Cisco BroadWorks

Xtended Services Interface (Xsi)

Configuration Guide

Release 23.0

Document Version 2

Notification

The BroadSoft BroadWorks has been renamed to Cisco BroadWorks. Beginning in September 2018, you will begin to see the Cisco name and company logo, along with the new product name on the software, documentation, and packaging. During this transition process, you may see both BroadSoft and Cisco brands and former product names. These products meet the same high standards and quality that both BroadSoft and Cisco are known for in the industry.

Copyright Notice

Trademarks

Any product names mentioned in this document may be trademarks or registered trademarks of Cisco or their respective companies and are hereby acknowledged.

Document Revision History

Release	Version	Reason for Change	Date	Author
16.0	1	Created document.	May 29, 2009	Omar Paul
16.0	1	Edited and published document.	August 28, 2009	Andrea Fitzwilliam
16.0	2	Made command line interface (CLI) changes to reflect Release16.0 Xtended Services Platform.	October 12, 2009	Omar Paul
16.0	2	Edited and published document.	November 27, 2009	Andrea Fitzwilliam
17.0	1	Updated document for Release 17.0.	April 28, 2010	Michael Boyle
17.0	1	Edited and published document.	April 28, 2010	Patricia Renaud
17.0	2	Updated section *5.3.1.2 XSP_CLI/Applications/Xsi-Actions/BWIntegration* for EV 107900.	December 22, 2010	Goska Auerbach
17.0	2	Edited changes and published document.	April 11, 2011	Jessica Boyle
18.0	1	Updated document for Release 18.0.	November 7, 2011	Martin Perron
18.0	1	Edited changes and published document.	November 10, 2011	Patricia Renaud
19.0	1	Updated document for Release 19.0.	November 16, 2012	Stephan Goulet
19.0	1	Edited changes and published document.	November 22, 2012	Patricia Renaud
20.0	1	Updated document for Release 20.0.	October 31, 2013	Stephan Goulet
20.0	1	Edited changes and published document.	November 11, 2013	Joan Renaud
20.0	2	Added section *8 Xsi Interface Deployment Security Best Practices* for EV 209773.	December 6, 2013	Stephan Goulet
21.0	1	Updated document for Release 21.0.	December 11, 2013	Sébastien Martineau
21.0	1	Updated the legal notice and edited changes.	November 23, 2014	Joan Renaud
21.0	1	Rebranded and published document.	November 27, 2014	Joan Renaud
21.0	2	Added information about using URIBocking to block test pages in production for PR-48679.	October 21, 2015	Sébastien Martineau
21.0	2	Edited changes and published document.	February 5, 2016	Jessica Boyle
22.0	1	Updated document for Release 22.0.	September 7, 2016	Sébastien Martineau
22.0	1	Edited changes and published document.	November 28, 2016	Joan Renaud
23.0	1	Modified sections *5.3.1 Parameter Values*, *6.3.1 Parameter Values*, and *7.3.1 Parameter Values* to adjust parameters with current version.	September 18, 2018	Sébastien Martineau

Release	Version	Reason for Change	Date	Author
23.0	1	Rebranded document for Cisco. Edited changes and published document.	October 4, 2018	Joan Renaud
23.0	2	Rebranded product name for Cisco and published document.	March 14, 2019	Joan Renaud

Table of Contents

1 Summary of Changes

This section describes the changes to this document for each release and document version.

1.1 Changes for Release 23.0, Document Version 2

This version of the document contains the following change:

- Rebranded product name for Cisco.

1.2 Changes for Release 23.0, Document Version 1

This version of the document contains the following changes:

- Modified section *5.3.1 Parameter Values* to adjust parameters with current version.
- Modified section *6.3.1 Parameter Values* to adjust parameters with current version.
- Modified section *7.3.1 Parameter Values* to adjust parameters with current version.

1.3 Changes for Release 22.0, Document Version 1

This version of the document contains the following change:

- Modified section *6.1 Xsi-Events Application Server Configuration* to adjust the CLI command required to add an Open Client Interface (OCI) call control application.

1.4 Changes for Release 21.0, Document Version 2

This version of the document contains the following change:

- Modified section *8.3 Xtended Services Platform Application Layer Protection* to indicate that URL Blocking mechanism can be used to block access to the test pages in a production environment.

1.5 Changes for Release 21.0, Document Version 1

This version of the document contains the following changes:

- Modified section *6.3.1.3 XSP_CLI/Applications/Xsi-Events/BWIntegration* to indicate the ability to log in with the BroadWorks Mobility Directory Number (DN) for Mobility users.
- Modified section *5.3.1.2 XSP_CLI/Applications/Xsi-Actions/BWIntegration* to indicate the ability to log in with the BroadWorks Mobility DN for Mobility users.
- Fixed an error in the description of Xsi-Actions paging parameters in section *5.3.1.2 XSP_CLI/Applications/Xsi-Actions/BWIntegration*.

1.6 Changes for Release 20.0, Document Version 2

This version of the document contains the following change:

- Added section *8 Xsi Interface Deployment Security Best Practices* for EV 209773.

1.7 Changes for Release 20.0, Document Version 1

This version of the document contains the following changes:

- Updated section *5.3 Xsi-Actions Default Configuration and Modification* for EV 155575.

- Updated the deployment procedure for each application.

1.8 Changes for Release 19.0, Document Version 1

This version of the document contains the following changes:

- Added section *6.1.1 Using Different Application ID with Xsi-Events.*
- Updated the deployment procedure for each application.

1.9 Changes for Release 18.0, Document Version 1

This version of the document contains the following changes:

- Starting with Release 18.0, Xtended Services Interface web applications are pre-installed as managed web applications. The process of updating web applications for the purpose of introducing new functionality or applying software fixes has been impacted. The enhancements and software fixes to the web applications are now provided through the standard Cisco BroadWorks software delivery and patching processes.
- Starting with Release 18.0, the logging subsystem of the Xtended Services Interface web applications is harmonized with standard Cisco BroadWorks logging. The configuration of the logging subsystem of the web applications has been impacted.
- Starting with Release 18.0, the Xtended Services Interface web applications can be configured from the Element Management System. The configuration of the web applications is standardized, but can still be modified through the command line interface.

1.10 Changes for Release 17.0, Document Version 2

This version of the document contains the following change:

- Updated section *5.3.1.2 XSP_CLI/Applications/Xsi-Actions/BWIntegration* for EV 107900.

1.11 Changes for Release 17.0, Document Version 1

There were no changes to this document for Release 17.0.

1.12 Changes for Release 16.0, Document Version 2

For this version of the document, CLI changes were made to reflect Release 16.0 of the Xtended Services Platform (Xsp).

1.13 Changes for Release 16.0, Document Version 1

This document was created for Release 16.0.

2 Overview

This document describes the steps necessary to configure the Xtended Services Interface (Xsi) on Cisco BroadWorks.

The Xtended Services Interface (Xsi) is an HTTP-based, REST-ful application programming Interface (API) available over Cisco BroadWorks, targeted to end-user functionality such as subscriber call control, contact and call list directories, and end-user service configuration.

This document assumes that the reader is familiar with the Cisco BroadWorks Xtended Services Platform (Xsp) Server. For information on how to configure the Xtended Services Platform, see *Xtended Services Platform Configuration Guide.*

The Xtended Services Interface is natively deployed in a Cisco BroadWorks Xtended Services Platform (Xsp) Server. This configuration guide is written for Xtended Services Interface configuration on a Cisco BroadWorks Xtended Services Platform.

There are three web applications that make up the Xtended Services Interface. They are:

- **Xsi-Actions**: This web application contains all Xtended Services Interface commands that are request-initiated, that is, all commands that are in the form of a request from a client/application to Cisco BroadWorks followed by a response from Cisco BroadWorks to that client/application.
- **Xsi-Events**: This web application contains the Xtended Services Interface commands that are notification-based, that is, all commands that are in the form of notifications issued by Cisco BroadWorks to a client/application, based on a previous request/subscription for such notifications.
- **Xsi-MMTel**: This web application exposes an MMTel (Multimedia Telephony) "simserv" document over Cisco BroadWorks that is compliant with the *ETSI/TISPAN Multimedia Simulation Services* specification.

