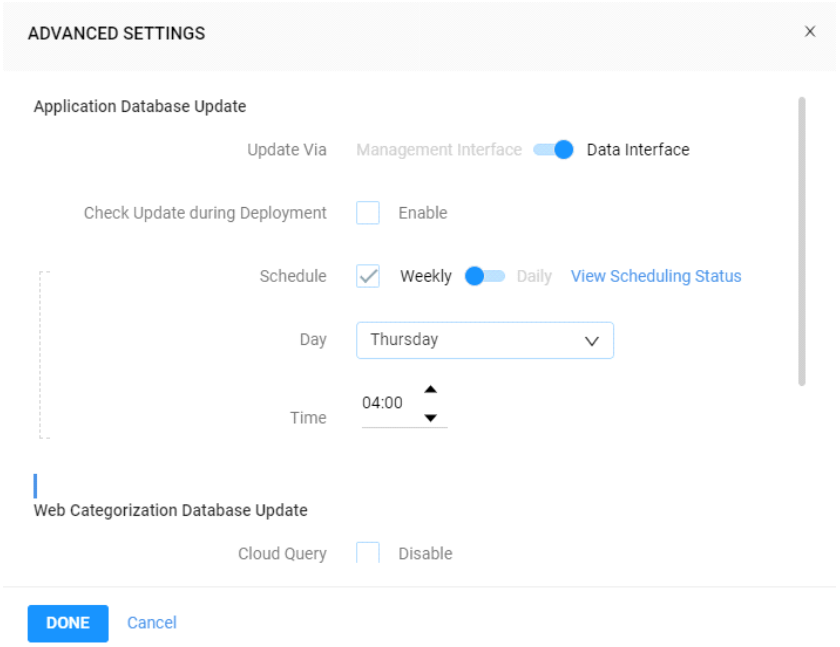
Changes to SSLi Policy Configurations

SSLi Policies provide centralized SSLi service and rules-based configuration management to all the sites of the site group. Following changes are introduced in SSLi Policy Configurations in SSLi App v4.1

Policy Add Ons

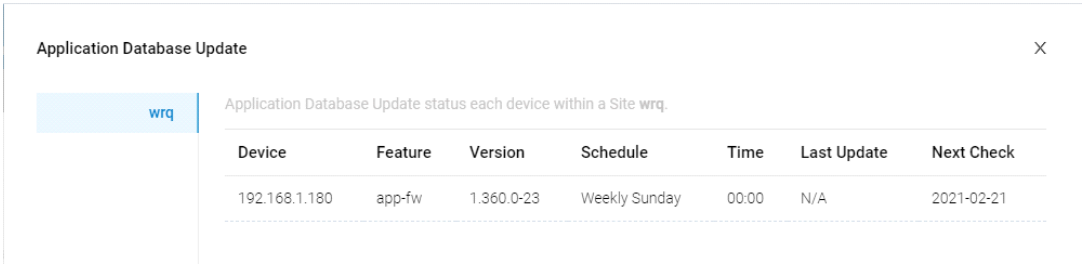
Schedule option is introduced in Add-Ons Advanced Settings in order to Schedule Automatic Application Database Update on Weekly or Daily basis. Day and time can be set for Weekly basis and only time can be configured for daily basis update schedule

FIGURE 8 : Schedule Update option



Schedule Status option is added to show to the summary of update schedule for each site in a site group.

FIGURE 9 : Scheduling Status



Policy Rules

Following changes are introduced in per rule policies:

- Custom servers along with variant health check status bound as a member In Custom Service Group
- Dynamic Service Templates are now referred as Data Interface DNS Tag
- For Inbound Policy Rules, Client SSL Inspection Profile is bound with Outside Rules while Server SSL Inspection Profile is bound with Inside Rules.

Following Options are not supported for Inbound Policy Rules:

- Bypass Traffic
- Tx/Rx Signaling using HTTP Header
- Virtual Ports Templates
- Source NAT (Auto/ Manual)
- Data Interface DNS Tags
- Inline Explicit Proxy
- Upstream Explicit Proxy

Services

Inbound Policy Rules support following services on the Outside Segment:

- ICAP
- User Access Control
- AFleX Script

Additions to Shared Objects

Shared objects are an abstraction of the configurations. The same configuration can be used and re-used across multiple policies. The following new Shared Objects are added to SSLi App v4.1.

