# Gemini Guide
# To Connectivity

**CONTENTS**

# Table of Contents

## LIST OF FIGURES

# 1. Introduction

This document details the configuration necessary for External Users to access the Gemini / Exit Service.
References to various aspects of the Gemini interface have been made throughout the document.
The key points that need the readers' attention are highlighted using Blue font.

## 1.1 Purpose and Scope

This document details the necessary configuration to be done by the external users to access the Gemini Production environment. It covers the following topics:

- ✓ Network configuration required to access Gemini / Exit screen service
- ✓ Accessing Gemini / Exit API Service
- ✓ Procedures to access the Gemini Production Screen service
- ✓ Disaster Recovery arrangements (XP1)

## 1.2 Intended Audience

- ✓ Gemini external users
- ✓ Teams who provide support to external users in facilitating access to Gemini through Citrix or API

## 1.3 Gemini Services

- ✓ Gemini runs two distinct services, a screen service (accessed via Citrix) and an Application Programming Interface (API) service.
- ✓ Both services are accessed via the private network which connects the Xoserve Data Centres with external parties holding shipper or supplier licenses. This private network is known as the IX Network or IXN for short.
- ✓ Both services are accessed via the HTTPS protocol

# 2. Online (Citrix) Access Configuration Details

## 2.1 Infrastructure

The diagram (figure 1) below shows target configuration required for all external users to access Gemini using fully supported infrastructure. To achieve a fully supported infrastructure, Xoserve recommends all external users to deploy Citrix client v13 that has been fully tested using vanilla Windows operating system.

This recommended change must be impact assessed by all external users to ensure any non-Gemini access using Citrix is retained.


## 2.2 Network Requirements

The Gemini Production Screen service is accessed through a Citrix connection and it is hosted in Xoserve Data Centre at Kettering. In the event of services not being accessible from the production site, then the same can be accessed from the Disaster recovery site at Peterborough. There are separate URLs for accessing Production and the DR to access target Gemini through Citrix which are mentioned in the following sections. The following network requirements must be met in order to access the Gemini Production Screen service through Citrix.

- ✓ Network link must be established from the user location to Xoserve Data Centres.
- ✓ Port 443 must be used to submit requests to Gemini Citrix in order to access Gemini Screen service. Therefore, if you connect to the IXN via a firewall you must have this port open.
- ✓ You must resolve the FQDN prod-ix-citrix.geminints.com to the IP address 194.129.160.241 on your network. Xoserve does not provide a DNS service for access via the IXN.
- ✓ You must resolve the FQDN dr-ix-citrix.geminints.com to the IP address 194.129.160.245 on your network. Xoserve does not provide a DNS service for access via the IXN.
- ✓ Requests to the IP address 194.129.160.241 and 194.129.160.245 must be routed to Xoserve Data centres via the IXN.

## 2.3 Citrix Client for Windows

Citrix client is required to be installed on the users' desktop to be able to connect to Citrix server for Gemini. Xoserve recommends users to upgrade to a later Citrix client version 13.1 (also known as Citrix receiver 3.1) which is a supported Citrix client version.

## 2.4 Best Practices to deploy Citrix Clients

Below are some best practice guidelines to follow when deploying the Citrix clients:

- ✓ It is recommended that you download the Citrix client versions from the Xoserve Website. This will ensure that you use the Citrix client versions which have been thoroughly tested with target GEMINI. However there are other Citrix client's versions which you may wish to use and are available from the vendor (Citrix website - www.citrix.com).
- ✓ It is highly important that you assess the impact of installation of new Citrix client versions to your systems, as you may have a different combination of Operating systems, Internet explorer version or any other potential non-Gemini services hosted on Citrix services e.g. MetaFrame, XenApp within your organization.
- ✓ It is good practice to test the installation and back-out of Citrix client versions on one desktop in your environment and verify that there is no impact, before rolling out to other users as applicable, to access target GEMINI.