3 Get Started

All Xtended Services Interface web application configurations are done via the Cisco BroadWorks command line interface (CLI) on an Xtended Services Platform. Xtended Services Interface web applications once installed and deployed on an Xtended Services Platform, present an application-specific tree of contexts and commands in the Xtended Services Platform CLI.

Reader familiarity in operating a Cisco BroadWorks server CLI command tree is assumed.

The following high-level steps must be carried out to configure one/more of the Xtended Services Interface web applications in a Cisco BroadWorks server cluster:

1) Configure all Cisco BroadWorks Application Server clusters appropriately.
2) Deploy the managed pre-installed version for applicable Xtended Services Interface web applications.
3) Review default configuration values for applicable Xtended Services Interface web applications.
4) Modify web application configurations for your specific deployment/installation.
5) Restart all Xtended Services Platform servers for changes to take effect.

NOTE: It is assumed that there are already one/more active Xtended Services Platform servers in a Cisco BroadWorks cluster, correctly configured as per the *Xtended Services Platform Configuration Guide,* prior to executing any Xtended Services Interface web application configuration.

4 Application Server Configuration

4.1 Required Configuration

Cisco BroadWorks Application Server (AS) clusters must be configured to allow Xtended Services Platform servers to provide connectivity via the Open Client Interface-Provisioning (OCI-P) and Open Client Interface-Call Control (OCI-C) protocols.

> **NOTE**: OCI-C is a private protocol interface that is used between the Xtended Services Platform servers and the Application Server.

The Xsi-Actions, Xsi-Events, and Xsi-MMTel web applications make use of one or both of these protocols.

1) Add all Xtended Services Platform servers to the Application Server External Authentication Network Access List on every primary Application Server in a Cisco BroadWorks cluster.

```
AS_CLI/System/NetworkAccessLists/ExtAuth> add <ipAddress> [<description>]
```

For example:

```
AS_CLI/System/NetworkAccessLists/ExtAuth> add 192.168.13.186 xsp1
...Done
AS_CLI/System/NetworkAccessLists/ExtAuth> add 192.168.13.187 xsp2
...Done
```

2) Add all Xtended Services Platform servers to the Application Server OCI Network Access List for provisioning on every primary Application Server in a Cisco BroadWorks cluster.

```
AS_CLI/System/NetworkAccessLists/OCI/Provisioning> add <hostAddress>
[<description>]
```

For example:

```
AS_CLI/System/NetworkAccessLists/OCI/Provisioning> add 192.168.13.186
xsp1
...Done
AS_CLI/System/NetworkAccessLists/OCI/Provisioning> add 192.168.13.187
xsp2
...Done
```

3) Add all Xtended Services Platform servers to the Application Server OCI Network Access List for call control on every primary Application Server in a Cisco BroadWorks cluster.

```
AS_CLI/System/NetworkAccessLists/OCI/CallControl> add <hostAddress>
[<description>]
```

For example:

```
AS_CLI/System/NetworkAccessLists/OCI/CallControl> add 192.168.13.186 xsp1
...Done
AS_CLI/System/NetworkAccessLists/OCI/CallControl> add 192.168.13.187 xsp2
...Done
```

4.2 Optional Configuration

4.2.1 OCI-C Application-level ACL

OCI-C can be optionally configured to provide “per application” access control list (ACL) control from a host/server.

Each OCI-C message received by Cisco BroadWorks is tagged as belonging to a specific OCI-C application, via an application ID. Xsi-Actions is one such application, and so is Xsi-Events. If there are multiple OCI-C applications present on a single host/server but it is desired to allow only a subset of applications from that host to actually use the OCI-C, adding the application to the application ACL for that host allows such control.

Cisco recommends that you do not configure application-level ACL for OCI-C unless there is a specific security/deployment need where multiple OCI-C applications are accessing Cisco BroadWorks per host/server, and it is desired to turn on/off some such applications.

For example, in the event that it is required to allow Xsi-Actions, but not Xsi-Events as an application to use OCI-C, the appropriate application ID string can be added to this ACL on each primary Application Server in a Cisco BroadWorks cluster.

```
AS_CLI/System/NetworkAccessLists/OCI/CallControl/Application> add
<applicationId> <ipAddress> [<description>]
```

For example:

```
AS_CLI/System/NetworkAccessLists/OCI/CallControl/Application> add
com.broadsoft.xsi-actions 192.168.13.186 xsi-actions allowed from xsp1
...Done
AS_CLI/System/NetworkAccessLists/OCI/CallControl/Application> add
com.broadsoft.xsi-actions 192.168.13.187 xsi-actions allowed from xsp2
...Done
```

4.2.2 OCI-C Application IDs for Xtended Services Interface

- The OCI-C application ID for Xsi-Actions is set by default to “com.broadsoft.xsi-actions”.
- The OCI-C application ID for Xsi-Events is set by default to “com.broadsoft.xsi-events”.

Cisco recommends that you do not modify these values unless required. The application IDs are changed only in special cases as described in *6.1.1 Use Different Application ID with Xsi-Events*.

5 Xsi-Actions

This section describes how to configure the Xsi-Actions component of the Xtended Services Interface.

5.1 Xsi-Actions Application Server Configuration

There are no configuration requirements on an Application Server other than the steps previously listed in section *4 Application Server Configuration* for Xsi-Actions.

NOTE: The Xsi-Actions application ID of com.broadsoft.xsi-actions for OCI-C is provisioned by default on Cisco BroadWorks Application Server installation/upgrades. This entry can be viewed at the *AS_CLI/Interface/OCI/CallControl* level. Cisco recommends that this entry not be modified.

5.2 Version Check and Deploy

5.2.1 Introduction

Starting with Release 18.0, the Xsi-Actions web application is pre-installed on the Xtended Services Platform server as a managed web application. This means that the version of the web application is aligned with the software version of the Cisco BroadWorks server. Enhancements and software fixes are delivered through the standard Cisco BroadWorks software delivery and patching process for the Xtended Services Platform server. For more information, see the *Cisco BroadWorks Software Management Guide* [2].

Two main installation/upgrade scenarios are identified:

- Fresh install or upgrade from Release 18.0 and higher.
- Upgrade from a pre-Release 18.0 version.

5.2.1.1 Fresh Install or Upgrade from Release 18.0 and Higher

When upgrading the Xtended Services Platform server to Release 21.0, the managed Xsi-Actions web application is automatically upgraded and will retain its deployment state.

After the upgrade or fresh installation, if the Xsi-Actions web application is not already deployed, follow the instructions in the *Cisco BroadWorks Xtended Services Platform Configuration Guide* [1] to deploy it. Essentially:

- Activate Xsi-Actions with the proper context path.
- Appropriately configure any parameters on the new version.
- Deploy Xsi-Actions version.
- Test it as described in step 5 of section *5.2.1.2.1 Steps*.

5.2.1.2 Upgrade from a Pre-Release 18.0 version

Upon upgrading the Xtended Services Platform server to Release 21.0 from a pre-Release 18.0 version, the managed Xsi-Actions web application must be activated and deployed, in replacement of the previous version of the Xsi-Actions web application. This is a single time maintenance operation. Once the managed web application is deployed, the introduction of new functionality or fixes does not require the re-deployment of the web application. The new functionality or fixes are applied as soon as the server is upgraded or patched.

> **NOTE**: During the upgrade to Release 21.0, the configuration values of the current version of Xsi-Actions are copied to the managed version of Xsi-Actions, when applicable. The logging subsystem of the managed version of Xsi-Actions is different from the previous version and its configuration is always set to the default values on upgrade. The configuration of the logging subsystem should be validated upon activating the web application. The configuration values of the managed version of Xsi-Actions are always maintained through software upgrades and patches.

The following steps describe the process for upgrading from an unmanaged version of Xsi-Actions (in this example 8.6) to the managed version of Xsi-Actions (in this example 20.0_1.571).