- Server Option Template
- Service Group
- Template Policy
- Authorization Policy
- Health Monitor
- Client SSL Inspection Profile for Inbound traffic flow Type
- Server SSL Inspection Profile for Inbound Traffic Flow Type

Enhancement to Existing Shared Objects

A number of features and enhancements are added to the existing shared objects in SSLi App v4.1. The details are as follows:

- Client SSL Inspection Profile (Outbound)

- Forward Proxy Log Disable field
- Forward Proxy Cache Persistence field
- Require SNI Cert No Matched Action field
- Forward Proxy Cert Validity options field
- Forward Proxy Cert Ext options field
- SSL Inspection Option – Server Certificate Issuer
- SSL Inspection Option – Server Certificate SAN
- SSL Inspection Option – Server Certificate Subject
- Domain Bypass Class List
- Cert Validation Failure – Support for Block Option
- Separate Support for Cert-Fetch as TLS Version and Higher/Lower TLS Version
- TLS Version 1.3 support
- TLS 1.3 Ciphers support
- Info Text of fields – Pinned Certificate Site List, User ID, Group ID, Cert-Fetch via Source-NAT

- Server SSL Inspection Profile
  - Cert Revocation List (CRL) support
  - Certificate Authority (CA) Certificate support
  - Advanced Settings options
- ICAP separate modes i.e.
  - Request Mode
  - Response Mode
- Object Group – Support for Any option in Network Type Object Group
- Access List - Support for “Less Than (LT)” & “Greater Than (GT)” method for Source & Destination Ports of TCP/ UDP Protocols
- Firewall Rule Set – Info Text of Fields (Application Filtering, Src. Threat Intel, Dest. Threat Intel, Track Application)

Enhancement to Site Configurations

- License activation through GLM License Request with or without Entitlement Token
- Device ACOS Version detection and warning
- Support check for ACOS Version sub-series
- Support for Preempt Mode in VRID Advanced Settings

- Private Partition support for L2 Topologies
- HTTP port support for Web Category Proxy Server
- Update EHM Logs for Bypass O365 Script
- Characteristics - Info Text of Fields – Upstream Explicit Proxy, Explicit Proxy
- Additional Security Services – Info Text of Fields – ICAP capable Security Device, User Access Control
- Server Tab in Site Advanced Settings

Feature Enhancements

The following feature enhancements are available in SSLi App v4.1:

- Certificate & Key Import from Device
- Brownfield Changes for SSLI Inbound/ Bidirectional Traffic Flow Topologies
- Multiple Interface Selection for Specified Role
- Warning for VCS Settings during Brownfield Deployment
- IP Address Pop-up View at Site Level
- Brownfield – Shared Objects Names Conflict Options
- Servers Tab in Site Advanced Settings

Certificate & Key Import from Device

The SSLi App supports certificate import from any Harmony Controller registered devices. Application asks the user to select any harmony controller registered device from where to import the certificates and keys, followed by partition and certificate/ key selection. During Brownfield, Certificates are fetched automatically from the device.

Brownfield Changes for SSLI Inbound/ Bidirectional Traffic Flow Topologies

SSLI App supports brownfield import of configuration consisting of Inbound or Bidirectional topologies in addition to Outbound topologies. Default Gateways for inbound traffic are detected and selected by default during brownfield import, though user is provided with an option to deselect any if required. Servers deselected will then be considered custom servers.

For Bidirectional topologies, traffic flows of each virtual server are detected by default, however user can change as per their convenience.

Multiple Interface Selection for Specified Role

SSLi App supports selection of multiple interfaces for each specified role using smart illustration. Only interfaces and Trunk Groups can be selected through interface dropdowns. VEs are not exposed at this level.

Warning for VCS Settings during Brownfield Deployment

If VCS configuration is enabled on the device, then during Brownfield Deployment, a warning message appears at this stage and NEXT button is disabled since SSLi App does not support VCS Configuration currently.

IP Address Pop-up View at Site Level

SSLi App now supports pop-up view of IP Addresses in smart illustration. The IP Address field in the illustration only shows the first IP Address entered but if the user has added more VLANs for the particular role then IP Addresses for those VLANs can be seen in VLAN Table as well as IP Address pop-up view.

It enables user to edit or remove IP Addresses as well.