- ✓ As per Infrastructure best practice, it is always recommended to keep a copy of the installable file for your current Citrix client (before you proceed with the upgrade to the Citrix client versions for target GEMINI), in case you are required to revert. (If you are upgrading the Windows OS to support the new version of Citrix client then you may want to consider the necessary back-out procedure for the OS installation as well). It is to be noted however, that you will need to have the Citrix client to be able to access target GEMINI.
- ✓ Consider any other procedures that your organization (or Infrastructure support team) suggests.

### 2.4.1 Citrix Client Installation Preparation

Make sure you have met all the prerequisites mentioned in this document in the Appendix section for Citrix client installations and follow the best practices suggested in section 2.3.1. Once all the requirements are met and Impact assessment output is found to be positive to go ahead, then the following needs to be done.

- ✓ Download the appropriate Citrix clients from Xoserve Website
- ✓ Uninstall the previous versions of any Citrix client if it's already installed on your machine
- ✓ Install the new Citrix client that is downloaded from Xoserve website

**Important Notes:**

- ✓ Uninstalling and reinstalling Citrix client will require you to have administrative privileges on your desktop.
- ✓ Upgrades are also supported with a few versions of Citrix client. However to keep the installation uniform across users, it's recommended to go with new installation instead of an upgrade.
- ✓ If your organization has any deployments methods in place for deploying new software, then you are advised to check with your internal IT department and follow their instructions.
- ✓ If users decide to upgrade their System OS or IE version or plan to deploy any patches in the future, then they need to ensure that they still comply with the system requirements/pre-requisites as mentioned in this Citrix user guide before they do so. If the prerequisites mentioned in this Citrix user guide are not met at any time, there is a risk that the Citrix client may not work with target GEMINI. As per best practice; it is also advised to perform appropriate impact assessment, review and tests prior to rolling any upgrade.

**Disclaimer:**

- Both the Citrix client versions are tested for accessing target Gemini on Windows XP Operating System with IE8 and Windows 7 Operating System with IE version 9. If you are using any other OS versions and/or browser versions, then it is recommended that you test the Citrix client versions with your setup and test access to target GEMINI. Xoserve will endeavor to provide assistance where possible; however the ultimate responsibility lies with you.
- Post GRP Go-live, Xoserve recommends that you install Citrix client version 3.1. However if you continue to use Citrix client version 11.0.0.5357 (which you would have installed as part of Readiness Testing before GRP Go-live) and if there are any support requirements, then vendor support might not be available.
- At any time, if user does not meet the pre-requisites mentioned for the Citrix clients under the Appendix section in this document, there is a risk that the Citrix client may not work with target GEMINI. User is responsible for ensuring the pre-requisites are met in order to be able to install/use the Citrix client mentioned in this document with target GEMINI.
- You will need to ensure that you follow the best practices for Infrastructure deployment and that you have the necessary backups/installable to revert back if you need to.

## 2.5 Gemini Production access through Citrix

Launch the URL prod-ix-citrix.geminints.com/ to access the Production Gemini Citrix. The Citrix home page displays with the heading "Gemini Production Citrix Access" (Figure 1).