5.2.1.2.1 Steps

1) Check the version of the Xsi-Actions web application currently deployed on all Xtended Services Platform servers by issuing the *get versions current* command at the Xtended Services Platform CLI level as shown in the following example:

```
XSP_CLI/Maintenance/ManagedObjects> get versions current
XSP version Rel_20.0_1.571

Built Sunday, October 27, 2013 12:15:14 PM EDT
- BASE revision 435006
- XSP revision 435018

Applications Info:
- WebContainer version 20.0_1.571
- Xsi-Events version 3.6 context path /com.broadsoft.xsi-events
- Xsi-MMTel version 2.1 context path /mmtel
- Xsi-Actions version 8.6 context path /com.broadsoft.xsi-actions

Patching Info:
  Active Patches: 0
```

2) Check the version of the managed Xsi-Actions web application installed on the Xtended Services Platform server by issuing the *get versions all* command at the Xtended Services Platform CLI level as shown in the following example.

```
XSP_CLI/Maintenance/ManagedObjects> get versions all
  Identity     Version  Install Date     Status
================================================
       XSP  20.0_1.571  Oct 29, 2013     Active

1 entry found.

* Applications:
                       Name     Version     Status
```

```
================================================
               BWCallCenter     20.0.18  Installed
                   BWOCTabs         3.2  Installed
                 BWPXSAastra         2.5  Installed
             BWPhoneXtension         2.5  Installed
              BWReceptionist     20.0.20  Installed
                 Bria-Webapp         3.3  Installed
               BroadworksDms  20.0_1.571     Active
       BusinessCommunicator         1.3  Installed
                   CommPilot  20.0_1.571     Active
           CommPilot-XS-TAS  20.0_1.571  Installed
  CustomMediaFilesRetrieval  20.0_1.571  Installed
       DeviceManagementTFTP  20.0_1.571     Active
                 FlashPolicy  20.0_1.571     Active
         ModeratorClientApp      20.0.4  Installed
                    OCIFiles  20.0_1.571     Active
                OCIOverSoap  20.0_1.571     Active
            OpenClientServer  20.0_1.571     Active
                    PXSAastra         1.0  Installed
               PhoneXtension         1.0  Installed
             PublicReporting  20.0_1.571  Installed
              RatingFunction  20.0_1.571  Installed
                  UC-Connect  20.0_1.571  Installed
               WebContainer  20.0_1.571     Active
                 Xsi-Actions         8.6     Active
                 Xsi-Actions  20.0_1.571  Installed
          Xsi-Actions-XS-TAS  20.0_1.571  Installed
                   Xsi-Events       3.6     Active
                  Xsi-Events  20.0_1.571  Installed
           Xsi-Events-XS-TAS  20.0_1.571  Installed
                    Xsi-MMTel         2.1     Active
                   Xsi-MMTel  20.0_1.571  Installed
            Xsi-MMTel-XS-TAS  20.0_1.571  Installed
                     Xsi-VTR  20.0_1.571  Installed

33 entries found.

* Third Party Software:
  Third Party      Version     Status
=====================================
         perl       5.14.1     active
         java  jdk1.7.0_21     active
     openldap      2.4.26d     active
      openssl       1.0.1e     active
       apache       2.2.24     active
       tomcat       6.0.36     active

6 entries found.

SWManager Version: 434408
```

3) Review the Xsi-Actions entries and note the active version number and the installed managed version. For example, from the outputs above, the active version of Xsi-Actions is 8.6 and the installed managed version of Xsi-Actions is 20.0_1.571.

4) Follow the instructions in the *Cisco BroadWorks Xtended Services Platform Configuration Guide* to undeploy the previous version of the Xsi-Actions and deploy the managed version of Xsi-Actions. Essentially:

   – Undeploy the previous version.

   – Deactivate the previous version.

   – Activate the new version at the same context path.

   – Appropriately configure any parameters on the new version.

- Deploy the new version.
- Uninstall the previous version after testing the new version.

> **NOTE**: Uninstalling the previous version is not mandatory, but it is recommended that you keep the list of applications manageable.

5) Assuming Xsi-Actions is deployed at the */com.broadsoft.xsi-actions* context path; there is an HTML test page for each Xsi-Actions command already present in the Xsi-Actions web application. These HTML pages can be used to test out Xsi-Actions commands. For example, https://xsp.xdp.broadsoft.com/com.broadsoft.xsi-actions/test is the Xsi-Actions root test page for the public Cisco/BroadSoft Xtended Developers Program Sandbox.

5.3 Xsi-Actions Default Configuration and Modification

The following Xsi-Actions parameters are available for configuration via an Xtended Services Platform CLI. Default values for each parameter are also listed.

All parameters are reachable via the *XSP_CLI/Applications/Xsi-Actions*> CLI level. As an example:

```
XSP_CLI/Applications/Xsi-Actions> ?
This level is used to configure the Xsi-Actions application.

Commands:
    0)    BWIntegration : go to level BWIntegration
    1)     FileTransfer : go to level FileTransfer
    2)  GeneralSettings : go to level GeneralSettings
    3)          Logging : go to level Logging
    4)  OverloadControl : go to level OverloadControl
    5)           Paging : go to level Paging
    6)      URIBlocking : go to level URIBlocking

  h (help),  e (exit),  q (quit),  r (read),  w (write),  t (tree),
  c (config),  cd (cd),  a (alias),  hi (history),  p (pause),  re
(repeat),  k (keyboardHelp)
```

5.3.1 Parameter Values

Each subsection lists the CLI level where parameters can be found. At each level, use the Cisco BroadWorks CLI get command to view the default value text string or any modified value that has been set. Use the CLI set command to change the value.

5.3.1.1 XSP_CLI/Applications/Xsi-Actions/GeneralSettings

Parameter	Default Value	Description
callControlApplicationName	com.broadsoft.xsi-actions	The OCI-C Application ID of the Xsi-Actions web application. Cisco recommends not changing this value. Values: String {1 to 255 characters}
enableCallCorrelationID	false	This parameter controls the presence of call correlation information in the application logs.
enableTestPages	true	This parameter controls whether the web test pages are accessible.

5.3.1.2 XSP_CLI/Applications/Xsi-Actions/BWIntegration

Parameter	Default Value	Description
allowDNAuthentication	true	Enable or disable the support of phone number/voice portal passcode-based authentication in addition to user ID/password-based authentication. Enable this if you want applications to issue Xtended Services Interface commands and have the option to authenticate using a user's phone number and voice portal passcode instead of the user ID and password, for example, via a VoiceXML-type application. If the user is a Mobile Private Branch Exchange (PBX) user, the mobile number can be used along with the voice portal passcode in order to log in. Values: Choice = {false, true}
allowSIPAuthentication	false	This parameter controls whether the SIP credentials are allowed for authentication. Values: Choice = {false, true}

5.3.1.1 XSP_CLI/Applications/Xsi-Actions/FileTransfer

Parameter	Default Value	Description
Username	nil	This parameter specifies the repository user name. Restart the system for modified values to take effect. Values: String {1 to 30 characters}
Password	nil	This parameter specifies the repository password. Restart the system for modified values to take effect. Values: String {1 to 40 characters}

5.3.1.1 XSP_CLI/Applications/Xsi-Actions/FileTransfer/Link

Parameter	Default Value	Description
connectionPoolSize	256	This parameter specifies the maximum number of concurrent connections. Restart the system for modified values to take effect. Values: Integer {1 to 2147483647}
connectionTimeout	5	This parameter specifies the maximum time period of inactivity allowed on a connection before it is declared failed. This time period includes the connection establishment and response reception. Restart the system for modified values to take effect. Values: Integer {1 to 300}

5.3.1.2 XSP_CLI/Applications/Xsi-Actions/Paging

Parameter	Default Value	Description
defaultPageSize	50	The number of results returned in a single page, applicable to all paged responses from Xsi-Actions except *EnhancedCallLogs*. Values: Integer {1 to 100}
enhancedCallLogsPageSize	50	The number of enhanced call log records returned in a single page. Call history, contact directory, and so on, responses are affected by this setting. Values: Integer {1 to 1000}
availableUserMaxLimit	100	Specifies the number of user/contact information returned in a single-paged response for requests made for the following features: AttendantConsole, BroadWorksReceptionistEnterprise, BroadWorksReceptionistOffice, BroadWorksReceptionistSmallBusiness, BusyLampField,PushToTalk Values: Integer {1 to 1000}

5.3.1.3 XSP_CLI/Applications/Xsi-Actions/Logging

Parameter	Default Value	Description
Enabled	true	Globally enable or disable logging for the application.
severity	info	Provides the default minimum log level severity for the application.
priority	5	Specifies the priority at which the logging thread will run (1 being the lowest priority and 5 the highest).
maxQueueSize	50000	Specifies the size of the logging queue.
showThreadName	true	Specifies whether the thread name is shown for individual log records.