Brownfield – Shared Objects Names Conflict Options

Shared Objects Names Conflict present a list of objects if shared object with same name already exists in the application. SSLi App supports three different options if name conflict occurs for any shared object:

- Use Existing – Objects present is shared objects are used in deployment and those present on device are discarded.
- Override Existing – Objects present in shared objects are overridden with those present in device in deployment.
- Create New – Object with new name is created in shared object and deployed in deployment.

Servers Tab in Site Advanced Settings

Default Servers are created in the background when Default Gateways are set. SSLi App now supports Custom Servers where Server Options Template can be used and reused for multiple Custom Servers. To configure Custom Servers, user needs to bind Server Options Template in Server tab of Site Advanced Settings as well as in members table of Service Group bound in Policy Rules advanced settings.

Another way is to bind that Service Group in Action table of Template Policy bound in service of Vports.

Video Tutorials

To view an introductory video on how to install and use the SSLi Harmony Controller, refer this video:

Supported Platforms

ACOS HC SSLi App Compatibility

SSLi App Version	*Harmony Controller Version*	*ACOS Verison*	*Compatibility*	*Configuration*	*Analytics*
SSLi App v4.1	Harmony Controller 5.3	ACOS 5.2.1-P1	Limited support	Yes	Yes
	Harmony Controller 5.3	ACOS 4.1.4-GR1-P5	Limited support	Yes	Yes

Browser

Recommended Chrome Version: 89.0.4389.114 (Official Build) (64-bit)

Pre-requisites

Thunder and Harmony Controller clock must be in sync, and must be within the time difference of less than one minute.

NOTE: When deploying High Availability (HA) based topologies, Thunder HA pair devices must have VRRP-A configured before registration with Harmony Controller as a HA cluster. Some VRRP-A configuration settings are not permitted after VRRP-A is enabled.

Known Issues

The following issues have been reported for SSLi App v4.1:

Tracking ID	*ACOS Tracking ID*	*System Area*	*Description*	*Version Reported*
GUI-4213	NA	SSLi App	Data from ACOS 5.2.0 will not be displayed in the "Certificates in Cache" chart on the Analytics > Traffic Insights widget.	SSLi 4.0
GUI-4049	NA	SSLi App	While inline EP feature is enabled, even though EP is able to decrypt/bypass HTTPS traffic, the statistics for HTTPS traffic cannot be shown in Analytics because inline EP vport is recognized as SLB app service.	SSLi 4.0
HSA-4608	534859 536653	ACOS	If a client-ssl has server-name-list configured already, then axAPI Request get failed when executing POST call for client-ssl	SSLi 4.1
GUI-3882	520102	ACOS	Additional burst traffic/throughput is displayed on Apps when Harmony Controller is rebooting and initializing,	Harmony Controller 5.2.0

Known Limitations

The known limitations for SSLi App v4.1 are:

- HTTP2 is not supported.
- Recent SSLi features, related settings such as dynamic routing, VCS and advanced custom topologies, are not supported.
- Harmony Controller tenant awareness for configuration objects is not supported. User must log in as Provider Admin.
- For ACL Remark rule if its position or content has been updated then bindings will get through delete and create flow.
- Some of the configurations are not supported in Brownfield and will be configured using the application as follows:
  - Bypass O365: Only if configured using SSLi Harmony Controller App.
  - WIA SPN: Not recognized.

The following limitations are tracked for SSLi App v4.1:

Tracking ID	*ACOS Tracking ID*	*System Area*	*Description*	*Version Reported*
HSA-5562	NA	SSLi App	IP Pop-view in illustration at site level will always show the IPv4 Address upfront even if IPv6 is configured for Dual IP networking type site group.	SSLi App 4.1
HSA-5561	NA	SSLi App	During Brownfield Deployment, at shared objects names conflict stage, if user creates new shared object then all those shared objects where it is bound, needs to be updated as well.	SSLi App 4.1
HSA-5560	NA	SSLi App	Custom Template Policy is not supported in Simple Guided Site group flow.	SSLi App 4.1
HSA-5559	NA	SSLi App	Review Updates Section will show only those configurations which are supported/ recognized through application. Out of band configurations (Device configuration objects/ commands which are not supported through SSLi Application) will not be shown.	SSLi App 4.1
HSA-5558	NA	SSLi App	In order to configure Custom Server, Server Options template needs to be bound in the Service Group Member Table. Then this Service Group should either be bound in Template Policy or in Vports Advanced Settings.	SSLi App 4.1
HSA-5557	NA	SSLi App	Combination of traditional IPLess for Outbound & vWire based Inbound is not supported in either greenfield or brownfield.	SSLi App 4.1
HSA-5556	NA	SSLi App	Field “Server Name” in Server SSL Inspection (Inbound) can only be configured on thunder devices with ACOS 5.0.0 Series & higher.	SSLi App 4.1
HSA-5555	NA	SSLi App	Server Name Bypass options available in Client SSL Inspection (Inbound) profile can be configured only if one of the following options in same profile are enabled: • Server Name AutoMap • Server Name List • Server Name Regex List	SSLi App 4.1

