Cisco Finesse
Release 12.6(1) ES04

May 2022

Table of Contents

Introduction

This document provides important information and issues addressed in Cisco Finesse Release 12.6(1) ES04.

Important Notes

1. This Engineering Special can be installed only on 12.6(1) FCS and earlier versions of ES releases. See the **Valid Upgrade Paths** section for more details.
2. The Engineering Special does not involve Switch Version. It replaces the necessary files on the existing active version.
3. Installation of the Engineering Special stops critical services on the Finesse nodes and requires a reboot after installation is completed. Therefore, the ES must be installed during off peak hours maintenance window.
4. ES installation is supported only through the CLI. GUI installation is NOT supported.
5. ES can be uninstalled using the Rollback COP file. The instructions and details are provided in the Rollback Instructions section in this document.

Compatibility Report

Finesse 12.6(1) ES04 is compatible with Unified CCE 11.6, 12.0, and 12.5 releases.

12.6(1) ES04 Details

File Name	MD5 Checksum
finesse-cce.1261.ES04.10000.cop.sgn	0055b0fc134c00f60d2e4a11e4f3310e
finesse-cce.1261.ES.Rollback.cop.sgn	5e261ea653e2a6acbcf06d226f571ee8
12.6-ES04-reverse-proxy-config.zip	b88f45840ea214c70c57a4177bf1a0e6

Valid Upgrade Paths

Cisco Finesse 12.6(1) ES04 is delivered as a Cisco Options Package (COP) file. You can apply this COP file only to systems that have Cisco Finesse Release 12.6(1) FCS installed or any previous 12.6(1) ES.

Installing Finesse Release 12.6(1) ES04

You must perform the following procedure first on the primary Finesse node and then on the secondary node.
IMPORTANT: You must use the CLI to perform this upgrade. Do not use the Cisco Unified Operating System Administration page to perform this upgrade or the installation may not proceed.
Installing this ES or performing a rollback stops and restarts certain Finesse services. To avoid interruption, perform the installation or rollback during a maintenance window.
During ES installation and rollback, ensure that the SSH session is active throughout the installation process. Else, installation will not be successful.

NOTE: Customer is advised to take a DRS backup BEFORE and AFTER applying the ES04 COP.

1. Download **finesse-cce.1261.ES04.10000.cop.sgn** to an SFTP server that can be accessed by the Finesse system.
2. Use SSH to log in to your system with the platform administration account.
3. Access the CLI and run the following command:
   ```
   utils system upgrade initiate
   ```
4. Follow the instructions that appear on your screen.
   When prompted, provide the location and credentials for the remote file system (SFTP server).
   Note*: The COP file performs a check to ensure that Finesse Release 12.6(1) FCS or the previous released ES is installed. If this release is not found on your system, an error is displayed, and the installation does not proceed.*
5. Select **finesse-cce.1261.ES04.10000.cop.sgn**.
6. After installation is complete, restart the system using the command:
   ```
   utils system restart
   ```
7. To verify if the correct version of Finesse is running, access the CLI by using the Administrator credentials and enter the following command:
   ```
   show version active
   ```
   Ensure that **finesse-cce.1261.ES04.10000.cop.sgn** is listed. Else, contact Cisco Technical Support.
8. Check if the installation is successful by signing into Finesse (https://FQDN- of-Finesseserver:8445/desktop).
   Note: *Ensure to clear the browser cache.*

Rollback

If there is a problem with the installation, you can roll back to the base version as follows:
***Note**: The Finesse Rollback COP file removes the ES installed on the system and reverts your system to the base version of Finesse (in this case, Finesse Release 12.6(1) FCS).*

1. Download the file **finesse-cce.1261.ES.Rollback.cop.sgn** to an SFTP Server that can be accessed by the Finesse system.
2. Use SSH to log in to your Finesse system with the platform administration Account.
3. Access the CLI and run the following command:
   ```
   utils system upgrade initiate
   ```
4. Follow the on-screen instructions. When prompted, provide the location and credentials for the remote file system (SFTP server).
5. When presented with the list of available upgrade options, select **finesse-cce.1261.ES.Rollback.cop.sgn**.
6. After rollback is complete, restart the system using the command:
   ```
   utils system restart
   ```
7. To verify if the correct version of Finesse is running, access the CLI using the Administrator credentials and enter the following command:
   ```
   show version active
   ```

   Ensure that **finesse-cce.1261.ES.Rollback.cop.sgn** is listed. Else, contact Cisco Technical Support.