5.3.1.1 XSP_CLI/Applications/Xsi-Actions/Logging/InputChannel

The application defines multiple logging input channels. Each input channel can be configured independently.

Parameter	Default Value	Description
enabled	Info	Enable/disable logging for a specific Input Channel.
Severity	5	Define the minimum log level severity for a specific Input Channel.

5.3.1.2 XSP_CLI/Applications/Xsi-Actions/Logging/OutputChannel

The application defines multiple logging output channels. Each output channel can be configured as follows.

Parameter	Default Value	Description
enabled	True	Enable/disable logging for a specific Output Channel.
directory	/var/broadworks/logs/xsp/	Define the minimum log level severity for a specific Input Channel.
filePrefix	XsiActionsLog	Define the prefix of the log files.
fileSizeInMB	30	Define the maximum size of a log file.
numberOfFiles	200	Define the maximum number of log files before the old log files are deleted.

5.3.1.3 XSP_CLI/Applications/Xsi-Actions/OverloadControls

Parameter	Default Value	Description
userDirectoryTransactionLimit	Not Set	Limits the rate of user transactions on */user/<userid>/directories* commands. Use this overload setting to control how often you want to allow each user account to issue directory-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
userServiceTransactionLimit	Not Set	Limits the rate of user transactions on */user/<userid>/services* commands. Use this overload setting to control how often you want to allow each user account to issue service-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}

Parameter	Default Value	Description
userCallsTransactionLimit	Not Set	Limits the rate of user transactions on */user/<userid>/calls* commands. Use this overload setting to control how often you want to allow each user account to issue call-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
globalDirectoryTransactionLimit	Not Set	Limits the rate of total transactions on */com.broadsoft.xsi-actions/v1.0/user/<userid>/directories* commands. Use this overload setting to control the total number of directory-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
globalServiceTransactionLimit	Not Set	Limits the rate of total transactions on */user/<userid>/services* commands. Use this overload setting to control the total number of services-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
globalCallsTransactionLimit	Not Set	Limits the rate of total transactions on */user/<userid>/calls* commands. Use this overload setting to control the total number of call-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
userProfileTransactionLimit	Not Set	Limits the rate of user transactions on */user/<userid>/profile* commands Use this overload setting to control how often you want to allow each user account to issue profile-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
globalProfileTransactionLimit	Not Set	Limits the rate of total transactions on */user/<userid>/profile* commands. Use this overload setting to control the total number of profile-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}

Parameter	Default Value	Description
routePointTransactionLimit	Not Set	This parameter limits the rate of user transactions on /routepoint/<routepointid> commands. Use this overload setting to control how often you want to allow each route point account to issue route point commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
globalRoutePointTransactionLimit	Not Set	This parameter limits the total rate of transactions on /routepoint/<routepointid> commands. Use this overload setting to control the total number of route-point-style commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
applicationtControllerTransactionLimit	Not Set	This parameter limits the rate of user transactions on system/services/RoutePoint/ApplicationController/<applicationControllerId> commands. Use this overload setting to control how often you want to allow each application controller commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
globalApplicationControllerTransactionLimit	Not Set	This parameter limits the total rate of transactions on system/services/RoutePoint/ApplicationController/<applicationControllerId> commands. Use this overload setting to control the total number of application controller commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65535}
transactionLimitPeriod	10	This parameter specifies the number of seconds for limiting the rate of transactions. Values: Integer {1 to 300}
userVoiceMessagingTransactionLimit	Not Set	This parameter specifies the maximum number of user transactions per second on /user/<userid>/voicemessaging commands. Use this overload setting to control how often each user account issues voice messaging-style commands per second. When the value is not set, this overload control is disabled. Values: Integer {1 to 65535}

Parameter	Default Value	Description
globalVoiceMessagingTransactionLimit	Not Set	This parameter specifies the total number of transactions per second for user/<userid>/voicemessaging commands. Use this overload setting to control the total number of voice messaging-style commands per second. When the value is not set, this overload control is disabled. Values: Integer {1 to 65535}

5.3.1.4 XSP_CLI/Applications/Xsi-Actions/URIBlocking

For the following sublevels, there are no parameters to be configured, but rather there are strings to be added into a table. Each string identifies a specific or wildcard URI filter to enable *Read, Write, All filtering* on any incoming command that matches the filter. By default, the string table is empty, and Xsi-Actions does not perform URI filtering.

- *XSP_CLI/Applications/Xsi-Actions/URIBlocking/BlockRead*

  Blocks the HTTP GET command on URIs added here with comma-separated string values.

- *XSP_CLI/Applications/Xsi-Actions/URIBlocking/BlockWrite*

  Blocks HTTP PUT, POST, DELETE commands on URIs added here with comma-separated string values.

- *XSP_CLI/Applications/Xsi-Actions/URIBlocking/BlockAll*

  Blocks all HTTP commands on URIs added here with comma-separated string values.

6 Xsi-Events

This section describes how to configure the Xsi-Events component of the Xtended Services Interface.

6.1 Xsi-Events Application Server Configuration

All Cisco BroadWorks Application Server clusters must be configured to allow Xsi-Events as an OCI-C application, identified by an OCI-C application ID for Xsi-Events. Section *4.2.2 OCI-C Application IDs for Xtended Services Interface* lists the OCI-C application ID for Xsi-Events, *com.broadsoft.xsi-events*.

Add the Xsi-Events OCI-C application ID to the primary Application Server in a Cisco BroadWorks cluster.

```
AS_CLI/Interface/OCI/CallControl> add <applicationId> <enableSystemWide>
<notificationTimeoutInSeconds> <maxEventChannelsPerSet>
<unresponsiveChannelSetGracePeriodSeconds> [<description>]
```

For example:

```
AS_CLI/Interface/OCI/CallControl> add com.broadsoft.xsi-events true 8 8 8
"BroadSoft Xsi-Events"
...Done
```

6.1.1 Use Different Application ID with Xsi-Events

Typically, the default application ID should not be changed. However, when HTTP contacts are used for event notifications, Xsi-events can be configured with different application ID in order to partition the event traffic across multiple Xtended Services Platforms. For a description of the various event notification mechanisms available, see the *Cisco BroadWorks Xtended Services Interface Interface Specification* [3].

If you change the application ID on the Application Server, it should also be changed in Xsi-Events. For more information, see section *6.3.1.2 XSP_CLI/Applications/Xsi-Events/GeneralSettings*.

6.2 Version Check and Deploy

6.2.1 Introduction

Starting with Release 18.0, the Xsi-Events web application is pre-installed on the Xtended Services Platform server as a managed web application. This means that the version of the web application is aligned with the software version of the Cisco BroadWorks server. Enhancements and software fixes are delivered through the standard Cisco BroadWorks software delivery and patching process for the Xtended Services Platform server. For more information, see the *Cisco BroadWorks Software Management Guide* [2].

Two main installation/upgrade scenarios are identified:

- Fresh install or upgrade from Release 18.0 and higher.
- Upgrade from a pre-Release 18.0 version.

6.2.1.1 Fresh Install or Upgrade from Release 18.0 and Higher

When upgrading the Xtended Services Platform server to Release 20.0, the managed Xsi-Events web application is automatically upgraded and will retain its deployment state.