Tracking ID	*ACOS Tracking ID*	*System Area*	*Description*	*Version Reported*
HSA-5554	NA	SSLi App	TLS_1.3 (Version 34) in Client & Server SSL Inspection profiles can only be configured at backend if “ssl-module software-tls13” is set (device reload/ reboot is required). TLS_1.3 is supported in ACOS 5.0.0 series and higher.	SSLi App 4.1
HSA-5436	534712	ACOS	In the inbound deployment mode, the outside HTTPS virtual port will not send the SSLi error logs.	ACOS 5.2.1-P1
HSA-5240	NA	SSLi App	The Analytics top indicator values such as control, data CPU, and memory may take time to load the data. Hence, it may display 0%. This is an intermittent issue.	SSLi App 4.1
HSA-5188	NA	SSLi App	In the inbound flow, the app service type for re-encryption virtual port inside SSLi will not be SSLi but SLB. This happens when the 'Forward Proxy Enable' option is not configured in the Server SSL inspection profile. Hence, Thunder will not send SSLi Connection or Error logs.	SSLi App 4.1
HSA-5182	NA	SSLi App	During Brownfield Import, Configurations of all shared objects are merged by name to make them unique. By doing this configs of Inside Partition objects are replaced with Outside Partition objects if their names are similar.	SSLi App 4.1
HSA-5176	NA	SSLi App	If client-ssl is imported from Brownfield Config Recognition, user will need to add passphrase value manually from the client-ssl shared object UI, in order to avoid deployment error *"msg": "Communication error with LB process"*	SSLi App 4.1

Tracking ID	*ACOS Tracking ID*	*System Area*	*Description*	*Version Reported*
HSA-5175	NA	SSLi App	If Server Name and Server Name Regex is configured from Server Name Table in shared objects (same name), then user cannot delete row in one deployment. Following steps should be taken to remove server name with regex. • Uncheck Regex checkbox and deploy. • Delete server name row and deploy.	SSLi App 4.1
HSA-5163	NA	SSLi App	User cannot configure Explicit proxy and SSLi on the same virtual port. For explicit proxy, only HTTP virtual port can be configured.	SSLi App 4.1
HSA-5159	NA	SSLi App	If the partition is created from Harmony Controller or SSLi Apps and removed from the backend, then the partition creation again from the HC or SSLi Apps may fail.	SSLi App 4.1
HSA-5093	NA	SSLi App	Any encrypted data will not be identified through brownfield import, instead “password” will be used in its place	SSLi App 4.1
HSA-5086	NA	SSLi App	Only those interfaces can be used as endpoints for default gateways that are configured in Virtual Wire. Virtual Wire feature is only supported in ACOS 5.2.0 series & higher.	SSLi App 4.1
HSA-5067	NA	SSLi App	The HTTP header template is applied to vport so that HTTP header “Frontend_SSL: Enabled” will be inserted regardless of whether traffic is decrypted by SSLi or not.	SSLi App 4.1
HSA-4970	NA	SSLi App	User will need to manually configure speed-forced from Device Terminal. SSLi App does not support this options and will not remove this command during deployment, if configured manually through terminal.	SSLi App 4.1