   ***Note:** Ensure to clear the browser cache.*

   If the TLS connections are configured to use ECDSA certificates, Rollback COP installation is not supported. Please change the certificate type to RSA using the command `set tls server cert_type rsa` and try again.

Feature Updates and Resolved Caveats in Release 12.6(1) ES04

New Features

None.

Updated Features

Nginx configuration is now added as Appendix to the Unified CCE Features guide, Packaged CCE Features guide, and HCS for CC Features guide.

Known Issues in Release 12.6(1) ES04

None.

Resolved Caveats in Release 12.6(1) ES04

CDET	Description	Severity
CSCwa25862	Using Russian or German with umlaut or unsupported language breaks the custom call variables layout	3
CSCwa33973	User is not able the select wrap up reason while ending a successful outgoing call to a PSTN number	3
CSCwa23488	Finesse Keypad does not show Alpha characters as dial pad	3
CSCwb62094	HTTP bosh connection getting disconnected intermittently	3
CSCwb48013	Webproxy fails to start when the proxy is not reachable even when mutual trust disabled	3
CSCwb65423	Reverse-proxy SDK throws exception when proxy mappings are deleted	3
CSCwb01969	Path parameter parsing is failing while creating http Workflow action	3
CSCwb02143	Gadget files hosted on finesse @ /3rdpartygadget/files/* are not accessible via reverse-proxy	3
CSCwb06546	Finesse Workflow Actions - HTTP request validation fix to fully resolve CSCvz85764	4
CSCwa60632	Finesse agent desktop shows last dialed number in the dialpad	4
CSCwa78986	Multiple Vulnerabilities in xstream	6
CSCwa78992	Multiple Vulnerabilities in xstream	6

Feature Updates and Resolved Caveats in Release 12.6(1) ES03

New Features

Configurable Reverse-Proxy Host Verification

You can enable and disable SSL certificate verification for connections that are established from reverse-proxy hosts to Cisco Web Proxy Service by using the **utils system reverse-proxy client-auth** CLI command. By default, the host authentication is disabled. For more information about reverse-proxy host authentication see the **Configure Reverse-Proxy Host Verification** section in Cisco Unified Contact Center Enterprise Features Guide.

Known Issues in Release 12.6(1) ES03

None.

Resolved Caveats in Release 12.6(1) ES03

CDET	Description	Severity
CSCwa46459	log4j zero day vulnerability exposed in webservice	1
CSCwa47021	desktop APIs are not CORS enabled	3
CSCvz08779	IP tables rules are not getting retained after build to build upgrade across solution	3
CSCvz08764	Delete of allowed-hosts is not working as expected	3
CSCwa26057	Multiple Certificates offered to agent during finesse desktop login	3
CSCwa24471	Finesse login page does not show SSO Agent FQDN name	3

CDET	Description	Severity
CSCwa24519	Webproxy service fails to restart if reverse proxy hostname is not resolvable from component	3
CSCwa23252	Web proxy mutual TLS auth is broken for CA signed certificate with depth more than 1	3
CSCwa15749	Maintenance mode alert banner inconsistent for agent login via vpnless proxy	4
CSCwa15981	Incorrect logging and lack of proper logging found on vpnless CLI command	4

Feature Updates and Resolved Caveats in Release 12.6(1) ES02

New Features

Locked Out Users

A new CLI **utils finesse locked_out_users list** has been added to view the list of locked out users.
For more information on the CLI, see the Finesse Administration guide.

Desktop Interface APIs

Three new APIs have been introduced which can be used for desktop development. The APIs are as follows:

- Desktop Configuration
- Languages List
- Verify Desktop and Third-Party URLs

For more information on the APIs, see the Cisco Finesse Desktop Interface API Guide on DevNet.