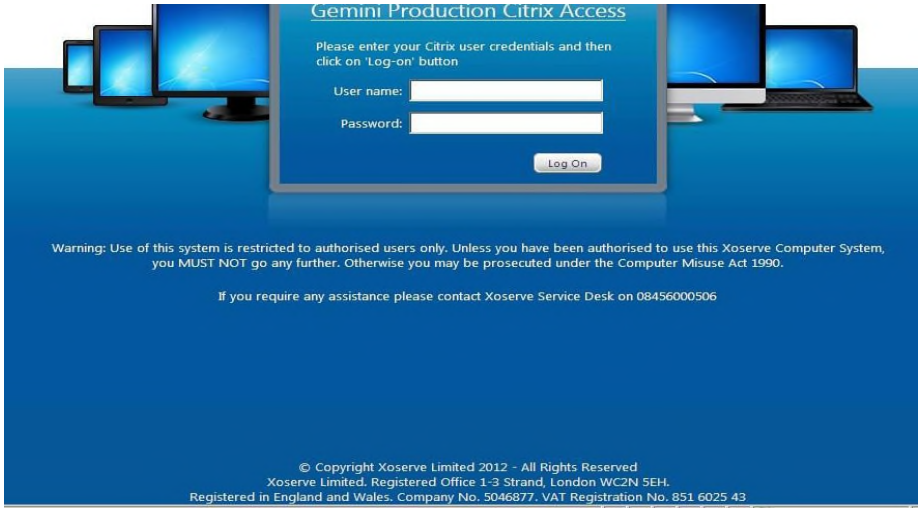



**Figure 1**

Enter your Citrix Username and Password and click the Logon button. The first time users' login they will be provided with a default password; Users will then be prompted to change the password for the first time. The following password complexity requirements should be met when setting up a new password:

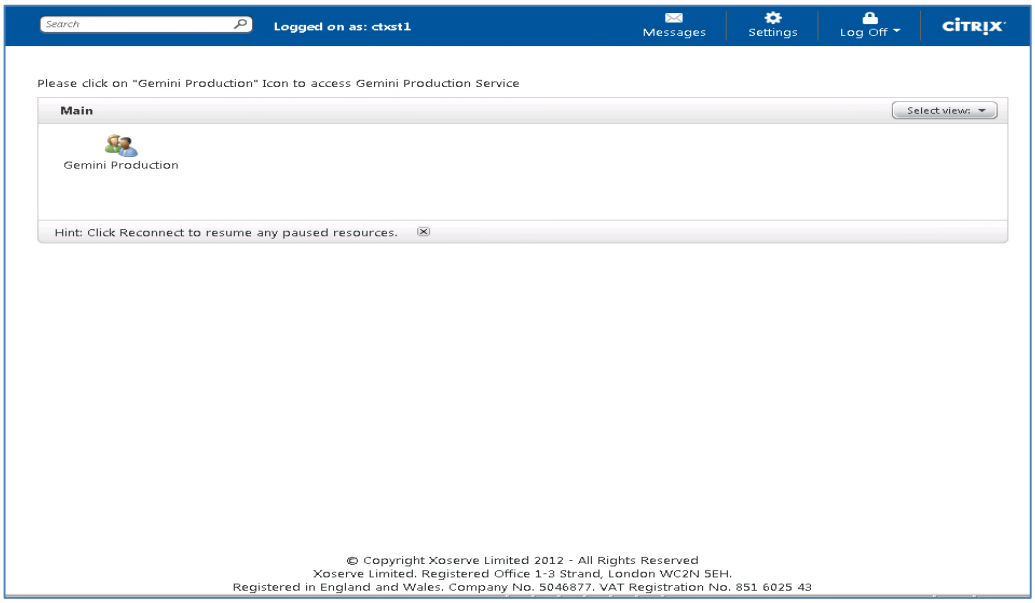
a. The password should not contain the user's account name or parts of the user's full name that exceed two consecutive characters
b. Minimum Password length should be 8 Characters
c. The password should contain characters from three of the following four categories:
   - ✓ English uppercase characters (A through Z)
   - ✓ English lowercase characters (a through z)
   - ✓ Base 10 digits (0 through 9)
   - ✓ Non-alphabetic characters (for example! $, #, %)

Other settings as per the group policy for Citrix users are:

- ✓ Minimum Password age (The period of time that a password must be used before the User can change it) - 1 Day