After the upgrade or fresh installation, if Xsi-Events web application is not already deployed, follow the instructions in the *Cisco BroadWorks Xtended Services Platform Configuration Guide* to deploy it. Essentially:

- Activate Xsi-Events with the proper context path.
- Appropriately configure any parameters on the new version.
- Deploy Xsi-Events version.
- Test it as described in step 5 of section *6.2.1.2.1 Steps*.

6.2.1.2 Upgrade from a Pre-Release 18.0 Version

Upon upgrading the Xtended Services Platform server to Release 20.0 from a pre-release 18.0 version, the managed Xsi-Events web application must be activated and deployed, in replacement of the previous version of the Xsi-Events web application. This is a single time maintenance operation. Once the managed web application is deployed, the introduction of new functionality or fixes does not require the re-deployment of the web application. The new functionality or fixes are applied as soon as the server is upgraded or patched.

NOTE: During the upgrade to Release 20.0, the configuration values of the current version of Xsi-Events are copied to the managed version of Xsi-Events, when applicable. The logging subsystem of the managed version of Xsi-Events is different from the previous version and its configuration is always set to the default values on upgrade. The configuration of the logging subsystem should be validated upon activating the web application. The configuration values of the managed version of Xsi-Events are always maintained through software upgrades and patches.

The following steps describe the process for upgrading from an unmanaged version of Xsi-Events (in this example 3.6) to the managed version of Xsi-Events (in this example 20.0_1.571).

6.2.1.2.1 Steps

1) Check the version of the Xsi-Events web application currently deployed on all Xtended Services Platform servers by issuing the *get versions current* command at the Xtended Services Platform CLI level that follows:

```
XSP_CLI/Maintenance/ManagedObjects> get versions current
XSP version Rel_20.0_1.571

Built Sunday, October 27, 2013 12:15:14 PM EDT
- BASE revision 435006
- XSP revision 435018

Applications Info:
- WebContainer version 20.0_1.571
- Xsi-Events version 3.6 context path /com.broadsoft.xsi-events
- Xsi-MMTel version 2.1 context path /mmtel
- Xsi-Actions version 8.6 context path /com.broadsoft.xsi-actions
```

```
Patching Info:
  Active Patches: 0
```

2) Check the version of the managed Xsi-Events web application installed on the Xtended Services Platform server by issuing the *get versions all* command at the Xtended Services Platform CLI level in the following example.

```
XSP_CLI/Maintenance/ManagedObjects> get versions all
  Identity     Version  Install Date     Status
================================================
       XSP  20.0_1.571  Oct 29, 2013     Active

1 entry found.

* Applications:
                        Name     Version     Status
=======================================================
               BWCallCenter     20.0.18  Installed
                   BWOCTabs         3.2  Installed
                BWPXSAastra         2.5  Installed
            BWPhoneXtension         2.5  Installed
             BWReceptionist     20.0.20  Installed
                Bria-Webapp         3.3  Installed
              BroadworksDms  20.0_1.571     Active
       BusinessCommunicator         1.3  Installed
                   CommPilot  20.0_1.571     Active
           CommPilot-XS-TAS  20.0_1.571  Installed
  CustomMediaFilesRetrieval  20.0_1.571  Installed
       DeviceManagementTFTP  20.0_1.571     Active
                FlashPolicy  20.0_1.571     Active
         ModeratorClientApp      20.0.4  Installed
                   OCIFiles  20.0_1.571     Active
                OCIOverSoap  20.0_1.571     Active
           OpenClientServer  20.0_1.571     Active
                  PXSAastra         1.0  Installed
              PhoneXtension         1.0  Installed
             PublicReporting  20.0_1.571  Installed
              RatingFunction  20.0_1.571  Installed
                  UC-Connect  20.0_1.571  Installed
               WebContainer  20.0_1.571     Active
                Xsi-Actions         8.6     Active
                Xsi-Actions  20.0_1.571  Installed
          Xsi-Actions-XS-TAS  20.0_1.571  Installed
                  Xsi-Events       3.6      Active
                 Xsi-Events  20.0_1.571  Installed
           Xsi-Events-XS-TAS  20.0_1.571  Installed
                   Xsi-MMTel         2.1     Active
                  Xsi-MMTel  20.0_1.571  Installed
            Xsi-MMTel-XS-TAS  20.0_1.571  Installed
                    Xsi-VTR  20.0_1.571  Installed

33 entries found.

* Third Party Software:
  Third Party      Version     Status
=====================================
         perl       5.14.1     active
         java  jdk1.7.0_21     active
     openldap      2.4.26d     active
```

```
      openssl       1.0.1e     active
       apache       2.2.24     active
       tomcat       6.0.36     active

6 entries found.

SWManager Version: 434408
```

3) Review the Xsi-Events entries and note the active version number and the installed managed version. For example, from the output above, the active version of Xsi-Events is 3.6 and the installed managed version of Xsi-Events is 20.0_1.571.

4) Follow the instructions in the *Xtended Services Platform Configuration Guide* to undeploy the previous version of the Xsi-Events and deploy this managed version of Xsi-Events. Essentially:

   – Undeploy the previous version.

   – Deactivate the previous version.

   – Activate the new version at the same context path.

   – Appropriately configure any parameters on the new version.

   – Deploy the new version.

   – Uninstall the previous version after testing the new version.

NOTE: Uninstalling the previous version is not mandatory, but is recommended to keep the list of applications manageable.

5) Assuming Xsi-Events is deployed at the */com.broadsoft.xsi-events* context path, there is an HTML test page for each Xsi-Events command already present in the Xsi-Events web application. These HTML pages can be used to test out Xsi-Events commands. For example, https://xsp.xdp.broadsoft.com/com.broadsoft.xsi-events/test is the Xsi-Events root test page for the public Cisco/BroadSoft Xtended Developers Program Sandbox.

6.3 Xsi-Events Default Configuration and Modification

The following Xsi-Events parameters are available for configuration via an Xtended Services Platform CLI. Default values for each parameter are also listed.

All parameters are reachable via the *XSP_CLI/Applications/Xsi-Events*> CLI level.

Example:

```
XSP_CLI/Applications/Xsi-Events> ?
This level is used to configure the general settings of the XSI-Events
application.

Commands:
    0)    BWIntegration : go to level BWIntegration
    1)  EventCollection : go to level EventCollection
    2)  GeneralSettings : go to level GeneralSettings
    3)          Logging : go to level Logging
    4)  OverloadControl : go to level OverloadControl
    5)      URIBlocking : go to level URIBlocking
```

```
  h (help),  e (exit),  q (quit),  r (read),  w (write),  t (tree),
  c (config),  cd (cd),  a (alias),  hi (history),  p (pause),  re
(repeat),
  k (keyboardHelp)
```

6.3.1 Parameter Values

Each subsection lists the CLI level where parameters can be found. At each level, use the Cisco BroadWorks CLI get command to view the default value text string or any modified value that has been set. Use the CLI set command to change the value.

6.3.1.1 XSP_CLI/Applications/Xsi-Events/EventCollection

Parameter	Default Value	Description
maxSessions	20	This parameter specifies the maximum event collection session allowed.
sessionTimeoutInSeconds	15	This parameter specifies the duration that a long polling request must be received by the Web Server (in seconds); otherwise; the session is marked as stale.

6.3.1.2 XSP_CLI/Applications/Xsi-Events/GeneralSettings

Parameter	Default Value	Description
callControlApplicationName	com.broadsoft.xsi-events	The OCI-C Application ID of the Xsi-Events web application. Cisco recommends not changing this value. Values: String {1 to 255 characters}.
eventTimeout	30	This parameter specifies the timeout in second for a comet connection.
enableCallCorrelationID	false	This parameter controls the presence of call correlation information in the application logs.
enableTestPages	true	This parameter controls whether the web test pages are accessible.