Authentication for Reverse-Proxy Connections

Finesse release 12.6(1) ES02 introduces authentication at the edge for the reverse-proxy. Authentication is supported for both SSO and Non-SSO deployments.
Authentication is enforced for all requests and protocols that are accepted at the proxy before they are forwarded to the respective component servers (Finesse, IdS, and IdP). The component servers also enforce the regular authentication locally. All authentications use the common Finesse login credentials to authenticate the requests. For more information on authentication, see the **Authentication** section Cisco Unified Contact Center Enterprise Features Guide.
For complete list of enhancements to the VPN-Less configuration, refer to the Nginx TechNote article.

Updated Features

VPN-less Access to Finesse Desktop (for Supervisors)

This feature, which was available for agents in 12.6 (1) ES01 has been extended to supervisors in 12.6(1) ES02. Supervisors can now access Finesse desktop without connecting to VPN.
Note: *There is no impact on any of the supervisor features.*

Reports

Historical and Realtime report gadgets are supported in supervisor desktop. The Stock reports can be viewed in the supervisor desktop. To configure custom reports as gadgets, you must run the CLI **`set cuic properties allow-proxy-custom-report`**. The report execution dataset size for Historical and Realtime reports can be configured using the CLI **`set cuic properties vpnless-response-size-ht`**. For more information, see the CUIC Administration guide.

SystemInfo API

SystemInfo API is now authenticated when accessed via VPN-Less proxy. For alternatives to be used in non-authenticated mode, refer to the Cisco Finesse Desktop Interface API Guide on DevNet.

API Authentication changes for VPN-Less Deployment

For changes related to the authentication model when running in VPN-Less deployment, refer to the Cisco Unified Contact Center Enterprise Features Guide. The authentication changes made for VPN-Less, primarily impacts third-party desktops and external API access. It does not impact the Finesse user authentication model and the functionality of the default desktop.

Security Enhancements

VPN-Less configuration update enhances the security posture for VPN-Less deployments. For details, refer to the Nginx TechNote article.

Special Instructions

After adding proxy hosts as trusted hosts through CLI on individual nodes, you must upload proxy server certificates to the respective components (Finesse, IdS, CUIC, and LiveData(12.6(1) ES01 and above)) Tomcat trust store. This is required for proxy authentication to work else traffic from proxy is rejected from the components. For more information, see the **Add Proxy IP by Using CLI** section in the Cisco Unified Contact Center Enterprise Features Guide.

***Note:** If you are upgrading from 12.6(1) ES01, you must copy and upload proxy server certificates to the respective components Tomcat trust store.*

Known Issues in Release 12.6(1) ES02

CDET	Issue	Workaround
CSCwa15981	Incorrect logging and lack of proper logging found on vpnless CLI command	This is specific to VPN-Less deployment
CSCwa15749	Maintenance mode alert banner inconsistent for agent login via vpnless proxy	This is specific to VPN-Less deployment
CSCwa23252	Web proxy mutual TLS auth is broken for CA signed certificate with depth more than 1 for CA certs chain	This issue exists in 126(1) ES02 only where mutual authentication between proxy and the components (Finesse, LD, IdS, IdP, and CUIC) was introduced. below are the possible workarounds for 1261 ES02: 1. Either use a CA signed certificate for reverse proxy of depth 1 i.e no intermediary CAs in the cert chain and server certificate be direct signed by root CA 2. Use a separate self-signed certificate for proxy-component mutual auth. This requires changing nginx ssl configuration to use different certificates for client ssl config and ssl config of the components.
CSCwa24519	Webproxy service fails to restart if reverse proxy hostname is not resolvable from component	Make sure allowed hosts added as part of reverse proxy CLI are resolvable from all the components (Finesse, LD, IdS, IdP, and CUIC). Hostname should not be resolved to more than one IP address from DNS.
CSCwa24471	Finesse login page does not show SSO Agent FQDN name	None
CSCwa26057	Multiple Certificates offered to agent during finesse desktop login	None