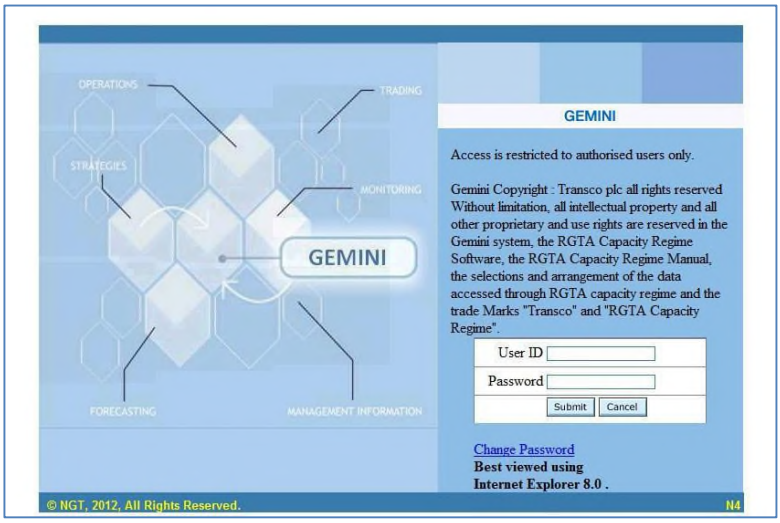
- ✓ Maximum Password age (The period of time that a password can be used before the system requires the User to change it) - 30 days
- ✓ Enforce password history - 5 passwords remembered

Once authenticated a window containing the "Gemini Production**"** icon will be displayed as shown in figure 2. Click the "Gemini Production" icon to access the Gemini Production environment.



## 2.6 Gemini Logon

The Gemini Production logon page is displayed as shown below. Enter your Gemini screen service credentials to access it further.




**Important Notes:**

Click on the "Gemini Production" icon to invoke the Citrix client. For the first time after invoking, you will be prompted to specify permissions you wish to grant to your local files. Gemini Citrix servers are configured with the setting "Map Client Drives" turned on. This will allow you to seamlessly save Adobe PDF report files to your desktop.

When you display these reports within the Citrix client they're generated within Adobe Acrobat Reader running on the Citrix server. You should open the "File Save" dialogue from within Adobe Acrobat Reader, your workstation local drives are mapped as "Local Disk ('*Drive Letter*': on '*your desktop name*') and appears in the list of available drives that are visible to the application, for example "Local Disk *C*: on *Computer1*".

In order to facilitate this feature, the following access permissions are recommended:

- Choose the "Permit All Access" option, if you are using Citrix Receiver 3.1, and check the "Do not ask me again for this site"
- Choose the "Full Access", if you are using Citrix Receiver 11 and check "Do not ask me again"

If you do not do this, you will be unable to save PDF files locally. The same principle applies when saving Comma Separated Variable (CSV) files locally.


**Client File Security Prompt in Citrix Receiver version 3.1**


**Client File Security Prompt in Citrix client version 11**

# 3 Disaster Recovery (D/R) Arrangements

Xoserve has arrangements in place to provide Gemini services from an alternative location in the event of loss of its primary site. Xoserve will notify external parties if Xoserve chooses to invoke these procedures.

## 3.1 Citrix DR

The alternative arrangements required on your part are as follows:

- ✓ Target Gemini screen service accessed via Citrix DR link (Disaster Recovery) will be hosted at Xoserve Peterborough Data centre. You must resolve the FQDN "dr-ix-citrix.geminints.com" to 194.129.160.245 on your network. And you need to use the URL dr-ix-citrix.geminints.com to access DR site services.

## 3.2 API DR

- ✓ The Gemini API service will also be hosted at Xoserve Peterborough Data centre. You will continue to use the same FQDN (prod-ix.geminints.com), but the IP address should be pointed to 194.129.160.246. This dictates that you cannot have simultaneous access configured to both production and DR API services, as the FQDN resolutions are mutually exclusive.

All other arrangements (https protocol, routing via the IXN, ports, etc.) are the same as for the Production services.

## 3.3 Access via XP1

### 3.3.1 XP1 Tokens

Xoserve supply any User who requests access via XP1 with a security token, logon name and PIN code allowing access to the XP1 Gemini contingency system. This enables Users to continue to access Gemini via a SSL VPN link based on the dual factor authentication. This link is intended to be used by users when their Primary IX link becomes unavailable. Please note that a User's Internet Explorer (IE) setting should allow the user to Install ActiveX control to successfully connect to the XP1 service.