6.3.1.3 XSP_CLI/Applications/Xsi-Events/BWIntegration

Parameter	Default Value	Description
allowDNAuthentication	false	Enable or disable phone number/voice portal passcode-based authentication in addition to user ID/password-based authentication. Enable this if you want applications to issue Xtended Services Interface commands and authenticate via a user's phone number/voice portal passcode as well as a user ID/password, for example, via a VoiceXML-type application. If the user is a Mobile PBX user, the mobile number can be used along with the voice portal passcode in order to log in. Values: Choice = {false, true}.

Parameter	Default Value	Description
useXSDiscoveryThread	true	Enable or disable Application Server discovery. The list of available Cisco BroadWorks Application Servers is checked periodically by an Xtended Services Platform to dynamically add/remove Application Servers available to an Xtended Services Platform.
xsDiscoveryPeriodInSeconds	60	The time interval in seconds after which the list of Cisco BroadWorks Application Servers is refreshed to determine added/removed servers. Values: Integer {1 to 3600}.
eventQueueSize	500	The size of the message queue containing events that are sent by an Application Server to Xsi-Events. When the queue size is exceeded, incoming events from the Application Server are discarded. Event notification messages sent by the Application Server are deposited on a queue while waiting for Xsi-Events to retrieve and process these notifications. Values: Integer {1 to 5000}.
eventHandlerThreadCount	4	The number of threads processing events deposited on the event queue. Each thread processes an event, converts it into an Xsi-Events notification payload, and attempts to call back the client/application that registered for this event. Cisco recommends not changing this value without consultation with Cisco Support. Values: Integer {1 to 50}.
allowSIPAuthentication	false	This parameter controls whether the SIP credentials are allowed for authentication. Values: Choice { false, true }

6.3.1.4 XSP_CLI/Applications/Xsi-Events/Logging

Parameter	Default Value	Description
Enabled	True	Globally enable or disable logging for the application.
severity	Info	Provides the default minimum log level severity for the application.
priority	5	Specifies the priority at which the logging thread will run (1 being the lowest priority and 5 the highest).
maxQueueSize	50000	Specifies the size of the logging queue.
showThreadName	true	Specifies whether the thread name is shown for individual log records.

6.3.1.5 XSP_CLI/Applications/Xsi-Events/Logging/InputChannel

The application defines multiple logging input channels. Each input channel can be configured independently.

Parameter	Default Value	Description
enabled	Info	Enable/disable logging for a specific Input Channel.
Severity	5	Define the minimum log level severity for a specific Input Channel.

6.3.1.1 XSP_CLI/Applications/Xsi-Events/Logging/OutputChannel

The application defines multiple logging output channels. Each output channel can be configured as follows.

Parameter	Default Value	Description
enabled	True	Enable/disable logging for a specific Output Channel.
directory	/var/broadworks/logs/xsp/	Define the minimum log level severity for a specific Input Channel.
filePrefix	XsiEventsLog	Define the prefix of the log files.
fileSizeInMB	30	Define the maximum size of a log file.
numberOfFiles	200	Define the maximum number of log files before the old log files are deleted.

6.3.1.2 XSP_CLI/Applications/Xsi-Events/OverloadControls

Parameter	Default Value	Description
subscriptionTransactionLimit	Not Set	Limits the rate of total subscriptions. Use this overload setting to control the total number of subscription commands within the configured transaction period. When not set, this overload control is disabled. Values: Integer {1 to 65536}
hostSubscriptionTransactionLimit	Not Set	Limits the rate of subscriptions per host application. Use this overload setting to control the number of subscription commands within the configured transaction period that a host application/client can send. When not set, this overload control is disabled. Values: Integer {1 to 65536}
transactionLimitPeriod	10	This parameter specifies the number of seconds for limiting the rate of transactions. Values: Integer {1 to 300}

6.3.1.3 XSP_CLI/Applications/Xsi-Events/URIBlocking

For the following sublevels there are no parameters to be configured but strings to be added into a table. Each string identifies a specific or wildcard URI filter to enable *Read, Write, All filtering* on any incoming command that matches the filter. By default, the string table is empty. Xsi-Events does not perform URI filtering.

- *XSP_CLI/Applications/Xsi-Events/ URIBlocking/BlockRead*

  Blocks the HTTP GET command on URIs added here with comma-separated string values.

- *XSP_CLI/Applications/Xsi-Events/URIBlocking/BlockWrite*

  Blocks HTTP PUT, POST, DELETE commands on URIs added here with comma-separated string values.

- *XSP_CLI/Applications/ Xsi-Events/URIBlocking/BlockAll*

  Blocks all HTTP commands on URIs added here with comma-separated string values.

7 Xsi-MMTel

7.1 Xsi-MMTel Application Server Configuration

There are no configuration requirements on an Application Server other than the steps previously listed in section *4 Application Server Configuration* for Xsi-MMTel.

7.2 Version Check and Deploy

7.2.1 Introduction

Starting Release 18.0, the Xsi-MMTel web application is pre-installed on the Xtended Services Platform server as a managed web application. This means that the version of the web application is aligned with the software version of the Cisco BroadWorks server. Enhancements and software fixes are delivered through the standard Cisco BroadWorks software delivery and patching process for the Xtended Services Platform server. For more information, see the *Cisco BroadWorks Software Management Guide* [2].

Two main installation/upgrade scenarios are identified:

- Fresh install or upgrade from Release 18.0 and higher.
- Upgrade from a pre-Release 18.0 version.

7.2.1.1 Fresh Install or Upgrade from Release 18.0 and Higher

When upgrading the Xtended Services Platform server to Release 20.0, the managed Xsi-MMTel web application is automatically upgraded and will retain its deployment state.

After the upgrade or fresh installation, if Xsi-MMTel is not already deployed, follow the instructions in the Xtended Services Platform Configuration Guide [1] to deploy it. Essentially:

- Activate Xsi-MMTel with the proper context path.
- Appropriately configure any parameters on the new version.
- Deploy Xsi-MMTel version.
- Test it as described in step 5 of section *7.2.1.2.1 Steps*.

7.2.1.2 Upgrade from Pre-Release 18.0 Version

Upon upgrading the Xtended Services Platform server to Release 20.0 from a pre-Release 18.0 version, the managed Xsi-MMTel web application must be activated and deployed, in replacement of the previous version of the Xsi-MMTel web application. This is a single time maintenance operation. Once the managed web application is deployed, the introduction of new functionality or fixes does not require the re-deployment of the web application. The new functionality or fixes are applied as soon as the server is upgraded or patched.

NOTE: The logging subsystem of the managed version of Xsi-MMTel is different from the previous version and its configuration is always set to the default values on upgrade. The configuration of the logging subsystem should be validated upon activating the web application. The configuration values of the managed version of Xsi-Events are always maintained through software upgrades and patches.

The following steps describe the process for upgrading from an unmanaged version of Xsi-MMTel (in this example 2.1) to the managed version of Xsi-MMTel (in this example 20.0_1.571).

7.2.1.2.1 Steps

1) Check the version of the Xsi-MMTel web application currently deployed on all Xtended Services Platform servers by issuing the *get versions current* command at the Xtended Services Platform CLI level that follows.

```
XSP_CLI/Maintenance/ManagedObjects> get versions current
XSP version Rel_20.0_1.571

Built Sunday, October 27, 2013 12:15:14 PM EDT
- BASE revision 435006
- XSP revision 435018

Applications Info:
- WebContainer version 20.0_1.571
- Xsi-Events version 3.6 context path /com.broadsoft.xsi-events
- Xsi-MMTel version 2.1 context path /mmtel
- Xsi-Actions version 8.6 context path /com.broadsoft.xsi-actions

Patching Info:
  Active Patches: 0
```