Resolved Caveats in Release 12.6(1) ES02

CDET	Description	Severity
CSCvz47125	UserAuthMode API expects authentication	2
CSCwa03436	Finesse 12.6 service crash where protocolReferenceGUID has some non-printable characters.	2
CSCvy95309	Webproxy Error.log needs log rotation	3
CSCvy78841	Finesse 12.6 - updateCuicGadgetUrl CLI command fails on Publisher	3
CSCvz44053	Finesse Desktop get stuck when TPG refreshes	3
CSCvz85764	Getting error when try to create a new Work flow in finesse 12.6	3
CSCvy71479	Finesse Desktop maxRows Attribute not working with the QueueStatistics Gadget for Agents	3
CSCvz70003	Queue Statistics gadget "Max time" not refreshing when using queuestatistics.js in 12.6	3
CSCvz41872	Solutions with Two ECE Gadgets May Encounter Error If One URL Is Invalid	3
CSCwa15747	Proxy failover for agent in SSO mode get redirected to other proxy with blank page	3
CSCvz08764	Delete of allowed-hosts is not working as expected	3
CSCvz68617	Voicea note for chat transcript gadget incorrect	4
CSCvy97673	Unable to add FQDN for CORS Allowed Origin if Starting with Numerical value	4
CSCwa08066	Reverse Proxy Url doesnt resolve the mapping if there is a space in the proxy map.tx	4
CSCvz26463	While updating frame-ancestors or CORS, extra message should be added to notify clearing RP cache	4
CSCvz70372	Finesse 12.6 False warning for ip change in cmplatform	5
CSCvy31448	Finesse 12.0+ Team performance Gadget always presents Scroll bar	5
CSCvy67682	Phonebook entry size should be increased in agent desktop	6
CSCvz26351	new gadgets.Prefs().getString("externalServerHostPort") fails to get proxymap value	6

Feature Updates and Resolved Caveats in Release 12.6(1) ES01

New Features

VPN-less Access to Finesse Desktop (for Agents)

This feature provides the flexibility for agents to access the Finesse desktop from anywhere through the Internet. To enable this feature, a reverse-proxy pair must be deployed in the DMZ. This feature is supported in Unified CCE, Packaged CCE, HCS for CC, and Webex CCE.
Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents can use Cisco Jabber over MRA or the Mobile Agent capability of Contact Center Enterprise with a PSTN or mobile endpoint. For more information on this feature, see the Cisco Unified Contact Center Enterprise

Features Guide Release 12.6(1) and Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1).

Note: *To use VPN-less access to Finesse desktop feature, you must upgrade Finesse, IdS, and CUIC to Release 12.6(1) ES01. If you are using Unified CCE 12.6, you must update Live Data also to 12.6(1) ES01. In 12.6(1) ES01, VPN-less access to the Finesse Desktop is supported only for Agents. Supervisors must connect to VPN to access the Finesse desktop.*

For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions refer to the Nginx TechNote article. Any reverse-proxy supporting the required criteria (as mentioned in the ***Reverse-Proxy Selection Criteria*** *section of Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)) can be used in place of Nginx for supporting this feature.*

Certificate Configuration

Finesse has introduced CLI commands to configure **Elliptic Curve Digital Signature Algorithm (ECDSA)** as another cryptography algorithm. You can now configure RSA or ECDSA cipher for TLS connections. For more information about the commands, see the **Certificate Configuration** section in the Cisco Finesse Administration Guide.

AI Services Configuration and Support for Unified CCE 12.5

Finesse now supports AI services for Unified CCE 12.5. You can use the newly introduced CLI commands to enable, disable, and view the service status of AI gadgets, such as, Agent Answers, Call Transcript, and Recording. The commands must be run in all the Finesse clusters. For more information about the commands, see the **AI Services Configuration** section in the Cisco Finesse Administration Guide.

Updated Features

Accessing Team API

A new configuration property **enableTeamAPIAccessForAllusers** is added for enabling the Team API access for all agents and supervisors. When you enable this property, all agents and supervisors will be able to access information of all the teams without any restriction.