A User may only use the XP1 service as a contingency mechanism, subject to the following limits:

- XP1 will be available on a best endeavors basis at all times other than during planned maintenance.
- Where a User invokes XP1 due to a perceived failure of their main IX system, the User must inform the Transporters of the failure.
- Transporters shall have no liabilities or obligations in respect of XP1 and its use by any UK Link User other than those which are set out in Appendix 3 (UK Link manual).
- There will be no consequential change to any procedure associated with energy balancing.
- If you do not have an XP1 token you should contact the Xoserve Customer Life Cycle team, customerlifecycle.spa@xoserve.com, to request one.

### 3.3.2 XP1 Link Set up instructions

Full details of system requirements and step by step instructions for invoking the XP1 link and for accessing the Gemini application over the XP1 link can be found via www.xoserve.com.

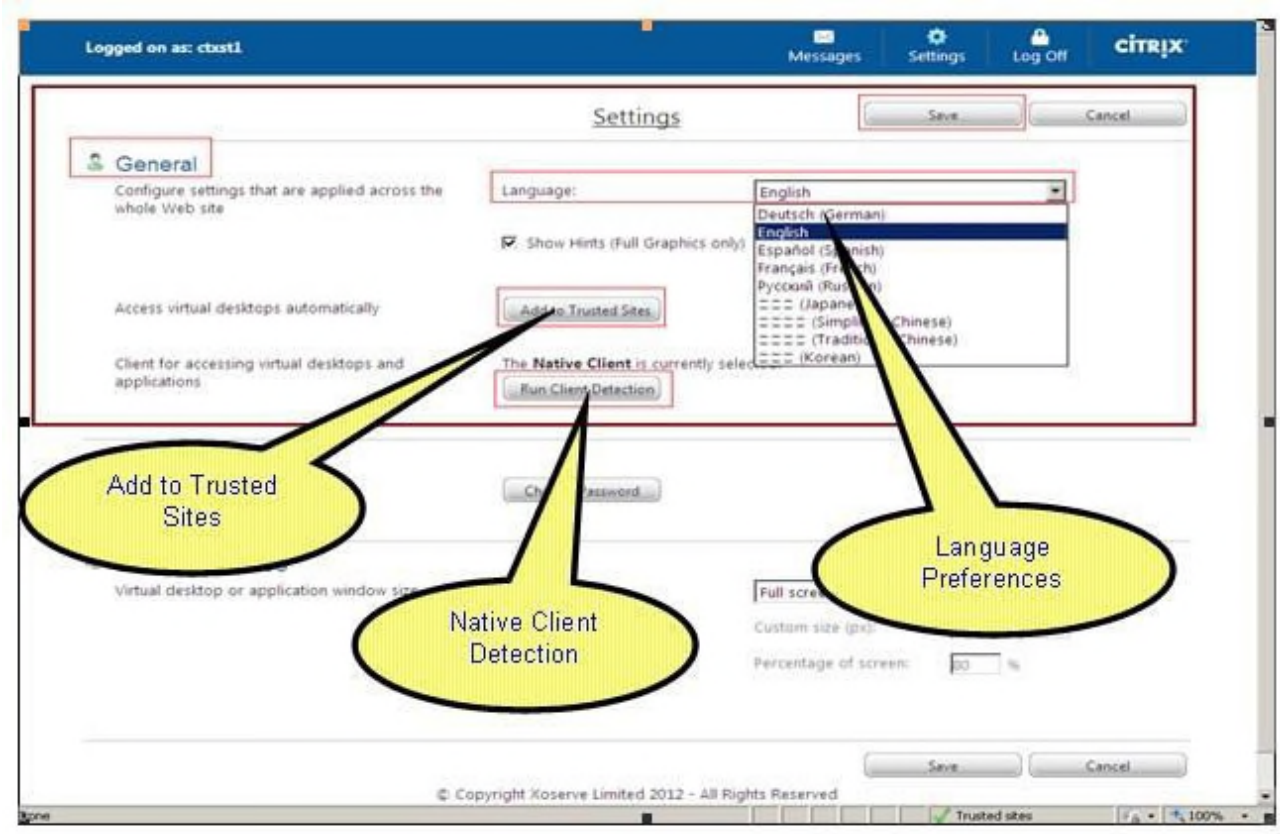
# 4. Other Settings

## 4.1General

- Citrix XenApp Settings portal provides the option to set the preferred language in the 'Language' dropdown of 'General' section. Please note that the settings you choose are applied