2) Check the version of the managed Xsi-MMTel web application installed on the Xtended Services Platform server by issuing the *get versions all* command at the Xtended Services Platform CLI level in the following example.

```
XSP_CLI/Maintenance/ManagedObjects> get versions all
  Identity     Version  Install Date     Status
================================================
       XSP  20.0_1.571  Oct 29, 2013     Active

1 entry found.

* Applications:
                        Name     Version     Status
=======================================================
               BWCallCenter     20.0.18  Installed
                   BWOCTabs         3.2  Installed
                BWPXSAastra         2.5  Installed
            BWPhoneXtension         2.5  Installed
             BWReceptionist     20.0.20  Installed
                Bria-Webapp         3.3  Installed
              BroadworksDms  20.0_1.571     Active
       BusinessCommunicator         1.3  Installed
                   CommPilot  20.0_1.571     Active
           CommPilot-XS-TAS   20.0_1.571  Installed
  CustomMediaFilesRetrieval   20.0_1.571  Installed
       DeviceManagementTFTP   20.0_1.571     Active
                 FlashPolicy  20.0_1.571     Active
         ModeratorClientApp       20.0.4  Installed
                    OCIFiles  20.0_1.571     Active
                OCIOverSoap   20.0_1.571     Active
            OpenClientServer  20.0_1.571     Active
                    PXSAastra         1.0  Installed
               PhoneXtension         1.0  Installed
             PublicReporting  20.0_1.571  Installed
              RatingFunction  20.0_1.571  Installed
```

```
                UC-Connect  20.0_1.571  Installed
             WebContainer  20.0_1.571     Active
              Xsi-Actions         8.6     Active
              Xsi-Actions  20.0_1.571  Installed
       Xsi-Actions-XS-TAS  20.0_1.571  Installed
                Xsi-Events       3.6     Active
               Xsi-Events  20.0_1.571  Installed
        Xsi-Events-XS-TAS  20.0_1.571  Installed
                Xsi-MMTel         2.1     Active
                Xsi-MMTel  20.0_1.571  Installed
         Xsi-MMTel-XS-TAS  20.0_1.571  Installed
                  Xsi-VTR  20.0_1.571  Installed

33 entries found.

* Third Party Software:
  Third Party      Version     Status
=======================================
         perl       5.14.1     active
         java  jdk1.7.0_21     active
     openldap      2.4.26d     active
      openssl       1.0.1e     active
       apache       2.2.24     active
       tomcat       6.0.36     active

6 entries found.

SWManager Version: 434408
```

3) Review the Xsi-MMTel entry and note the active version number and the installed managed version. For example, from the outputs above, the version of Xsi-MMTel is 2.1 and the installed managed version of Xsi-MMTel is 20.0_1.571.

4) Follow the instructions in the *Cisco BroadWorks Xtended Services Platform Configuration Guide* to undeploy the previous version of the Xsi-MMTel and deploy this managed version of Xsi-MMTel. Essentially:

   – Undeploy the previous version.

   – Deactivate the previous version.

   – Activate the new version at the same context path.

   – Appropriately configure any parameters on the new version.

   – Deploy the new version.

   – Uninstall the previous version after testing the new version.

NOTE: Uninstalling the previous version is not mandatory, but recommended to keep the list of applications manageable.

5) Assuming Xsi-MMTel is deployed at the */org.etsi.ngn.simservs* context path; there is an HTML test page for each Xsi-MMTel command already present in the Xsi-MMTel web application. These HTML pages can be used to test out Xsi-MMTel commands. For example, https://xsp.xdp.broadsoft.com/org.etsi.ngn.simservs/test is the Xsi-MMTel root test page for the public Cisco/BroadSoft Xtended Developers Program Sandbox.

7.3 Xsi-MMTel Default Configuration and Modification

The following Xsi-MMTel parameters are available for configuration via an Xtended Services Platform CLI. Default values for each parameter are also listed.

All parameters are reachable via the *XSP_CLI/Applications/Xsi-MMTel>* CLI level. For example:

```
XSP_CLI/Applications/Xsi-MMTel> ?
Configure the Xsi-MMTel web application.

Commands:
    0)           Logging : go to level Logging

  h (help),  e (exit),  q (quit),  r (read),  w (write),  t (tree),
  c (config),  cd (cd),  a (alias),  hi (history),  p (pause),  re
(repeat)
```

7.3.1 Parameter Values

Each subsection lists the CLI context where parameters can be found. At each context, use the Cisco BroadWorks CLI get command to view the default value text string or any modified value that has been set. Use the CLI set command to change the value.

7.3.1.1 XSP_CLI/Applications/Xsi-MMTel/Logging

Parameter	Default Value	Description
Enabled	True	Globally enable or disable logging for the application.
Severity	Info	Provides the default minimum log level severity for the application.
Priority	5	Specifies the priority at which the logging thread will run (1 being the lowest priority and 5 the highest).
maxQueueSize	50000	Specifies the size of the logging queue.
showThreadName	True	Specifies whether the thread name is shown for individual log records.

7.3.1.2 XSP_CLI/Applications/Xsi-MMTel/Logging/InputChannel

The application defines multiple logging input channels. Each input channel can be configured independently.

Parameter	Default Value	Description
enabled	Info	Enable or disable logging for a specific Input Channel.
Severity	5	Define the minimum log level severity for a specific Input Channel.

7.3.1.3 XSP_CLI/Applications/Xsi-MMTel/Logging/OutputChannel

The application defines multiple logging output channels. Each output channel can be configured as follows.

Parameter	Default Value	Description
enabled	true	Enable or disable logging for a specific Output Channel.
directory	/var/broadworks/logs/xsp/	Define the minimum log level severity for a specific input channel.
filePrefix	XsiMMTelLog	Define the prefix of the log files.
fileSizeInMB	30	Define the maximum size of a log file.
numberOfFiles	200	Define the maximum number of log files before the old log files are deleted.

7.3.1.4 XPS_CLI/Applications/Xsi-MMTel/GeneralSettings

Parameter	Default Value	Description
enableTestPages	true	This parameter controls whether the web test pages are accessible.

7.3.1.5 XSP_CLI/Applications/Xsi-MMTel/TrustedAuthenticationProxies

This CLI context allows adding, removing and listing IP addresses.

Name	Default Value	Description
trustedAuthenticationProxies	empty	This parameter, when set, allows for setting a list of IP addresses for trusted authentication proxies to contact the XSI-MMTel application on the Xtended Services Platform. A remote address from an HTTP request to XSI-MMTel that does not match this white list is not authenticated. If this occurs, then the whole authentication is rejected.

8 Xsi Interface Deployment Security Best Practices

This section outlines Cisco's recommended security best practices when deploying the Cisco BroadWorks Xsi interface in a public internet-facing (open) fashion.

8.1 Segregate Open Xsi to Dedicated Xtended Services Platform

When offering open Xsi interfaces to the outside world, the publicly facing Xsi-Action and/or Xsi-Events applications should not be overlaid on Xtended Services Platforms (Xsps) that support other publically facing Xtended Services Platform solutions like Cisco BroadWorks thin client applications or UC-One Communicator deployments. These open Xsi interfaces should be segregated to a dedicated Xtended Services Platform in order to limit the impact of an attack. For example, an attack against these open Xsi interfaces should not impact other publically-facing Xtended Services Platform applications.

8.2 Basic Firewall Protection

The Xtended Services Platform (Xsp) is not a firewall. Network level protection should be provided by an internet facing firewall or at the very least for Xtended Services Platform that are directly accessing the public internet, using IPTABLES locally. Denial-of-Service (DoS) attacks can happen at different layers. Attacks can range from lower layer TCP SYN floods to application layer "valid" HTTP floods. In general, firewalls can be configured to successfully manage lower layer attacks and higher application layer attacks such as "invalid" HTTP attacks (for example, invalid URI or malformed headers) or HTTP traffic storms from specific source addresses. "Valid" application layer floods are difficult to mitigate against since it can be a challenge for the firewall to distinguish between malicious and non-malicious "valid" requests. This is where Xtended Services Platform application layer protection can help.