If this property is disabled, only the administrator and supervisors can access the Team API. Supervisors can access the information of the teams that they are assigned to, and Administrators can access all the teams. By default, this property is disabled. For more information about this property, see the **Service Properties** section in the Cisco Finesse Administration Guide.

Maintenance Mode

A new CLI has been introduced to control the agent state when migrating to the secondary Finesse during Maintenance Mode. The CLI is intended for deployments using Unified CCE Agent PG older than 12.6. For more information, refer to the **utils finesse set_property desktop agentStateAfterMigration** command in the Cisco Finesse Administration Guide.

Special Instructions

Clear Reverse-Proxy Cache

While updating frame-ancestors or CORS, you must manually clear the reverse-proxy cache along with the required service restarts in Finesse. The instructions to clear reverse-proxy cache is available in the Nginx TechNote article.

Add Self-Signed Certificate

If you are using Chrome browser and self-signed certificates to access the Platform web applications, such as **Cisco Unified OS Administration**, **Cisco Unified Serviceability**, **Disaster Recovery System** and **Cisco Unified Intelligence Center Administration**, add the **RSA** or the **ECDSA** certificates to the Client OS trust store.

Known Issues in Release 12.6(1) ES01

CDET	Issue	Workaround
CSCvz08764	Deleting allowed hosts through the command **utils system reverse-proxy allowed-host delete** will delete the existing list of allowed hosts.	Add the deleted list back using the add command. **utils system reverse-proxy allowed-host add host1,host2**

CSCvz26351	As described in the Unified CCE Features guide for VPN-Less Access to Finesse Desktop, sending hostname and port information to gadgets through the new **gadgets.Prefs()** does not work.
	The following is an example of the API which does not give a response
	`var hostPort = new gadgets.Prefs().getString(“externalServerHostAndPort_chat”);`
	Instead, the same can be achieved via:
	`var hostPort = “__UP_externalServerHostAndPort_chat__”;`
	`window.proxyHostPort = hostPort;`
	`window.proxyHostPort` - can be used in all the **js** modules of the gadget.
		`var hostPort = “__UP_externalServerHostAndPort__”;`
		`window.proxyHostPort = hostPort;`

CSCvz26463	While updating frame-ancestors or CORS, along with the required service restarts in Finesse, reverse-proxy cache must be cleared as well.	Clear reverse proxy cache manually.

Resolved Caveats in Release 12.6(1) ES01

CDET	Description	Severity
CSCvz26771	CTI server 12.5 does not handle 50045 reason code	2
CSCvy66252	Team message is broken for agents	3
CSCvy87804	ASC gadget Queue mgmt tab not working due to big header size	3
CSCvz03952	Finesse to treat & amp ; and & in url parameter same while validating IFR requests	3
CSCvy52741	Finesse Contact List(Phonebook) usability issue due to current scrollbar behavior	3
CSCvy99583	Finesse does not respond to request - No response body	3
CSCvy21294	UPN format for SSO login not showing properly in case of subsequent logins	4
CSCvz26921	MultiTab gadgets doesn't show error when configured with invalid ur	6
CSCvz26922	Pressing conference button twice breaks functionality On Finesse UI	6
CSCvy05535	Connected Agents gadget shows general error \"Error loading items.\"	6

Troubleshooting

All logs related to the ES and Rollback installation are available in the Finesse server in the following location:

```
file get install <CopName>.log
```

For example, the log file for **finesse-cce.1261.ES02.10000.cop.sgn** ES, will be available in:

```
file get install ciscofinesse.1261.ES02.-.cop.log
```

Additional ES and Rollback COP install logs shall be located in:

```
file get install install_log_YYYY-MM-DD.HR.MIN.SEC.log
```

where YYYY-MM-DD.HR.MIN.SEC is the date and timestamp when the ES or COP was installed.

Bug Search Tool

To access the Bug Search Tool, go to https://bst.cloudapps.cisco.com/bugsearch/ and log in with your Cisco.com user ID and password.