Tracking ID	*ACOS Tracking ID*	*System Area*	*Description*	*Version Reported*
HSA-4206	NA	SSLi App	For per Interface or per segment network deployments, SSLi App only recognises the interfaces and associated VLANs that are selected by the user in the "Interface" selection steps.	SSLi App 4.0
HSA-3969	NA	Harmony Controller	All devices must belong to the same provider, otherwise after using "Upgrade Feature" some devices will face authentication error problems as each provider maintains its own set of clusters or devices on Harmony Controller. We recommend using root provider with the application to avoid any unexpected issues.	Harmony Controller 5.2.0
HSA-3964	NA	SSLi App	'vrrp-a l3-inline-mode' command must be pre-configured before Harmony Controller registration. This configuration cannot be added from SSLi Application.	SSLi App 4.0
HSA-3871	NA	SSLi App	AAM LDAP domain name server configurations are not supported and does not recognize the domain name.	SSLi App 4.0
HSA-3865	NA	SSLi App	Router BGP configurations can not be configured from Harmony Controller or SSLi App.	SSLi App 4.0
HSA-3815	NA	SSLi App	OSPF settings are not supported by SSLi App.	SSLi App 4.0
HSA-3964 HSA-3762 HSA-3677	NA	SSLi App	L2 High Availability is not supported. It is recommended to use L2 redunancy, that requires an external switch with STP.	SSLi App 4.0
HSA-3538	NA	SSLi App	Any site cannot be deployed or deleted if it contains a device that has been deregistered.	SSLi App 4.0
HSA-3537	NA	SSLi App	Device reload required for "ip allow-promiscuous-vip" to be configured on interface ethernet.	SSLi App 4.0
HSA-3536	NA	Harmony Controller	Any configuration update made directly on ACOS Thunder device and not through the Harmony Controller App may not be recognized in some of the cases and can cause conflicts.	Harmony Controller 5.2.0

Tracking ID	*ACOS Tracking ID*	*System Area*	*Description*	*Version Reported*
HSA-3535	NA	SSLi App	The decryption (inside) partition must have access to the Microsoft endpoint so that the automatic update feature for Microsoft Office 365 bypass can function.	SSLi App 4.0
HSA-2400	NA	SSLi App	VLAN and interface numbers used in one partition cannot be exchange in another partition in the very next deployment, one has to first unbind and then bind again.	SSLi App 4.0

Partition flow Limitations

- Cluster partitions on Harmony Controller are created for active partitions on the device or previously defined and created through Harmony Controller.
- Any Inactive partitions will not be detected by Harmony Controller and the App before and after the registration of the device.

Configuration Limitations

- Any configuration made on the Thunder device directly and not through the Harmony Controller App will not be recognized and may be lost when the Harmony Controller App deploys the configuration.

Miscellaneous

Harmony SSLi App documents can only be managed through Root level access.

Fixed Issues

Some of the configurations are now supported in Brownfield deployment:

- URL Filtering: URL Configurations can be fetched through brownfield deployment now as template polcy is now supported.
- Service groups are now auto generated as well as custom made as per user requirements. A separate shared object Service Group is introduced in SSLi App v4.1.

- Pass phrase protected private key can now work in L3V partition.

The following fixed issues are tracked for SSLi App v4.1.

Tracking ID	*ACOS Tracking ID*	*System Area*	*Description*	*Version Reported*
GUI-4229	NA	SSLi App	The predefined Clusters are not reinstated correctly on Harmony Controller after it is restored.	Harmony Controller 5.2.0
GUI-4104	NA	SSLi App	Trigger Configuration backup does not function correctly on Harmony Controller.	Harmony Controller 5.2.0
HSA-3968	NA	SSLi App	Cluster partitions must be bound to tenant from which the Application will be used otherwise App services will not get updated for Analytics and Watchlist.	Harmony Controller 5.2.0
HSA-3580	NA	SSLi App	L2 or dual appliance configurations (Single partition) from greenfield can be pushed to shared as well as private partition.	SSLi App 4.0
HSA-1598	NA	SSLi App	The server certificate and server key can be applied to SLB template client-SSL from SSLi App GUI.	SSLi App 4.0
HSA-1238	NA	Harmony Controller	Tenant creation and mapping to device partition is now handled through SSLi App.	Harmony Controller 5.2.0

Support Information

The A10 Networks® technical and customer support team is available at your service on phone, email and web channels for your queries on SSLi App.

Technical and Customer Support

To know more about A10 Networks® Harmony Controller and SSLi App, refer the following:

- ***Contact:*** https://www.a10networks.com/company/contact-us
- ***Support:*** https://www.a10networks.com/support
- ***Call (International):*** 1-408-325-8676
- ***Call (Toll-Free USA & Canada):*** 1-888-TACS-A10