throughout the Citrix XenApp website. Whatever setting you choose is remembered from one Citrix session to the next. It becomes the default for your Citrix user-id until you use the Settings menu to alter it again.
- You may also add the Target Gemini Citrix URL to Trusted Sites by clicking "Add to Trusted Sites" and follow the instructions mentioned in that wizard. Note that you may need to obtain the agreement of your system administrator before you change the security zone setting for a Web site.
- You may click "Run Client Detection" which enables users to start the client detection and deployment process manually. It can also detect the presence or absence of an installed client and prompt the user, when necessary.

The above mentioned settings are marked red in the following figure:

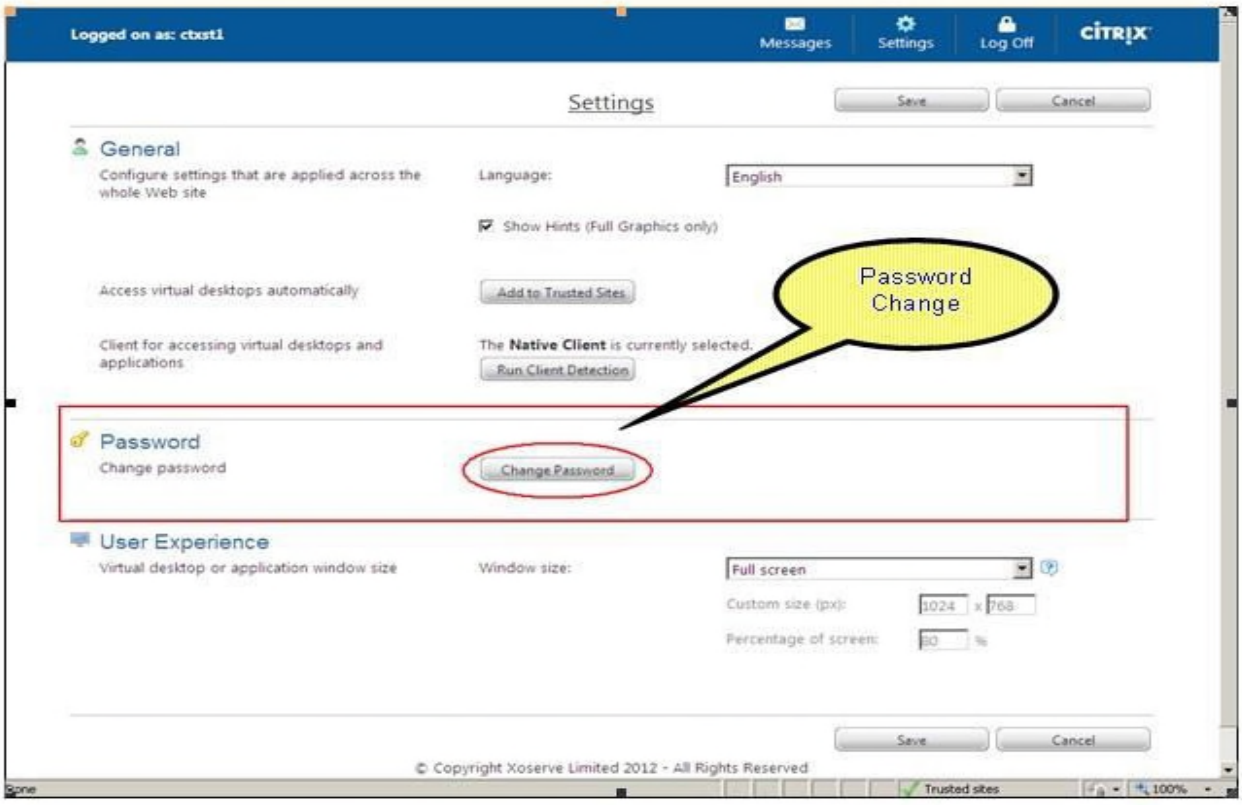
**Figure 11 -Citrix Settings**



## 4.2 Manually Changing Password

You can also manually change your Citrix login-id password anytime as and when required once you login to the Citrix portal by clicking 'Settings' toolbox. Citrix XenApp Settings portal provides the option to change your Citrix Login Password by clicking Change Password from the Password section, as shown below.