8.3 Xtended Services Platform Application Layer Protection

Xtended Services Platform (Xsp) application layer protections are available to ensure that DoS attacks (malicious or otherwise) do not propagate back into the core impacting the function of other applications. The following outlines the different levels of Xtended Services Platform protection available:

- **Xtended Services Platform (Xsp) Resource Thresholds**: Not all DoS attacks involve large flows of traffic. Some attacks are crafted to slowly consume server resources (for example, Slowlaris). Although Apache tuning can mitigate some of the impact of these types of attacks, they cannot be eliminated. For all types of attacks, the key is identifying when a server's resources are being overly consumed so the carrier can investigate and institute the proper action (for example, blacklisting addresses at the firewall). The Xtended Services Platform is equipped with Apache and Tomcat resource threshold alarms (*bwHttpWorkersBusyExceeded*, *bwExecutorQueueUsageExceeded*, *bwExecutorThreadPoolBusyExceeded*) that by default will trigger when resource usage hits 90% and rearm when they return to less than 82%. These thresholds are not only useful for potential DoS identification, but as part of normal capacity scaling. For more information on these alarms, see the Cisco BroadWorks *Fault and Alarm Interface Specification* document for the applicable Cisco BroadWorks server.

- **URIBlocking**: The Xsi-actions and Xsi-events applications have the ability to limit the available URI that can be accessed. For example, the carrier can decide that specific commands or subset of commands (for example, all Xsi-Actions directories commands) should not be opened up on the Open Xsi interface. URIBlocking also allows the carrier to block requests related to specific users from accessing that Xtended Services Platform, allowing the creation of a blacklist. URIBlocking can also be used to block access to the test pages in production by adding the "/test/*" pattern to the BlockAll list.
- **Transaction Limit Thresholds**: The Xtended Services Platform is equipped with per-user transaction limits based on a sliding time window. If the user transaction limit is surpassed, a Simple Network Management Protocol (SNMP) alarm is generated (*bwWebContainerTransactionUserRateLimitExceeded*) and subsequent requests for that user receive a *503* response. The Xtended Services Platform is also equipped with server-level and per-application transaction limits. If the global server transaction limit or per-application limit is surpassed, an alarm is generated (*bwWebContainerTransactionGlobalRateLimitExceeded*) and subsequent requests receive a *503* response.

8.4 Segregate Network Servers used by Xtended Services Platform Dedicated to Open Xsi (Optional)

Xtended Services Platform (Xsp) Servers use the Network Server to identify valid Cisco BroadWorks users and provide serving Application Server information via the Location Lookup API. The Network Server Location Lookup API can scale to thousands of request per second and in general would not be overloaded by an external Xsi attack as the Xtended Services Platform (Xsp) application layer protection prevents the overload. For higher-level segregation of the core Cisco BroadWorks network from externally driven attacks, optionally, Xtended Services Platforms (Xsps) dedicated to open Xsi can use dedicated Network Server cluster members for location lookups. This ensures that any potential external attack does not impact the ability of other Xtended Services Platforms (Xsps) to perform the required location lookups.

8.5 Xsi Attack Vectors

Since external attacks (malicious or otherwise) on an open Xsi interface cannot be stopped, the main goal is to identify when these are occurring and ensure the Cisco BroadWorks core (for example, the Application Server and other applications running on other Xtended Services Platforms) is not impacted by the attack. In general, there are four different types of attacks that can reach an open Xsi-exposed Xtended Services Platform. The following outlines the different attacks and how Xtended Services Platform (Xsp) application layer protection can mitigate the situation.

1) **Web service HTTP attacks (traffic flood, invalid URI, malformed HTTP, slow resource consumption)**: In general, this type of attack is intended to deny web service by consuming resources. For invalid URI and malformed HTTP, the Apache front end deals with the problem by returning appropriate *4xx* responses. If the URI does contain a valid Xtended Services Platform (Xsp) application root context (for example, com.broadsoft.xsi-actions), then it is the application that determines if the rest of the URI is valid and if not, sends the appropriate 4xx response. Server-level and per-application transaction limits can be set to mitigate traffic floods but in general Apache and Tomcat are very good at self-regulating these types of attacks based on their maximum client and thread counts, which are automatically tuned by the Xtended Services Platform (Xsp) based on server resources. Trying to derive a proper server level and/or per-application transaction limit is not a trivial task and as such Cisco recommends letting the Apache and Tomcat configuration deal with these type of attacks. Carriers are informed via alarms when Apache or Tomcat resources are being exhausted via the resource threshold alarming capability and can then trigger an investigation and act accordingly. These type of attacks are restricted to the Xtended Services Platform and do not flow back into the core (for example, Network Server or Application Server).

2) **Enumeration attack for valid Cisco BroadWorks user Ids**: In this attack scenario, the attacker is hitting a valid URI and attempting to identify valid Cisco BroadWorks user Ids. The Xtended Services Platform sends a location lookup request containing the authentication user Id to the Network Server to validate if the user Id is known on the system and identify the serving Application Server cluster. For invalid user Ids, the Network Server returns an "Unknown User" response to the Xtended Services Platform, which then returns an HTTP 401 authentication challenge response to the requesting client. On the Network Server Location Lookup API "Unknown User" responses are tracked via the *bwUserLocationRequestUnknownUser* SNMP counter. A sudden increase in *bwUserLocationRequestUnknownUser* count can be indicative of a user Id Enumeration Attack. Once identified, defensive action can be applied against the attack at the firewall and/or Xtended Services Platform (for example, URIBlocking). Also, impact to the Cisco BroadWorks core from this type of attack can further be mitigated by optionally assigning a dedicated Network Server for location lookups. This type of attack is limited to the Xtended Services Platform and Network Server.

3) **Dictionary/Brute Force attack on valid user id**: In this attack scenario, the attacker is hitting a valid URI with a valid authentication user Id. The Xtended Services Platform sends a location lookup request containing the authentication user Id to the Network Server to validate if the user Id is known on the system and identify the serving Application Server cluster. The Xtended Services Platform forwards an OCI-P authentication request to the Application Server serving the user Id. The Application Server returns an OCI-P authentication failure response which results in the Xtended Services Platform returning a HTTP 401 authentication challenge response to the requesting client. This type of attack flows back into the Cisco BroadWorks core to the Application Server. On the Application Server, password hacking attempts against users can be mitigated by enabling account disabling after a configurable number of authentication failures. The Application Server tracks authentication failures via the *psOciStatsNbAuthorizationRequestFailures* SNMP counter. A sudden increases in *psOciStatsNbAuthorizationRequestFailures* count can be indicative of a Dictionary/Brute Force Attack. Once identified, defensive action can be applied against the attack at the firewall and/or the Xtended Services Platform (for example, URIBlocking).

4) **Traffic flood from authenticated User Id**: In this attack scenario, a valid logged in user is attempting to flood Cisco BroadWorks with a large amount of Xsi requests. These requests flow back into the core to the serving Application Server. This type of attack is mitigated through use of Xtended Services Platform-based per-user transaction thresholds. Xtended Services Platform-based per-user transaction thresholds count the number of transactions over a configurable rolling window. Once the user hits the transaction limit, all subsequent requests related to that user during the remaining time in the rolling window. Per-user transactions limit exceeds are reported via the *bwWebContainerTransactionUserRateLimitExceeded* SNMP trap. A sudden increase in *bwWebContainerTransactionUserRateLimitExceeded* traps can be indicative of a user-based traffic flood.

Acronyms and Abbreviations

This section lists the acronyms and abbreviations found in this document. The acronyms and abbreviations are listed in alphabetical order along with their meanings.

ACL	Access Control List
API	Application Programming Interface
AS	Application Server
BW	BroadWorks
CLI	Command Line Interface
DN	Directory Number
DoS	Denial-of-Service
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
OCI	Open Client Interface
PBX	Private Branch Exchange
SNMP	Simple Network Management Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
Xsi	Xtended Services Interface
Xsp	Xtended Services Platform

References

[1] Cisco Systems, Inc. 2019. *Cisco BroadWorks Xtended Services Platform Configuration Guide, Release 23.0.* Available from Cisco at xchange.broadsoft.com.

[2] Cisco Systems, Inc. 2019. *Cisco BroadWorks Software Management Guide, Release 23.0.* Available from Cisco at xchange.broadsoft.com.

[3] Cisco Systems, Inc. 2019. *Cisco BroadWorks Xtended Services Interface Interface Specification, Release 23.0*. Available from Cisco at xchange.broadsoft.com.