**Figure 12 -Citrix Settings for password change**




The following password complexity requirements should be met while setting the password:

- Password should not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Minimum password length should be 8 Characters.
- Contains characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, $, #, %)

Other settings as per the group policy for Citrix users are:

- Minimum password validity - 1 day
- Maximum password validity - 30 days
- Enforce password history - 5 passwords remembered

# 5. Appendix:

## 5.1 Prerequisites for Citrix Client Installation

Before you install the Citrix client on your machine, refer to the prerequisites details attached for Citrix client version 13.1 (also known as Citrix receiver 3.1) as below. Make sure you have met all the requirements mentioned in the document for various versions before you install them.

## 5.2 Acronyms

**Table 1-Acronyms**

| Acronym | Description |
|---|---|
| AD | Active Directory |
| API | Application Programming Interface |
| DNS | Domain Naming System |
| DR | Disaster Recovery |
| FQDN | Fully Qualified Domain Name |
| GRP | Gemini Re-platform Programme |
| HTTPS | Hypertext Transfer Protocol Secure |
| IE | Internet Explorer |
| IXN | Information Exchange Network |
| NIC | Network Interface Card |
| OS | Operating System |
| SSL | Secure Socket Layer |
| SVGA | Super Video Graphics Array |
| TCS | TATA Consultancy Services |
| TTD | Test Trail and Development |
| UAC | User Access Control |
| URL | Uniform Resource Locator |
| VGA | Video Graphics Array |

# 6. Document Control

## 6.1 Superseded Documents

| Version Number | Status | Date | Organisational Unit | Revision Summary |
|---|---|---|---|---|
| 0.1 | Draft | 13/09/2012 | TCS | Created document |
| 1.0 | For Review | 05/09/2012 | TCS | Approved for UKL representation |
| 1.0 | For Representation | 26/09/2012 | TCS | |
| 1.1 | For Representation | 10/12/2012 | TCS | Updated DR Section |
| 2.0 | Approved | 11/12/2012 | TCS | Approved Version |
| 2.1 | Approved | 05/02/2013 | TCS | Updated done post pip testing |
| 2.2 | Approved | 08/02/2013 | TCS | Changed TCS DC to Xoserve DC |
| 2.3 | Approved | 26/02/2013 | TCS | Updated DR IP address |

## 6.2 Version History

| Version Number | Status | Date | Organisational Unit | Revision Summary |
|---|---|---|---|---|
| 0.1 | Draft | 10/7/13 | GRP Project Team | Created document |
| 1.0 | Approved | 19/08/13 | Andrew Boyton | Quality Review |
| 2.0 | For Review | 23/11/2016 | Gemini Application Support | Modified after EU implementation |
| 3.0 | Approved | 27/03/2017 | Gemini Application Support | Document restructured |

## 6.3 Reviewers

| Name | Organisational Role | Organisational Unit |
|---|---|---|
| Rob Smith | Gemini System Manger | Xoserve |
| Palanisamy, Gokulakannan | System Analyst | Wipro |
| Nikhil Kumar | Application Support Manager | Wipro |
| Mark Hall | IS Strategy Officer | Xoserve |
| Darren Jackson | Customer Lifecycle | Xoserve |
| Kumar Dhanapal | TCS Supply Lead GRP | TCS |
| Nathan Fellows | IS Coordinator | Xoserve |

## 6.4 Approvers

| Name | Organisational Role | Organisational Unit |
|---|---|---|
| Andrew Boyton | GRP Project Manager | Xoserve |